Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы
Международной научно-практической конференции
(Минск, 18 мая 2017 г.)

Минск
Академия МВД
2018

УДК 004:34
ББК 32.81
Т33

Т33 **Теоретические и прикладные проблемы информационной безопасности** : тез. докл. Междунар. науч.-практ. конф. (Минск, 18 мая 2017 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» ; редкол.: А.В. Яскевич (отв. ред.) [и др.]. – Минск : Академия МВД, 2018. – 231 [1] с.
ISBN 978-985-576-096-3.

Рассматриваются вопросы, посвященные теоретическим и прикладным проблемам информационной безопасности, анализу перспективных методологических подходов к ее решению, созданию и внедрению систем защиты информации в информационных системах правоохранительных органов, а также подготовке специалистов в сфере защиты информации и информационно-аналитического обеспечения правоохранительной деятельности.

Издание предназначено для научных работников, занимающихся проблемами информационной безопасности, сотрудников правоохранительных органов, а также специалистов в области защиты информации и специалистов подготовки кадров.

УДК 004:34
ББК 32.81

ISBN 978-985-576-096-3

ПРИВЕТСТВЕННЫЕ СЛОВА УЧАСТНИКАМ КОНФЕРЕНЦИИ

**Приветствую вас на белорусской земле,
в городе Минске, в учреждении образования
«Академия Министерства внутренних дел Республики Беларусь»!**

Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности» проводится уже пятый раз в стенах академии. Со времени проведения первой конференции в 2010 г. научные круги Республики Беларусь и наши коллеги из государств ближнего и дальнего зарубежья активно включились в разработку вопросов информационной безопасности. Сегодня данный форум стал одним из ведущих международных мероприятий, на котором обсуждаются перспективные методологические подходы к проблеме информационной безопасности и вырабатываются адекватные средства ее решения, происходит обмен опытом создания и внедрения систем защиты информации в информационных системах, анализируются инновационные подходы к подготовке специалистов в сфере защиты информации и информационно-аналитического обеспечения правоохранительной деятельности, исследуются теоретические и прикладные вопросы использования современных информационных технологий в работе правоохранительных органов.

Мы осознаем, что информационно-коммуникационные технологии являются эффективным инструментом содействия делу мира, безопасности и стабильности, укрепления демократии и социальной сплоченности граждан, надлежащего управления и верховенства права на национальном, региональном и международном уровнях. Современные информационные технологии не только существенно расширяют возможности повышения эффективности государственного управления, но и являются важным фактором экономического развития общества, повышения эффективности социальной политики государства, развития политической культуры граждан.

В то же время всех нас объединяет понимание того, что для продолжения интенсивного развития информационной сферы наших стран необходимо обеспечить эффективное противодействие угрозам использования современных информационных технологий в целях нарушения международного мира и безопасности, совершения преступлений, подготовки и осуществления террористических актов, распространения террористической идеологии и практики разрешения противоречий общественного развития.

Следует констатировать, что эффективное противодействие всем этим угрозам невозможно без широкой международной координации политики в данной области. Универсальный подход к анализу задач защиты информации, нацеленность на рассмотрение вопросов, имеющих высокую практическую значимость, способствуют утверждению репутации конференции «Теоретические и прикладные проблемы информационной безопасности» как важной инициативы по обеспечению безопасности Республики Беларусь и стран СНГ.

В этой связи нельзя не отметить высокую представительность данной научно-практической конференции. В ней принимают участие практически все заинтересованные стороны: сотрудники правоохранительных органов, работники государственных органов и предприятий, специалисты в сфере информационной безопасности, профессорско-преподавательский состав учреждений высшего образования Беларуси и соседних стран, аспиранты, курсанты Академии МВД Республики Беларусь.

Выражаю уверенность в том, что приоритеты развития информационных технологий, которые предстоит определить участникам конференции, позволят значительно повысить эффективность защиты информационного пространства наших государств в современных условиях, помогут содействовать установлению и развитию взаимовыгодного сотрудничества Академии МВД Республики Беларусь с учреждениями образования Сербии, Молдовы, Украины и России.

Желаю участникам конференции успехов в решении поставленных задач, активной и результативной работы в достижении целей обеспечения безопасности информации!

Проректор Академии МВД Республики Беларусь
по научной работе кандидат юридических наук, доцент
А.В. Яскевич

Приветствую организаторов, участников и гостей Международной научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности», проводимой Академией Министерства внутренних дел Республики Беларусь!

Тематика конференции традиционно охватывает широкий круг правовых, методологических и организационно-технических аспектов теоретических и прикладных проблем обеспечения информационной безопасности. Ученые Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) принимают участие в организации, подготовке и работе конференции с самого ее основания.

Инициативно возникшее сотрудничество и кооперация ученых и специалистов СПИИРАН, Института государства и права РАН, Академии МВД Республики Беларусь и Института национальной безопасности Республики Беларусь оказалось весьма плодотворным. Только за последнее пятилетие совместными усилиями выполнен ряд интеграционных разработок, подготовлены проекты десятка международно-правовых документов, относящихся к сфере информатизации, информационного права и информационной безопасности, защищены диссертации. Материалы этих работ представлены в докладах участников конференции.

Желаю участникам конференции плодотворной работы! Выражаю уверенность, что проводимая конференция будет способствовать более глубокому пониманию проблем информационной безопасности, внесет существенный вклад в укрепление национальной безопасности Беларуси и России, способствуя развитию и углублению интеграционных процессов между нашими государствами.

Директор Санкт-Петербургского института информатики и автоматизации Российской академии наук член-корреспондент РАН
Р.М. Юсупов

Уважаемый Владимир Владимирович!

От имени Секретариата Парламентской Ассамблеи Организации Договора о коллективной безопасности приветствуем участников международной научно-практической конференции «Теоретические и прикладные проблемы информационной безопасности» (Минск, 18 мая 2017 г.).

Многие годы конференция является одной из площадок конструктивного диалога и сотрудничества ученых, специалистов, представителей высших законодательных и исполнительных органов государств – членов ОДКБ по разработке региональных стандартов регулирования отношений, складывающихся в области обеспечения безопасности стремительно развивающейся информационной сферы.

Высоко ценим вклад участников конференции, ученых Академии МВД и других компетентных органов Республики Беларусь в интернациональные усилия, направленные на обеспечение информационной безопасности и решение особо чувствительных вопросов в данной области.

Искренне верим в то, что установившаяся тесная кооперация, гармонично дополняемая рамками ежегодно проводимой конференции, позволит и впредь успешно решать общие задачи, встающие перед государствами – членами ОДКБ.

Желаем организаторам и участникам конференции успехов в достижении поставленных целей.

Ответственный секретарь Парламентской Ассамблеи Организации Договора о коллективной безопасности
П.П. Рябухин

РАЗДЕЛ 1

АКТУАЛЬНЫЕ ПРАВОВЫЕ И МЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

УДК 343

Д. Ранделович, К. Кук, В. Боровик, Д. Младенович, Д. Эрлевайн

INFLUENCE OF THE OPERATING SYSTEM ON THE FORENSICS TOOLS

A large number of computer crimes is emerging almost every day in the world. Following the technology development this situation will continue for sure. It is obvious that we are more often the victims of a new type of crime, the modalities and the 'modus operandi' develops with a hitherto unseen dynamics. To successfully counter this type of crime, it is necessary to implement a comprehensive prevention, and if it does not produce the desired results, a key role in the discovery of the perpetrator and collection of the evidence of his guilt is now taken by a young discipline of forensics – digital forensics.

In the literature pertaining to the field of digital forensics, you may see different names for the discipline, such as computer forensics, digital forensics, cyber forensics, etc. Computer forensics: computer uses digital technology to develop and provide evidence in court and prove or disprove a claim. A slightly different definition is given by John Vacca, and in his opinion, computer forensics involves the preservation, identification, extraction and documentation of evidence stored on digital computer. It is interesting that in some cases, digital forensics is also seen as a science and as an art using IT knowledge and skills to assist in the resolution of any legal process. Simply put, digital forensics is the process of collecting, preserving, analyzing and presenting digital evidence. In most cases, the terms 'computer forensics' and 'digital forensics' are regarded as synonymous, but among them there is still some difference. Unlike computer forensics relating to the collection of digital evidence stored on a computer (PC), digital forensics is a more general term and refers to all the devices that can carry digital data.

When an incident occurs, the process of digital forensic investigations starts. Digital forensics is crucial for the successful detection and prosecution of criminals in the area of computer crime. When you start this procedure, its duration must be conducted in accordance with the law, because only in this way evidence gathered in this process may be valid in court. There is general agreement in the literature on the sequence of procedures, but there are different opinions on the number of phases. In most cases, we talk about the four stages, although there are cases where this number is three, five and even seven stages.

The process of digital forensic investigation consists of the four following stages:

acquisition, the so-called bit-by-bit copy of data is made- this copy is called a disk image;

searching, disk images are 'start-up' on a computer-elimination of files which not digital evidence;

analysis, where comes the interpretation of digital evidence;

presentation of the results obtained from the previous phase.

According to one definition, digital evidence is defined as any information that is stored or transmitted using a computer and that supports or refutes the theory of how the offense was performed and who was its executor. Also, they can be defined as the data and information that are of relevance to the investigation, which are stored or transmitted by electronic device in digital form. Simply put, digital evidence is any information in digital format (consisting of 1 and 0), which is relevant to the legal proceedings. These can be various patterns of text, images, sound clip, video clip, or combinations thereof. UNIX was a serious system when Windows was introduced so the majority of free tools and utilities are developed under Linux.

As widely known, digital evidence is stored within a computer system, so it is impossible to see the content without the help of appropriate forensic tools. There are a number of tools. Some of them are used for one purpose, while others have a much greater range of options. The choice of tools to use depends on the specifics of the investigation. It is always desirable to choose the tool that will contribute to the most reliable way of achieving the objective for which it is used. Forensic tools can be divided into several groups, but it should be noted that, according to the functions they perform, they must not strictly belong to one particular group. In the literature, in most cases, the tools are classified into commercial and non-commercial tools, i. e. those that are licensed and those that are open source.

Commercial tools are made mainly for the Windows platform. These tools have many modules integrated into a single program, so generally cover more areas of the process of digital forensic investigations. What appears as a problem with these tools is that they are paid and are costly.

Non-commercial tools are not paid, they are running on Linux, and they usually incorporate all aspects of the process of digital forensic investigations. What is important for these tools is that they can make a full investigation, i. e. provide all the features that have the expensive commercial tools. In the open source tools, source code is available for consideration and further customization. That is what makes them very functional and we can find this in literature.

The origins of computer forensic analysis lie not with the Windows operating systems which has achieved such popularity today but with UNIX, an operating system with its roots in the early 1970-s. The developers of UNIX preferred to create a fairly large number of small programs which could be used together to perform more complex tasks rather than one program which could do everything and it is from these small programs that the sophisticated commercial computer forensic packages available today have grown. The small programs are still found in modern versions of the UNIX operating system and many are also available for Windows.

In addition to shortly described non-commercial software for digital forensics, it is necessary and obligatory to stress out so called integrated forensics tools group, which integrate various (mentioned) non-commercial tools and their different combinations. So, for example, SIFT workstation tool developed at the SANS Technology Institute (as a master's level graduate school in the USA) integrated among others Autopsy, Grep and Wireshark software, and iA3, developed at the Academy of Criminalistics and Police Studies, Belgrade, Serbia integrated only DD, Autopsy and Wireshark software.

The difference between the SIFT Workstation and iA3 tools are that the SIFT Workstation can be started only by virtual machines which leads to that using this tool is impossible to perform live forensic analysis of data, as this causes a disruption of media. What distinguishes iA3 tool, which we designed in relation to the SIFT Workstation is that it can start live, from a USB drive or by using a 'live' version of Windows To Go system where there is no access to or modification of the media or the data on them.

Another important difference between these two tools is that when taking pictures of the media 'Put to death', to prepare and raise system to work SIFT Workstation certainly needs more time than it is necessary for the preparation and awareness tools iA3. From the foregoing, we conclude that these are two evident advantages of iA3 tool in relation to the SIFT Workstation.

To find influence of Windows and different Linux platform on integrated digital forensics tool IA it is necessary to give a practical example comparing just these versions of tools and it will be the subject of the next

part of this scientific work. For the purposes of this example we used a USB memory, 512 MB and therein lies the document prazan.docx and document proba.docx we previously deleted. In this particular case we compare the time which is necessary that these integrated tools of digital forensics do their bit by bit recording media.

In these examples, the timing that is needed to run some analyses or the features provided by these tools was measured. The speed start tool, the speed of acquisition of the media, evidence download speed, the speed of file analysis, the speed of search by keyword, the speed of search by file types, the speed of live analysis and the speed of drafting the report were measured for both integrated and non-integrated tools.

This research was based on measuring the between start and finishing each of observed i3A tool actions. While iA3 tools start was instantly, it was much longer with the SIFT Workstation, ABOUT 1 minute and 25 seconds (fig. 1–3).

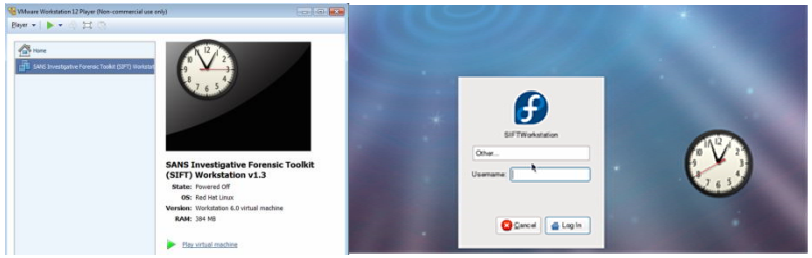

Fig. 1. Start to finish SIFT-Fedora Linux based tool from the virtual machine

Figure 2 and Figure 3 show one of this measurement which is connected with loading files in Autopsy.

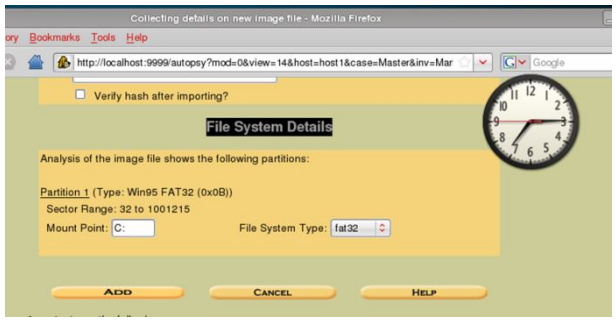

Fig. 2. Start of loading in Autopsy

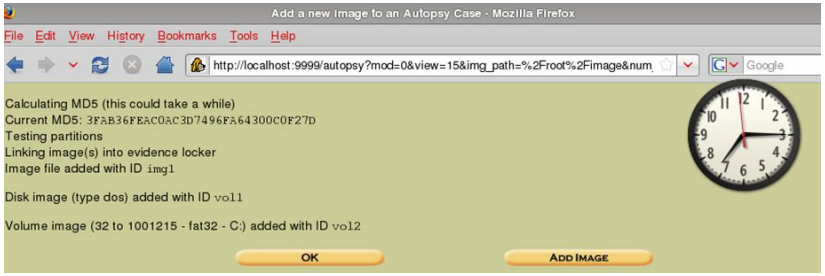

Fig. 3. Completion of loading in Autopsy

Also, the time needed to produce a report in Autopsy was watched and it was immediately. The next chapter will show all the values obtained from these measurements and comparisons performed.

Table 1 shows the results obtained when measuring the speed that is needed to perform certain analyses. And here we see that every tool has its own advantages and disadvantages.

Table 1

Comparison of the most important technical characteristics of integrated and non-integrated tools

Type of analysis	SIFT Windows	IA3 Windows	I3A Ubuntu	I3A Knoppix
Start	1min 25s	Immediately	Immediately	Immediately
Acquisition	1min 52 s	Seen 55 s	55 s	55 s
Loading Image	14 s	14 s	14 s	14 s
Analysis of the file	19 s	19 s	17 s	18 s
Search by keyword	1 min 40 s	1 min 40 s	1 min 38 s	1 min 40 s
Search by file type	39 s	39 s	38 s	40 s
'Living' analysis	1 min 24 s	1 min 24 s	1min 24 s	1 min 24 s
Preparing reports	Immediately	Immediately	Immediately	Immediately

Application I3A based and created in a way that using a GUI it is fully implemented in Windows environment, was tested on different Linux versions, therefore with different demands.

The functionality of I3A was tested with the following Linux OS versions, Ubuntu, Fedora and Knoppix, as live versions, together with desktop (Workstation) versions.

Necessary components for this application to work is the application Wine Developer, addition package named Wine-Mono which has the necessary files for working under the Linux. We also needed an implemented runtime dot Net Framework 4, along with an active internet connection for acquiring the right packages and installers (fig. 4).

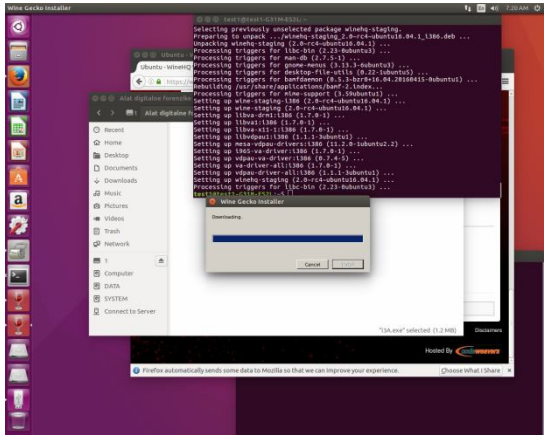

Fig. 4. Online instalation and acquirement of necessary packages of Wine application

Successful results, were accomplished with Ubuntu and Knoppix and the following Figures show the test results (fig. 5–6).

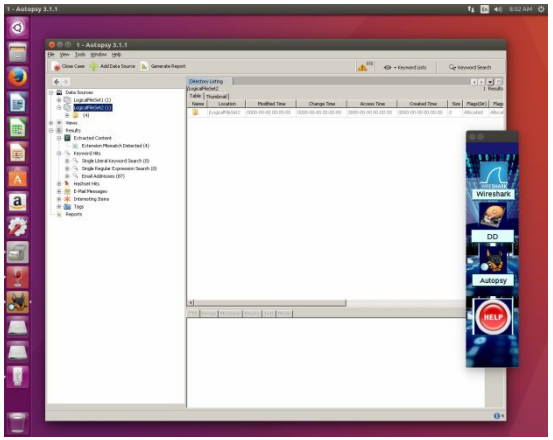

Fig. 5. The end of a second session. The data was fully readable and clear

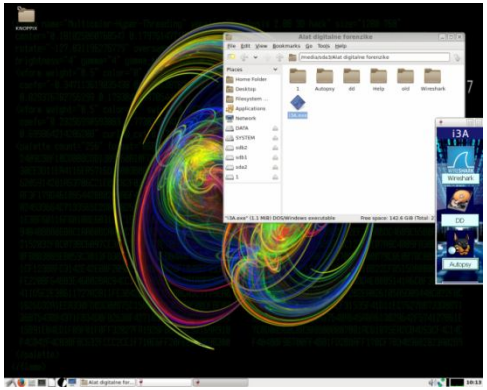

Fig. 6. Testing I3A on a Knoppix OS

The tool mentioned in this paper, SIFT workstation as integrated tool, is recognized and accepted by the courts of the USA on the basis of permanent positive Daubert test. In order to determine whether the forensic tool iA3, which is developed at the Academy of Criminalistic and Police Studies, is acceptable to the court, or whether the evidence obtained with this tool are admissible in court Daubert test was used.

Daubert process identifies four general categories that were used as the main evidence in assessing acceptability of the tool in court:

1. Testing: Can it be tested and whether the procedure was tested?
2. Expectancy: Is there a known probability of error of the procedure?
3. Publications: Is the procedure public?
4. Acceptability: Are the procedures generally accepted by the relevant scientific community?

The software solution has been done according to the regulations of the Ministry of Education, Science and Technological Development, and the tool iA3 is tested by the Ministry of Internal Affairs (the Cybercrime Department). The tool testing started in 2015 and it is still being tested. After completion of the test the evaluation and the possibility of its admissibility in court will be given.

The probability of error, which refers to errors known as “bugs” in the work tools where not noticed while working with these tools and in the previous test.

The tool has been published in several publications:

a) D. Randjelović, D. Delija, D. Stojković, M. Velicković, D. Erlevajn. COMPARING INTEGRATED AND NON-INTEGRATED DIGITAL FORENSICS TOOLS, Thematic Conference proceedings Archibald Reiss days, Vol. 3. Pp. 239–262. Belgrade, 2016;

b) T. Milanović, K. Kuk, D. Randjelović, P. Čisar Text mining techniques and identification of information by documents written (in Serbian) in High-end International Forum on Public Security Technology Informatisation, Shenyang, China, September 2015.

The tool is set up and is available on the website of the Academy of Criminalistic and Police Studies.

Based on everything mentioned above, we can say that iA3 is pretty good software solution that could be accepted in court and also from the technical standpoint it has best characteristics under Linux Ubuntu.

This work was supported by the Ministry of Science and Technology of the Republic of Serbia under the Project no. III 44007 and TR34019.

УДК 343.346.8:004:351.746:007

Ю.Г. Булай, Р.И. Булай, А.В. Патрашко

СЕТЕЦЕНТРИЧЕСКАЯ И КИБЕРВОЙНА – РЕАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ СОВРЕМЕННОГО МИРА

Существование современного мира немыслимо без информационных технологий, они стали неотъемлемой частью общества и каждого индивида в отдельности. Информационные технологии представляют огромные возможности для упрощения и улучшения всей жизнедеятельности человечества.

Стремительное развитие информационных технологий и информатизации общества привело к появлению новых видов преступлений и угроз, таких как киберпреступность, кибертерроризм, сетецентрическая и кибервойна.

Кибершпионаж, киберпреступность, кибертерроризм – феномены, получившие развитие в виде глобальной киберугрозы сетецентрической и кибервойны. При этом необходимо подчеркнуть, что как в материальном мире, так и в электронном пространстве все эти феномены тесно переплетены и взаимодействуют между собой. Такое взаимодействие характерно также для атакующих субъектов и объектов, подвергаемых атакам. Эти участники преступного поведения используют зачастую схожие программные средства, имеют сходные режимы их применения.

Боевые действия, к которым мы привыкли, меняют свое лицо, действующих агентов и саму логику. Помимо стандартных вооруженных конфликтов мы все чаще говорим о кибератаках, киберпреступности, кибершпионаже и кибертерроризме, информационной войне. Все эти процессы приводят к появлению новой терминологии: от гибридных и

асимметричных войн до сетецентричных операций и боевых действий вне условий войны. Такие причудливые определения пополняют новые военные доктрины различных стран.

Феномен сетецентрической войны и кибервойны – концепции, ставшие реальностью в XXI в. В оперативном искусстве и тактике за последние десятилетия произошли принципиальные перемены, которые требуют от государств радикального пересмотра прежних военных доктрин и критической переоценки всего спектра областей военного искусства. По сути дела, сегодня речь идет уже о появлении нового военного искусства, когда прежние оценки, опыт и знания требуют радикального пересмотра либо даже отказа от прежних взглядов.

Период глобализации с переходом от промышленной к информационной эре затрагивает все страны, что определяет информацию не только как важную составляющую этого процесса, но и наиболее эффективное оружие. А так как преобладающим типом человеческого поведения в информационную эпоху является сетевое поведение, то, по мнению некоторых авторов, сетецентрическая война подходит этому времени как нельзя лучше. Согласно доктрине Пентагона, ядро такой войны находится на пересечении социальной, физической, информационной и когнитивной областей. Если информация еще связана с определенной инфраструктурой, то когнитивная сфера наименее материальна из всех четырех областей, потому что существует в сознании человека.

Эксперт по безопасности правительства США Ричард Кларк пишет в своей книге «Кибервойна» (2010): «Кибервойна – действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Британский журнал The Economist описывает киберпространство как «пятую область войны, после земли, моря, воздуха и космоса».

На данный момент существуют феномены информационной войны и сетецентрической и кибервойны. Кажется, что они похожи, но они разделяются по объектам и средствам боевого воздействия.

Информационные войны – это войны, имеющие своей целью изменение массового, группового и индивидуального сознания. В процессе информационных войн идет борьба за умы, ценности, установки, поведенческие паттерны и т. п. Информационные войны велись задолго до интернета, они имеют историю, измеряемую даже не сотнями, а тысячами лет. Интернет просто перевел эти войны на качественно иной уровень интенсивности, масштабности и эффективности. Что же касается сетецентрической и кибервойны, то они предполагают целенаправленное воздействие информационных потоков в виде программ-

ных кодов на материальные объекты и их системы с целью разрушения, нарушение функционирования или перехвата управления.

В идеальной форме агентами сетевой войны являются сети небольших разнотипных объединений, напоминающие ячейки, которые рассредоточены, но взаимосвязаны. Сеть должна быть аморфной – без сердца и головы, хотя не все узлы сети должны быть эквивалентны друг другу. По мнению некоторых специалистов, наилучшая тактика ведения боя в прямом и переносном смысле – роение. Подобно рою пчел, группы лиц, объединенные общей идеей, синхронно начинают атаковать цель, будь то государство или транснациональная корпорация. Превосходящая по силе и потенциалу своих противников цель, тем не менее, вынуждена реагировать на каждый мельчайший «укус», а если атакующие обладают определенной техникой и искушены в конфликте, то исход практически предрешен. Эта тактика напоминает «волчью стаю» подводных лодок Германии времен Второй мировой воины.

Реальное существование киберугроз кибертерроризма, сетецентрической и кибервойны требуют от государств радикального пересмотра прежних доктрин кибербезопасности и критической переоценки информационных систем, обеспечивающих деятельность объектов критической инфраструктуры (предприятия топливно-энергетического комплекса, энергораспределяющих сетей, систем контроля и управления наземным, морским и в особенности воздушным трафиком), так как в случае поражения программными средствами они могут представлять угрозу национальной и международной безопасности.

Органы государственной власти и местного самоуправления подчас подвергаются еще большему воздействию киберпреступников и кибертеррористов, организующих шпионаж, хищение данных из государственных или частных стратегических информационных систем и/или препятствующих нормальной работе. Одна из первых подобных кибервойн произошла в апреле 2007 г., когда в связи с решением эстонского правительства о переносе памятника Воину-освободителю сайты государственных структур страны подверглись организованным атакам.

Крайне болезненным этот удар стал из-за наличия в Эстонии развитой системы так называемого электронного государства, к которой активно стремятся перейти не только европейские, но и ведущие азиатские страны.

В июне 2010 г. жертвой кибератаки стал Иран: когда в компьютерную сеть исследовательского ядерного центра в Натанзе был занесен компьютерный вирус Stuxnet, пострадали более 60 тыс. компьютеров. В марте 2013 г. были взломаны компьютерные сети ряда крупных банков Южной Кореи – Shinhan Bank, Woori Bank и Nonghyup Bank, а

также многих телерадиокомпаний – KBS, YTN и MBC, в общей сложности было затронуто более 30 тыс. компьютеров. Это была наиболее мощная кибератака в истории Южной Кореи.

С 2013 г. власти США и другие международные агенты официально считают именно кибератаки угрозой номер один (ранее эту позицию занимал международный терроризм).

В силу разного рода причин все труднее становится отделить военную кибербезопасность одного государства, региона от военной кибербезопасности других государств, что неизбежно ведет к региональной военно-политической интеграции. Угроза государству может исходить, как и повод для атаки, из того, что оно вследствие политического конфликта принадлежит к другому военному блоку, экономическо-политическому союзу. Создание блоков и военно-политических союзов и нахождение государства в сфере военного или экономическо-политического влияния представляет собой естественную политико-экономическую закономерность. На данный момент все развитые страны и некоторые другие создали и развивают кибервойска, расходуя многомиллионные, миллиардные средства в этом направлении, которые могли бы быть использованы в научных, учебных и других целях.

Существующая ситуация представляет возможность нам считать, что наилучший результат в борьбе против киберугроз дает развитие сотрудничества на национальном, региональном и международном уровне. Что-то можно реализовать на данном этапе, а что-то в перспективе.

На национальном уровне считаем необходимым предпринять следующие меры:

приступить к разработке международной стратегии противодействия киберугрозам, создавав единые международно-правовые механизмы регулирования виртуального пространства;

разработать и внедрить концепцию национальной стратегии кибербезопасности, которая должна основываться на законах, предусматривающих ее реализацию в различных сферах и направлениях.

На международном уровне необходимо разработать и внедрить соглашение по предотвращению и расследованию киберагрессии – киберкодекс.

Наибольшего продвижения на пути к созданию международного киберкодекса удалось добиться летом 2015 г., когда группа правительственных экспертов ООН по международной информационной безопасности (в нее входят представители 20 стран, включая Россию, США и Китай) сформировала основу глобального пакта об электронном ненападении. В соответствии с достигнутыми договоренностями государства приняли обязательство использовать кибертехнологии исключительно

в мирных целях. Предполагается, что атакам не будут подвергнуты объекты критически важной инфраструктуры друг друга (банки, АЭС, системы управления транспортом и т. п.), перестанут вставляться вредоносные «закладки» (вредоносный софт) в производимую IT-продукцию, государства воздержатся от необоснованного обвинения друг друга в кибератаках и начнут прилагать усилия в борьбе с хакерами, осуществляющими компьютерные диверсии как с их территорий, так и через них.

Теоретически меры предусмотрены хорошие, но в случае реального физического конфликта, сопряженного с использованием информационных методов войны, маловероятно, что всего этого будут придерживаться, так как главное правило войны – любые средства хороши в борьбе для победы над противником.

Проблема современного мира заключается в существовании двойных стандартов, в разделении по региональному, экономическому, политическому, религиозному, идеологическому критериям.

Действующие агенты так и не осознали, что мир принадлежит не нам, а следующим поколениям, что человечество – это единая цивилизация и процветание, что развитие этой цивилизации невозможно, пока идет противоборство на международном и региональном уровне за превосходство и контроль в политической, военной, экономической сфере.

Наша цивилизация имеет шанс выжить и возможность процветать, если предотвратить феномены войн, в том числе сетецентрической и кибервойны, если изменить мировые векторы: план противоборства «кто сильнее» на вектор «как сделать вместе», план «кто больше» на «как лучше», план «все лучшее и большее для себя» на «как нужно и как рациональнее для всех теперь и что наименее важно для будущих поколений».

Действующие мировые агенты напоминают подростков, которые стараются показать себя и стать сильнее, богаче, умнее, нередко за счет других. Предложенные изменения векторов мировой политики касаются и принятия мер в направлении структурного изменения, повышения ответственности, авторитета международных институтов ООН, в экономическом направлении – ВТО, идеологическом и т. д.

Для преодоления и минимализации противоборства нужно в корне изменить существующие международные и региональные структуры и механизмы, элементы мирового законодательства.

Начать надо с создания нового международного института, который не имел бы привилегированных и постоянных членов с правом вето. Необходимо видоизменить формат института и состав его членов, определить месторасположение международного института на нейтраль-

ной для всех территории, придать полномочиям, распоряжениям и санкциям этой организации статус уровня международного правительства в политической, идеологической, и экономической сферах.

При любой проблеме нужно устранять не только последствия, но и причины ее порождающие.

УДК 004.9

Р.М. Юсупов, В.В. Бондуровский, М.А. Вус

ПРОЕКТ МОДЕЛЬНОГО ЗАКОНА ОДКБ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ»

Гармонизация национального законодательства по вопросам обороны, военного строительства и безопасности является одним из направлений уставной деятельности Организации Договора о коллективной безопасности (ОДКБ) и важнейшей задачей законотворческой деятельности Парламентской Ассамблеи ОДКБ (ПА ОДКБ). В рамках ОДКБ действует Соглашение о взаимной сохранности государственных секретов. Рекомендации по сближению национального законодательства по вопросам защиты государственной тайны стали одним из первых законодательных актов, принятых ПА ОДКБ.

Проект модельного закона ОДКБ «О государственной тайне» разрабатывается в соответствии с Программой деятельности ПА ОДКБ по сближению и гармонизации национального законодательства государств – членов ОДКБ на 2016–2020 гг. Головным разработчиком выступает Санкт-Петербургский институт информатики и автоматизации Российской академии наук в содружестве с Институтом национальной безопасности Республики Беларусь.

Первая рабочая версия законопроекта представлялась на Экспертно-консультативном совете при Совете ПА ОДКБ в ноябре 2016 г. По материалам работы вышел в свет ряд публикаций. Постоянная комиссия по вопросам обороны и безопасности ПА ОДКБ 20 апреля 2017 г. одобрила проведенную работу по разработке законопроекта и приняла решение направить проект модельного закона ОДКБ «О государственной тайне» в парламенты государств – членов ОДКБ для получения экспертных заключений.

Правовой институт тайны является одним из важнейших институтов и определяет: соотношение интересов личности, общества и государства, частного и публичного права; основания и пределы вмешательства государства в негосударственную сферу. Институт государственной тайны является предметом разрабатываемого для ОДКБ законопроекта. Разработчики законопроекта подчеркивают, что «государственная тайна» и «государственные секреты» – суть различные правовые категории.

В настоящее время правовая категория «государственная тайна» как объект защиты представлена в национальных законодательствах всех шести государств – членов ОДКБ; вместе с тем в тексты конституционных актов она включена только в Российской Федерации и в Республике Таджикистан (в Конституции Республики Казахстан упоминается более широкая категория «государственные секреты»).

Институт государственной тайны призван обеспечивать безопасность государства, он носит публично-правовой ограничительный характер – ограничивает основные конституционные права и свободы граждан. Целями закона о государственной тайне являются установление критериев отнесения к государственной тайне тех или иных сведений, установление критериев их засекречивания и рассекречивания, а также регулирование обращения таких сведений.

Разработчики модельного законопроекта исходят из постулата, что общественные отношения, связанные с защитой сведений, распространение которых может нанести ущерб безопасности государства, являются разновидностью конституционных правоотношений. Значимость конституционно-правовых отношений подразумевает более высокий уровень их регулирования, чем уровень регулирования обычными законами. Вследствие этого, как отмечают исследователи, логичном считается, что законодательство о государственной тайне объективно носит межотраслевой характер и вправе называться государственным (общеправовым), а не административно-правовым, хотя административное право и соответствующий административно-правовой режим играют наиболее заметную роль в регулировании обращения государственной тайны.

Представленный на заседании постоянной комиссии по вопросам обороны и безопасности ПА ОДКБ законопроект состоит из преамбулы и 7 разделов, включающих 31 статью. С учетом вышеотмеченного и в целях усиления системообразующей роли самого закона о государственной тайне и большей системности правового регулирования ее оборота предполагается необходимым придать национальным законам, разрабатываемым на основе модельного закона ОДКБ «О государственной тайне», статус конституционных. Это положение нашло отражение в преамбуле законопроекта.

В обсуждаемом законопроекте в сравнении с национальными законодательствами государств – членов ОДКБ расширен понятийный аппарат. В перечень используемых в законопроекте понятий дополнительно

включены такие правовые понятия, как «информация», «сведения, составляющие государственную тайну», «межгосударственные секреты», «режим защиты государственной тайны (режим секретности)», «информационная система в защищенном исполнении, отнесенная к государственной тайне», «национальная система защиты государственной тайны».

Использованное в данном законопроекте определение понятия «государственная тайна» представляется более точным и конкретным, чем его трактовки в действующих законах государств – членов ОДКБ. Государственная тайна определяется как «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, несанкционированное распространение которых может нанести ущерб или повлечь тяжкие последствия для национальных интересов государства и общества, их безопасности и обороноспособности, а также создать реальную угрозу безопасности либо конституционным правам, свободам граждан и их законным интересам». Предмет защиты – государственная тайна – очерчен конкретными областями государственной деятельности, сведения о которых могут или не могут быть отнесены к государственной тайне.

В представленном законопроекте расширен перечень – более подробно представлены критерии отнесения сведений к государственной тайне и их засекречивания. Помимо «хрестоматийных», которыми являются законность, обоснованность и своевременность, к таким принципам отнесены: безопасность личности, общества и государства, уважение права собственности на информацию и соотнесенность с системами защиты зарубежных государств.

Законодательные положения, касающиеся порядка отнесения сведений к государственной тайне, засекречивания сведений и их носителей, в основном коррелируют с нормами, содержащимися в национальных законах. Основная новелла обсуждаемого проекта модельного закона ОДКБ состоит в том, что для сведений, составляющих государственную тайну, в нем предусмотрены только две степени секретности и два грифа секретности для носителей таких сведений: «Совершенно секретно» и «Совершенно секретно – особой важности».

Представляется, что такая конструкция не противоречит национальным законодательствам государств – членов ОДКБ, где используется трехуровневое деление засекречиваемой информации по степеням секретности, так как нижний гриф и реквизит «Секретно» используются для обозначения сведений, составляющих служебную тайну. В Российской Федерации для сведений, отнесенных к государственной тайне, применяются все три грифа секретности, однако, как неоднократно

указывали исследователи, сведения с грифом «Секретно» по своему содержанию являются служебной тайной и должны защищаться иными правовыми нормами, нежели институт государственной тайны.

В разделе законопроекта «Владение, пользование и распоряжение сведениями, составляющими государственную тайну» прямо определено, что «государственная тайна является (объявляется) информационной собственностью государства».

Отдельной статьей законопроекта определен порядок передачи сведений, составляющих государственную тайну, другим государствам или международным организациям. Такая передача может осуществляться на основании решения президента государства при наличии международного договора.

К национальной системе защиты государственной тайны отнесен уполномоченный государственный орган по защите государственной тайны, являющийся коллегиальным органом. Он координирует деятельность органов государственной власти по защите государственной тайны при разработке и выполнении государственных программ, создании нормативных и методических документов, обеспечивающих реализацию национального законодательства о государственной тайне.

Важной новеллой законопроекта является императивное требование о введении в органы государственной власти, органы местного самоуправления, на предприятия, в учреждения и организации со значительным объемом работ, связанных с государственной тайной, должности заместителя руководителя по вопросам режима защиты государственной тайны, на которого возлагаются обязанности и права руководителя подразделения по защите государственной тайны. Подразделения по защите государственной тайны органов государственной власти, органов местного самоуправления, предприятий, учреждений и организаций комплектуются специалистами основного профиля работ, возраст которых не должен превышать предельного возраста, законодательно установленного для нахождения на государственной службе. Принятие временных работников на должности в этих подразделениях не допускается.

Отдельная статья законопроекта определяет предоставление должностным лицам и гражданам допуска к государственной тайне в связи с их избранием (назначением) на должность. К таковым относятся: президент страны, премьер-министр, депутаты парламента государства, судьи. (Адвокаты в эту категорию лиц не входят: их трудно причислить к субъектам национальной системы защиты государственной тайны.)

В тексте законопроекта нашли отражение результаты современных научных исследований и рекомендации специалистов, успешно защитивших диссертационные работы по профильной тематике. Так, на-

пример, конкретизировано содержание понятия «угроза безопасности государства», включающее основания для отказа в допуске к сведениям, составляющим государственную тайну. Такими основаниями будут являться:

попытка своими действиями, призывами осуществить изменение конституционного строя государства, нелегитимным путем изменить состав высших органов государственной власти; либо финансирование этой деятельности, а равно содействие данной деятельности в иной форме;

непосредственное участие в экстремистской деятельности, проявление социальной, расовой, национальной, религиозной нетерпимости в виде пропаганды превосходства по таким основаниям;

подтвержденные контакты с участниками террористических организаций и организованных преступных группировок;

попадание гражданина или его близких родственников в материальную зависимость от иностранных государств, иностранных организаций, отдельных граждан иностранных государств, в отношении которых имеются подтвержденные сведения, что они занимаются или содействуют разведывательной, а также иной противоправной деятельности.

В обсуждаемом законопроекте подробнее в сравнении с большинством национальных законодательств определены вопросы доступа должностного лица или гражданина к сведениям, составляющим государственную тайну.

Ответственность за обеспечение защиты государственной тайны на предприятиях, в учреждениях и организациях возлагается на их руководителей. Условия по защите сведений, составляющих государственную тайну, должны создаваться в органах государственной власти, на предприятиях, в учреждениях и организациях до получения (начала разработки) ими таких сведений. Законопроектом предусматривается государственная аттестация руководителей, ответственных за защиту сведений, составляющих государственную тайну. Состояние защиты государственной тайны в подведомственных организациях учитывается при проведении государственной аттестации их руководителей.

Отдельная статья законопроекта определяет вопросы защиты государственной тайны иностранных государств, секретов международных организаций, межгосударственных образований.

За нарушение законодательства о государственной тайне предусмотрена уголовная, административная, гражданско-правовая или дисциплинарная ответственность в соответствии с нормами действующего национального законодательства. При этом законопроект предусматривает, что вред, причиненный в результате нарушения законодательства о государственной тайне, подлежит возмещению в порядке, установленном актами национального законодательства.

УДК 004

Д.Н. Вяткин

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

В настоящее время, по оценке Международного союза электросвязи, Республика Беларусь по итоговому индексу развития информационно-коммуникационных технологий (ИКТ) поднялась с 52-го места в 2011 г. на 31-е в 2016 г. среди 175 стран. За данный период в Беларуси создан базовый комплекс электронного правительства, в который входят такие компоненты, как общегосударственная автоматизированная информационная система, система межведомственного электронного документооборота, государственная система управления открытыми ключами проверки электронной цифровой подписи, единое расчетное информационное пространство. Завершено строительство Республиканского центра обработки данных. Осуществляется информатизация здравоохранения, образования, социально-трудовой сферы. Основной задачей внедрения ИКТ в реальный сектор экономики является повышение эффективности управления полным циклом производства, создание интегрированных информационных систем, осуществляющих управление ресурсами предприятия.

Развитие информатизации в Республике Беларусь может привести к появлению новых угроз национальной безопасности в информационной сфере, с которыми уже столкнулись некоторые страны.

Примерами таких угроз являются следующие:

компьютерная атака, совершенная на металлургическое предприятие в Германии. Злоумышленникам удалось удаленно вывести из строя доменную печь, заразив вредоносным программным обеспечением офисную сеть, что привело к поломке оборудования и простою производства;

компьютерная атака на энергетическую систему «Прикарпатьеоблэнерго», специализирующуюся на передаче и снабжении электроэнергией потребителей в Западной Украине. Злоумышленникам удалось получить несанкционированный доступ к системе управления компании, в результате чего на протяжении нескольких часов в ряде городов отсутствовало энергоснабжение.

В целях организации защиты от информационных угроз важных для государства информационных систем в Республике Беларусь создан институт критически важных объектов информатизации (КВОИ). Основополагающими документами в данной сфере являются Концепция национальной безопасности Республики Беларусь и Указ Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (далее – Указ № 486).

В соответствии с Концепцией национальной безопасности Республики Беларусь одним из основных национальных интересов в информационной сфере является обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Указом № 486 утверждено Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации.

В развитие Указа № 486 утверждены следующие документы:

постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации»;

Положение о Государственном реестре критически важных объектов информатизации приказом Оперативно-аналитического центра при Президенте Республики Беларусь (далее – ОАЦ) от 20 декабря 2011 г. № 96;

Инструкция о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации приказом ОАЦ от 30 апреля 2012 г. № 42;

Технический кодекс установившейся практики ТКП 483-2013 «Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования» приказом ОАЦ от 17 июля 2013 г. № 47.

Вместе с тем необходимо отметить, что, так как имеющиеся показатели уровня ущерба, в соответствии с которыми объекты информатизации относятся к КВОИ, являются неоднозначными, владельцы КВОИ испытывают затруднения при создании системы безопасности (в соответствии с требованиями системы менеджмента информационной безопасности СТБ ISO/IEC 27001), было принято решение о необходимости внесения соответствующих изменений в Указ № 486 и нормативные правовые акты, изданные в его развитие. Завершение мероприятий по внесению изменений запланировано на 2017–2018 гг.

УДК 34.09

М.В. Губич

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Проблемы стратегического управления в сфере безопасности в последние годы становятся все более актуальными. Это совсем не случайно, поскольку XXI в. в целом характеризуется переходом мировой цивилизации из информационной стадии в стадию интеллектуального развития. Время случайных шагов в управлении проходит, наступает время системной работы, которая становится все более сложной и интеллектуально наполненной. В связи с этим в управлении происходит естественное смещение внимания с информационных потоков на процессы принятия стратегических решений, т. е. в ту сферу, где рождаются новые знания.

На сегодняшний день стратегия информационной безопасности становится неотъемлемым компонентом любого сложного действия либо проблемной ситуации, в которой задействовано много социальных субъектов. При этом стратегия информационной безопасности является компонентом стратегии более высокого уровня – безопасности в целом. В этой связи управление процессами в информационной сфере нельзя рассматривать в отрыве от общих вопросов безопасности.

Несмотря на принимаемые в нашей стране меры, направленные на реализацию политики стратегического управления в правоохранительной сфере, – разработку и реализацию Концепции национальной безопасности Республики Беларусь, Национальной стратегии устойчивого развития и ряда иных управленческих решений, в том числе связанных с реорганизацией правоохранительной системы, – до настоящего времени она не приобрела окончательных очертаний. Представляется, что в определенной мере это связано со сложностью понимания тонкостей и нюансов данного процесса и недостаточной разработанностью алгоритма применения его в практической деятельности.

В первую очередь необходимо констатировать факт того, что стратегическое управление – самая сложная разновидность управленческой деятельности, представляющая собой совокупность множества приемов, способов и методов управления, понятийных категорий, необходимых для знания и понимания, а также включающая в себя стратегический анализ, прогнозирование и планирование. Кроме того, отдельные должностные лица правоохранительных органов, в том числе

руководители, не обладают четким пониманием всех факторов, обуславливающих стратегическое управление информационной безопасностью в правоохранительной сфере.

Указанное определяет необходимость развития национальной школы стратегического управления в правоохранительной сфере, выделения в ней отдельного вектора – стратегического управления информационной безопасностью, осознания и понимания уровня его развития, определения необходимости корректировки направления развития правоохранительной стратегии в будущем.

На сегодняшний день теория стратегического управления как направление в науке и практике базируется на значительном арсенале научных разработок и концепций: теории научной организации труда и социологии управления, теории социальных явлений, общей теории систем, кибернетике, концепции стратегического моделирования и планирования, современной философии менеджмента, теории управленческих решений, теории формирования стратегии как коллективного процесса, научном управлении обществом и т. д.

Современные теоретики и практики главной составляющей стратегического управления считают стратегию, улучшение технологии принятия решений и их выполнение. Проблемой стратегического управления является его развитие в качестве самостоятельного практического направления в сфере информации, а также построение теоретической концепции в рамках научной отрасли социологии управления. В настоящее время существует лишь приблизительная рабочая модель, вокруг которой необходимо построить теоретическую конструкцию. Как предметная сфера человеческой деятельности, стратегическое управление информационной безопасностью в правоохранительной сфере представляет собой подсистему социального управления, призванную обеспечить информационную безопасность личности, общества, государства в различных сферах жизнедеятельности.

Научным сообществом исследованию стратегического управления в последние годы стало уделяться значительно больше внимания. Научная деятельность в этом направлении активизировалась, прежде всего, по причине необходимости разработки теоретических основ, вызванной цивилизационными процессами в обществе и трудностями создания эффективной правоохранительной организации, которая призвана обеспечить безопасность в информационной сфере.

Увеличение числа работ, посвященных отдельным проблемным аспектам организации и реализации стратегического управления в правоохранительной сфере, связано с осознанием практиками и теоретиками необходимости полноценного формирования данного института с учетом постоянно меняющихся вызовов и угроз общественной безопасности, противодействия закону и праву, угрожающим общественным и государственным ценностям.

Безусловно, общетеоретическая значимость работ, раскрывающих теоретические основы стратегического управления, высока. Однако следует иметь в виду необходимость комплексного изучения проблемных вопросов стратегического управления информационной безопасностью в правоохранительной системе, с учетом норм времени и происходящих событий в современном мире, чтобы полученные теоретико-правовые выводы учитывали и проблемы современности, и специфику правовой системы Республики Беларусь, а потому были применимы к ней. Необходимо понимать, что в процессе движения нашего общества решающее значение приобретает выработка научно-обоснованной стратегии осуществления глубинных социально-экономических преобразований.

Исходя из изложенного, представляется необходимым стратегическое управление информационной безопасностью в правоохранительной сфере рассматривать в качестве уникальной системы, которая должна своевременно распознавать проблемы, выдвигать научно-обоснованные стратегические цели, пути и способы их достижения; формировать представления о состоянии системы в будущем с сохранением традиционных и приобретением (созданием) новых способностей и возможностей управления, подстраивающихся под изменяющиеся и открывающиеся возможности; своевременно улавливать и распознавать возможности и угрозы, исходящие из внешней среды; вырабатывать способы изменения внешнего окружения, реформирования правоохранительной сферы, системы оперативного управления по мере увеличения собственного потенциала, выполнения стратегических задач.

УДК 342.951

А.В. Калиберов

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННЫХ ОРГАНОВ

В Послании Президента Республики Беларусь белорусскому народу и Национальному собранию в качестве одной из точек роста экономики названо повсеместное внедрение новых информационных технологий.

В системе таможенных органов функционируют 40 информационных систем и 30 баз данных по таким ключевым направлениям деятельности, как таможенный транзит, декларирование товаров и транспортных средств юридическими и физическими лицами, анализ поступления таможенных платежей, автоматизация финансово-хозяйственной деятель-

ности таможенных органов и т. д. При этом все информационные системы объединены в единую автоматизированную информационную систему таможенных органов.

Как показывает практика, применение информационных технологий в деятельности таможенных органов позволяет снизить временные затраты на оформление, обеспечить оперативность контроля, тем самым улучшить транзитную привлекательность страны.

Вместе с тем нельзя оставлять без внимания факт, что процесс информатизации таможенной сферы имеет и оборотную сторону – наряду с положительными изменениями возможны и негативные последствия, такие как использование возможностей информационных технологий в противоправных целях. Это ставит вопрос об обеспечении перехода информационной безопасности на новый уровень, тем более, с 1 января 2018 г. вступил в силу новый Таможенный кодекс Евразийского экономического союза (ТмК ЕАЭС), знаменующий собой более высокий этап не только экономической, но и информационной интеграции.

Основными причинами, которые поднимают актуальность вопросов обеспечения информационной безопасности на единой таможенной территории Евразийского экономического союза (ЕАЭС), являются:

объединение в единое информационное пространство деятельности таможенных органов государств – членов ЕАЭС, включая сопряжение их информационных систем;

динамичное развитие информационных технологий в таможенном деле, которые требуют новых адаптированных к ним подходов по обеспечению безопасности информации;

закрытость технологий и средств защиты конфиденциальной информации таможенных органов, в том числе национальной государственной тайны.

Анализ существующих подходов государств – членов ЕАЭС в решении задач по обеспечению безопасности информации показал, что они имеют в целом одни и те же взгляды на эту сферу деятельности. Так, в ТмК ЕАЭС содержится ряд норм, в которых отражены положения по регулированию деятельности таможенных органов в сфере обеспечения безопасности информации, в частности этим вопросам посвящены гл. 48 и 49.

Следует отметить, что ТмК ЕАЭС в вопросах обеспечения информационной безопасности сохранил те же подходы, которые в свое время были закреплены в действующем Таможенном кодексе Таможенного союза. Это касается, прежде всего, основополагающих положений обеспечения таможенными органами информационной безопасности:

целевое назначение получаемой таможенными органами информации (любая информация, полученная таможенными органами, используется таможенными органами исключительно для выполнения возложенных на них задач и функций);

запрет на разглашение, использование в личных целях либо передачу иным лицам получаемой таможенными органами информации;

законодательно закрепленный порядок обмена информацией между таможенными органами.

Однако надо иметь в виду, что при реализации указанных положений необходимо решить ряд вопросов, среди которых можно выделить такие, как:

1) соблюдение конституционных прав и свобод граждан в области получения и использования таможенной информации;

2) информационное обеспечение деятельности ЕАЭС, связанное с доведением до населения государств – членов ЕАЭС и международной общественности достоверной информации о его деятельности, его официальной позиции по значимым вопросам в таможенной сфере, с возможностью доступа граждан к его открытым информационным ресурсам;

3) применение и развитие современных информационных технологий собственного производства;

4) защита информационных ресурсов и информационно-телекоммуникационных технологий от угроз в сфере информационной безопасности.

Это, в свою очередь, подразумевает дальнейшее совершенствование и проведения единой политики в области обеспечения безопасности таможенных органов в условиях ЕАЭС, разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации.

УДК 004.315.5

С.Н. Касанин

НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В Указе Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделены концептуальные источники угроз национальной безопасности в информационной сфере, на решение которых и направлены наши усилия.

В Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» четко определено, в каких целях организуются и проводятся научно-исследовательские и опытно-конструкторские работы в сфере технической и криптографической защиты информации.

Приказом Государственного комитета по науке и технологиям Республики Беларусь от 30 мая 2016 г. № 93 утверждена государственная научно-техническая программа «Развитие методов и средств системы комплексной защиты информации и специальных технических средств», 2016–2020 годы.

Эти документы в области технической защиты информации гармонично дополняют и другие соответствующие нормативные правовые акты.

Анализ состояния дел в сфере технической защиты информации показывает:

1. Сложились вполне сформировавшаяся концепция и структура, основу которой составляют:

актуальная и проработанная законодательная база, где достаточно четко очерчена система взглядов на эту сферу деятельности;

весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;

большое число фирм, специализирующихся на решении вопросов технической защиты информации;

наличие значительного практического опыта и др.

2. Эффективность и соразмерность мер, предпринимаемых в Республике Беларусь, позволяет обеспечить защиту информации от утечек по техническим каналам в соответствии с требованиями действующих нормативно-методических документов и технических нормативных правовых актов.

Несмотря на все предпринятые в законодательстве меры, тем не менее, злоумышленные действия с информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Исследования в данной области свидетельствуют, что для борьбы с этой тенденцией нельзя ограничиваться отдельными и разовыми мероприятиями. Необходим системный подход, немаловажное и первостепенное значение в котором отводится непрерывному развитию и совершенствованию научно-методологических аспектов в области технической защиты информации.

Во-первых, необходима проработка и конкретизация приоритетных научных исследований в области технической защиты информации.

Анализ структуры ведущих разведок мира позволяет сделать вывод о том, что подразделения, занимающиеся добыванием информации по

техническим каналам, а также вопросами преодоления программных и аппаратных средств защиты в сфере информационных технологий, играют более важную роль, чем подразделения традиционной разведки.

Научные исследования в данной области не должны стоять на месте, требуется четкое взаимодействие и участие в этом процессе: государственных и коммерческих организаций, специальных служб, которые способны предоставить информацию специалистам данного направления.

Необходимо адекватное выявление моделей угроз информационной безопасности. Требуется дальнейшая проработка вопросов количественной оценки рисков и преимуществ, основанной на рациональных математических моделях.

Исследования и результаты работ по этому направлению зачастую являются коммерческой тайной. Однако доступные исследования, как, впрочем, и сам факт защиты информации о методиках оценки информационной безопасности, указывают на актуальность исследований в данной области.

Приоритетными научными исследованиями в области технической защиты информации, на наш взгляд, должны стать следующие направления:

1. Исследование места и роли проблем технической защиты информации в становлении современного информационного общества.

2. Разработка и научное обоснование системы мониторинга состояния технической защиты информации.

3. Совершенствование нормативно-методической базы проведения экспертизы и контроля качества защиты информации.

4. Проблемы формирования международной системы в области технической защиты информации.

5. Исследования, направленные на создание комплекса отечественных инструментальных средств проектирования средств технической защиты информации.

6. Разработка и совершенствование моделей угроз безопасности, систем и способов их реализации, определение критериев уязвимости и устойчивости систем к деструктивным воздействиям, разработка методов и средств мониторинга для выявления фактов применения несанкционированных информационных воздействий, разработка методологии и методического аппарата оценки ущерба от воздействия угроз информационной безопасности.

7. Анализ возможности использования достижений физики и техники для получения доступа к информации, обрабатываемой на современных технических средствах, в том числе исследование физических основ утечки информации от технических средств по побочным каналам, разработка проблем аналитической обработки побочных сигналов.

8. Исследование алгоритмических и технологических особенностей новейших зарубежных и отечественных технических средств обработки информации.

9. Разработка методологии оценивания защищенности, комплексных методов и средств защиты технических средств обработки информации от физико-технических методов несанкционированного доступа, совершенствование соответствующей нормативной базы.

10. Сравнительный анализ тенденций развития физико-технических проблем защиты информации в стране и за рубежом.

11. Разработка и научное обоснование моделей угроз и стратегий защиты объектов от технических разведок.

12. Разработка методов и средств противодействия техническим разведкам с учетом эффективности функционирования.

13. Разработка методов и средств контроля состояния и достаточности принимаемых мер по противодействию техническим разведкам на объектах защиты.

Во-вторых, значимой для развития исследований в области технической защиты информации остается проблема хронического недофинансирования.

С целью минимизации пробелов в данном направлении, целесообразно разработать меры по стимулированию:

публикационной и патентной активности исследователей;

привлечения молодежи в исследовательскую деятельность;

привлечения бизнес-организациями молодых ученых к выполнению научных исследований в области информационной безопасности.

Одним из ключевых условий научного и технологического развития в области технической защиты информации должно стать участие крупных компаний. Поддержка научной деятельности – важнейший фактор сохранения коммерческой тайны и удержания сферы влияния на отечественном и мировом рынках. Кроме того, обеспечивается устойчивое финансирование научных организаций, которое позволяет формировать новые знания.

В-третьих, необходимо совершенствование кадровой политики в сфере технической защиты информации.

Существенное противодействие росту компьютерных преступлений может оказать грамотная политика в подборе и подготовке национальных кадров в сфере информационной безопасности.

Проведенные социологические исследования студентов и специалистов, работающих в области защиты информации, позволяют сделать следующие выводы:

1. Дерзость совершения компьютерных правонарушений у молодежи вызывает восхищение, желание самоутвердиться, показать себя с

лучшей стороны и привлечь к себе внимание. Среди других факторов, определяющих желание осуществлять компьютерные правонарушения, можно выделить желание заработать.

2. Многие абитуриенты, поступая на специальности, связанные с защитой информации, преследуют корыстную цель – научиться методам совершения компьютерных преступлений.

3. Подавляющее большинство студентов, обучающихся на специальностях, связанных с вычислительной техникой, очень слабо знают нормативные правовые документы по защите информации.

Анализ информации позволил выявить ряд условий, реализация которых даст возможность обеспечить качественную подготовку специалистов в области технической защиты информации.

Для выработки рекомендаций по совершенствованию подготовки специалистов в области технической защиты информации необходимо выделить три направления: учебно-воспитательное, учебно-методическое, организационно-административное.

Немаловажной задачей становится повышение квалификации специалистов в области защиты информации.

Приоритетным направлением должна быть подготовка кадров высшей научной квалификации, которые проводили бы исследования в области технической защиты информации.

УДК 343.985

А.А. Ковальчук

КЛАССИФИКАЦИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

В настоящее время жизнь людей буквально невообразима без привычных программно-технических средств, например компьютеров, которые позволяют автоматизировать сложнейшие процессы и существенно расширить человеческие возможности. Однако далеко не всегда достижения науки и техники используются во благо. Нередко отдельные представители общества, руководствуясь корыстными и иными деструктивными мотивами, совершают различного рода противоправные деяния.

На современном этапе широкое распространение получили хищения, совершаемые с использованием компьютерной техники. Впервые подобные преступления были выявлены на территории Республики Беларусь на рубеже прошлого и нынешнего веков и основывались на незаконном использовании банковских платежных карточек (БПК). В дальнейшем с развитием информационных технологий происходил процесс эволюции способов совершения хищений.

Изучение оперативно-розыскной практики подразделений по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь, а также анализ уголовных дел, возбуждавшихся по ст. 212 Уголовного кодекса Республики Беларусь «Хищение путем использования компьютерной техники», позволили привести соответствующую классификацию после упорядочения и систематизации полученных сведений.

По мнению автора, все способы хищений, совершаемых с использованием компьютерной техники, могут быть разделены на две группы:

связанные с осуществлением прямого доступа к счету без нарушения системы защиты (совершаются лицами, имеющими в силу служебного положения такой доступ);

связанные с осуществлением опосредованного несанкционированного доступа к счету.

В свою очередь, во второй группе выделяются способы хищения:

неквалифицированные (характерные особенности: носят, как правило, случайный характер; преступник не имеет четкого плана по совершению преступного деяния, в том числе относительно завладения БПК или ее реквизитами, и дальнейшему распоряжению похищенным имуществом или сведениями);

квалифицированные (характерные особенности: чаще всего совершаются в составе организованных групп, участники которых могут быть незнакомы друг с другом; общение между участниками происходит посредством интернет-форумов, различных приложений, предназначенных для обмена сообщениями, с использованием возможностей шифрования каналов передачи данных; совершаются в соответствии с заранее разработанными схемами; участники выполняют определенные функции и решают конкретные задачи).

Квалифицированные способы делятся на:

реальный кардинг (основан на изготовлении дубликатов БПК с использованием специального оборудования);

вещевой кардинг (связан с целенаправленным неправомерным завладением реквизитами БПК, необходимыми для осуществления денежных переводов либо онлайн-платежей с целью последующего хищения имущества в различных предприятиях интернет-торговли);

хищения, основанные на использовании вредоносного программного обеспечения, позволяющего оказывать влияние на функционирование банковских технических средств.

Подводя итог, следует отметить, что высокие темпы информатизации в нашей стране оказали существенное влияние на стремительность эволюционных процессов в сфере хищений, совершаемых с использованием компьютерной техники. В течение относительно небольшого периода времени спектр таких преступлений значительно расширился в направлении от довольно простых и заурядных до высокотехнологичных. Выявленные тенденции предоставляют возможность сделать вывод о том, что приоритетное направление в сфере рассматриваемой противоправной деятельности заняли хищения, совершаемые с использованием реквизитов БПК. Этому способствовало удобство эксплуатации глобальной сети Интернет с практически безграничным числом возможностей, низкий уровень конкуренции, позволяющий людям с невысокой технической квалификацией получать существенные доходы по сравнению со средней в стране заработной платой, многообразие обучающей литературы и простота внедрения в преступную среду на условиях анонимности, а также беспечность людей во всем мире по отношению к своему имуществу и вопросам информационной безопасности.

УДК 355.4

О.О. Лемешевский

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ФАКУЛЬТЕТЕ ВНУТРЕННИХ ВОЙСК МВД РЕСПУБЛИКИ БЕЛАРУСЬ

В XXI веке – веке информации и новых, доселе неизвестных, технологий – трудно найти какую-либо область жизни общества, где бы ни использовались современные способы обработки и передачи информации. Однако подобные реалии не только развивают наше общество, но и создают условия, в немалой степени облегчающие осуществление преступных планов. Организованные преступные группы максимально используют возможности новых информационных технологий как для подготовки и совершения преступлений, так и для их сокрытия.

Еще 20–25 лет назад в Республике Беларусь этой проблемы, казалось, вообще не существовало. Не было ни самих киберпреступников, ни соответствующей законодательной базы. С приобретением независимости наша страна получила доступ к технологическим новшествам. Произошел своеобразный обмен: из бывшего СССР «утекали мозги», взамен наши знания обогащались тем бесценным высокотехнологическим опытом стран рыночной экономики, которого мы были лишены. Но к новым технологиям прилагался достаточно разнообразный «набор» совершенно новых, неизвестных ранее, преступлений. Кроме преступных деяний, где компьютерная техника была лишь средством или объектом преступления, появились совершенно специфические преступления, где объектом преступления стала информация, размещен-

ная и на персональных компьютерах, и на компьютерах, соединенных как в локальную, так и в глобальные информационные сети. Эти виды преступлений вошли в отдельный раздел Уголовного кодекса Республики Беларусь «Преступления против информационной безопасности».

Компьютерная преступность стала настоящим бичом экономики развитых государств. Так, например, 90 % фирм и организаций в Великобритании в разное время становились объектами электронного пиратства или находились под его угрозой, в Нидерландах жертвами компьютерной преступности стали 20 % различного рода предприятий. В ФРГ с использованием компьютеров ежегодно похищается 4 млрд евро, а во Франции – 1 млрд евро.

Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Известно, рассматриваемые правонарушения имеют очень высокую латентность, которая по различным данным составляет 85–90 %. Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений, в большинстве случаев стали:

1) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать ЭВМ в качестве орудия совершения преступления;

2) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

3) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

4) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации;

5) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности;

6) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Для эффективной защиты от компьютерных преступлений и утечки служебной информации на факультете внутренних войск был выполнен ряд мероприятий:

1) просмотрена вся документация;

2) определены возможные каналы утечки информации;

3) ликвидированы слабые звенья в защите;

4) определены категории допуска для лиц, имеющих право доступа;

5) определена дисциплинарная ответственность за сохранность и санкционированность доступа к имеющимся информационным ресурсам;

6) организован периодический системный контроль качества защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением специалистов;

7) проведена классификация информации в соответствии с ее важностью;

8) определено должностное лицо, отвечающее за режим секретности и конфиденциальности информации;

9) обновлено защитное программное обеспечение.

Таким образом, на факультете внутренних войск на высоком уровне осуществляется защита и предупреждение утечек служебной информации, защита от возможности компьютерной преступности, совершенствование программного обеспечения.

УДК 343

В.Ю. Арчаков, О.С. Макаров

ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Заканчивается второе десятилетие XXI в. Наряду с такими вызовами человечеству, как потепление климата, истощение природных ресурсов, мы рассматриваем угрозы, вызванные глобальным процессом информатизации нашей цивилизации.

В связи с тем, что современное общество переместило свои социальные отношения в информационную среду, где традиционные, выработанные тысячелетиями регуляторы безопасности не действуют, а адекватные системы их защиты в информационной сфере пока не разработаны, социум претерпевает негативные последствия реализации информационных угроз: растет информационная преступность, на личность оказывается деструктивное информационное воздействие, развивается кризис тайн и т. д.

В обозначенных условиях рельефно проявляется дилемма: обозримый путь общественного развития пролегает через процессы информа-

тизации, однако информатизация общества порождает геометрическое возрастание угроз национальной безопасности.

Информационная сфера становится доминантой в структуре национальной и международной безопасности. Информация выступает сегодня как предмет деятельности и объект защиты, как источник опасности и как оценочный индикатор безопасности общества и всех его институтов.

По мере развития социума информация превратилась в высокоэффективное оружие, с помощью которого решается широкий спектр задач в экономической, политической и в военной сферах. Возникшие глобальные информационные поля оказались способными воздействовать на людей, не взирая на государственные границы, создавать возможность манипуляции сознанием в планетарном масштабе. Факты свидетельствуют, что духовная сфера – сознание и ценностные ориентации людей – оказалась наиболее уязвимой областью национальной безопасности. Распространение посредством СМИ, а также социальных сетей недостоверной или умышленно искаженной информации способно спровоцировать не только массовые беспорядки в обществе, но и обвал экономической и финансовой систем государства.

Основным угрозообразующим для информационной безопасности фактором во втором десятилетии XXI в. стал нарастающий дисбаланс между прорывным насыщением потребностей социума технологиями информатизации и ощутимым отставанием в организации использования информационного ресурса общества. Цифровая эпоха сделала первые шаги в технологическом направлении, но испытывает сложности в синхронизации интересов акторов и обеспечении их безопасности.

Еще одним побочным эффектом технологического прогресса становятся негативные факторы социального, культурного, экономического планов (киберпреступность, кибертерроризм, информационные войны и др.), питательной средой которых среди прочих выступает информационное, цифровое неравенство, правовая неопределенность и безнаказанность. Это затрудняет определение правовых, политических, этических параметров отношений как внутри государств, так и в их сообществах, а также в решении проблем общемирового значения.

Для продолжения развития информационного общества необходимо обеспечить эффективное противодействие угрозам использования современных информационных технологий для нарушения мира и безопасности, совершения преступлений, подготовки и осуществления террористических актов, распространения террористической идеологии и практики разрешения противоречий общественного развития. Данная работа в силу трансграничности угроз информационной безопасности

должна проводиться на национальном уровне и с позиций международного взаимодействия.

Представляется, что решение указанных проблем находится не в технической, а в социальной плоскости, а значит, предполагает осознание обществом новых, обусловленных процессами информатизации условий социальной жизни и выработку определенных правил безопасной межличностной, общественной, государственной и межгосударственной коммуникации с последующим их юридическим закреплением и формированием соответствующего механизма защиты складывающихся отношений.

За последние 15 лет произошло значительное расширение сферы информационной безопасности и увеличение методов ее обеспечения, что связано с пониманием недостаточности методов защиты и охраны информационных ресурсов. Границы информационной безопасности позволяют информации быть открытой и доступной и влиять на все слои и группы пользователей.

В этих условиях особую роль в обеспечении информационной безопасности призвано исполнить право, именно взаимодействие в рамках правовых систем разных государств и отраслей законодательства. Нормативно-правовая основа необходима для поддержания стратегической стабильности и развития партнерства во всех областях жизни общества и одновременно для создания условий формирования безопасного информационного общества.

В то же время в области современного правового регулирования сферы информационного взаимодействия складывается ситуация напряжения, что предопределяет поиск решений по оздоровлению информационной среды, особенно интернет-среды, обеспечению информационной безопасности.

В силу трансграничного характера информационных отношений на первый план правового обеспечения информационной безопасности выступает международное право.

Критический взгляд на современное состояние правового обеспечения информационной безопасности на международном уровне позволяет сделать вывод о его концептуальной неопределенности. Правовое регулирование в данной сфере очевидно поверхностно, так как постоянно лавирует, решая сиюминутные политические задачи, «залатывает» социальные пробелы, вызванные скачками информатизации, и запоздало реагирует на информационные угрозы правам и интересам субъектов отношений. Локомотивом нормативного урегулирования отношений в области обеспечения международной информационной безопасности сегодня выступают документы политического характера (различные стратегии, доктрины, правила поведения, планы и т. п.).

В результате у правоведов формируются очевидные фобии нормотворчества, обуславливающие появление правовых лакун в регулировании информационной безопасности на национальном и международном уровнях.

Так, например, научное сообщество и законодатели большинства стран определились, что термины «кибербезопасность» и «информационная безопасность» не тождественны, однако в ряде нормативных актов они сосуществуют, в других конкурируют, в третьих эквивалентны друг другу.

Схожая ситуация в отношении понятий «информационная война» и «информационное оружие». Их введение (после долгих научных споров) в соглашение Шанхайской организации сотрудничества (ШОС) презентовалось как прорыв в правотворчестве. Но сегодня ряд ученых считает данные термины неудачными, не отвечающим и международной трактовке базового понятия «война». Наметилась тенденция к вытеснению их не милитаристическим понятием «деструктивное информационное воздействие».

Также представляет интерес подмена в юридически значимых документах стволового понятия «киберпреступления» политизированным термином «киберугрозы».

Кроме этого, в нормативных актах в области обеспечения информационной безопасности начал подвергаться ревизии неоспоримый примат основы основ европейской правовой модели – свобода информации. В теории, а затем в международных документах его теснит принцип баланса информационных свобод с интересами обеспечения информационной безопасности.

При этом просматривается сдержанность юристов в формулировании запретов в области обеспечения информационной безопасности (например, запрета на распространение заведомо недостоверной информации, запрета на использование информационных технологий в ущерб безопасности других лиц и т. д.).

Правовое регулирование общественных отношений в целях обеспечения информационной безопасности уверенно опирается на сформировавшиеся институты ответственности за киберпреступления и посягательства на всякого рода тайны. Остальные правила поведения формулируются в политическом ключе как «озабоченность», «порицание», «неприятие».

Складывается впечатление, что в области обеспечения международной информационной безопасности государства стараются избегать жестких правовых ограничений, оставляя правовой недосказанностью «серые зоны» для политических решений.

Обобщение современной практики правового обеспечения информационной безопасности в глобальном масштабе позволяет выделить две основные конкурирующие правовые модели, которые, исходя из географии применения, условно можно назвать европейской и евразийской.

Европейская модель основывается на конвенции Совета Европы о киберпреступности, принятой в 2001 г. в Будапеште. Она достаточно эффективно используется в ряде государств и преимущественно охватывает области деятельности, непосредственно связанные с использованием технических средств сбора, обработки, защиты, распространения и использования информации. Поэтому в рамках данной платформы оперируют такими понятиями, как «кибербезопасность», «киберугрозы», «кибератаки».

К недостаткам европейской модели, на наш взгляд, относится принципиальное отсутствие упоминаний о деструктивном информационном воздействии на сознание населения, а также умалчивание о современных инструментах совершения киберпреступлений (ботнеты, спам, фишинг и др.). Против Будапештской конвенции выступают Китай, Индия, Южная Африка, Бразилия, а также не подписавшая данный документ Россия.

Евразийская модель, в отличие от европейской, строится на более широкой трактовке угроз, и вопросы чистой кибербезопасности рассматриваются наряду и в тесной взаимосвязи с общими проблемами всей сферы массовых коммуникаций, в том числе с распространением противоправного либо нежелательного контента. Поэтому речь идет именно об информационной безопасности, а не о безопасности информации или безопасности компьютерных систем и сетей.

Евразийская модель нашла отражение в Соглашении между правительствами государств – членов ШОС в области обеспечения международной информационной безопасности, в документах ОДКБ, в Соглашении о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности и в других документах СНГ.

Антагонизм вышеназванных моделей отчетливо указывает на то, что в ближайшем обозримом будущем не следует рассчитывать на общее в глобальном смысле понимание и согласование правовых норм в сфере международной информационной безопасности. Необходимо незамедлительно совершенствовать механизмы регионального сотрудничества, выстраивая жизнеспособную систему международной информационной безопасности в рамках существующих организаций, объединений и союзов.

Сегодня на повестке для регионального взаимодействия в области обеспечения международной информационной безопасности находятся проекты Соглашения о сотрудничестве государств – членов Организа-

ции Договора о коллективной безопасности в области обеспечения информационной безопасности и Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств. Полагаем, принятие данных актов повысит эффективность обеспечения международной информационной безопасности.

УДК 004.42

С.С. Мишук

СИСТЕМА ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ЭЛЕМЕНТ НООСФЕРЫ

Возникновение и функционирование информационного общества, ядром которого является система инфокоммуникационных технологий, стало объективной реальностью XXI в. Различные аспекты данного явления постоянно описываются в современной литературе. Однако исследованию его в качестве необходимого и закономерного этапа эволюции как человеческого общества, так и планеты Земля в целом уделяется, на наш взгляд, недостаточно внимания. Между тем использование имеющихся в науке подходов к изучению явлений подобного типа позволило бы глубже понять специфику этого периода общепланетарной эволюции. Одной из теорий, формирующих методологическую основу анализа данной проблемы, безусловно, является учение академика В.И. Вернадского о ноосфере.

На наш взгляд, инфокоммуникационные технологии превратились на современном этапе в один из важнейших компонентов ноосферы как планетарной оболочки. Для корректного анализа их роли и значения именно в данном качестве необходимо зафиксировать, по крайней мере, две содержательных трактовки понятия «ноосфера» в трудах В.И. Вернадского.

Во-первых, ноосфера трактовалась им как определенный этап в планетарном развитии Земли.

Во-вторых, ноосфера трактовалась и как этап именно разумного преобразования той среды, в которой живет человек. В.И. Вернадский подчеркивал, что наличие сознания как необходимого компонента предметно-преобразовательной деятельности человека не означает автоматически, что данная деятельность осуществляется разумно в подлинном смысле слова. Активность человека может приводить и к нежелательным, даже опасным для него самого последствиям.

Сам факт возникновения ноосферы как принципиально новой планетарной оболочки означает также известный отрыв человека от процессов собственно земной эволюции. Именно на данном этапе человечество оказывается в состоянии преодолеть земное притяжение и покинуть пределы среды своего возникновения. Иными словами, человеческая деятельность превращается в фактор не только земной, но и космической эволюции. В подобных условиях значение именно разумности человека в самом широком смысле слова возрастает многократно. И в этом смысле ноосфера (именно как сфера разума, как разумно устроенная сфера обитания человечества) должна пониматься не только как одна из планетарных оболочек и этап земной эволюции, но и как цель будущего развития человечества. И данная цель может быть достижима при условии понимания человека уже не как чисто планетарного, земного фактора, но и как силы, которая выходит за рамки отдельной планеты и в бесконечном времени становится значимой для всей Вселенной.

В своих трудах В.И. Вернадский достаточно полно систематизировал факторы, которые необходимы для формирования и успешного функционирования и развития ноосферы. Постараемся кратко проанализировать те из них, которые непосредственно связаны с функционированием системы инфокоммуникационных технологий, – «резкое преобразование средств связи и обмена информацией» и «свобода научной мысли и научного поиска от давления религиозных, философских и политических построений».

Возникновение в конце XX в. и функционирование в современных условиях информационного общества со всей очевидностью демонстрирует значение инфокоммуникационных технологий как системообразующего элемента. Они выступают одним из важнейших факторов устойчивого существования и дальнейшего развития человеческой цивилизации.

Для изучения действительной значимости инфокоммуникационных технологий следует рассмотреть их функционирование в структуре ноосферы как уже достаточно сформированной планетарной оболочки. Раз возникнув, ноосфера начинает эволюционировать как самостоятельная система. Присущие именно ей законы приводят к необходимому появлению и последующему отбору таких механизмов, объективная потребность в которых возникает на определенном этапе развития. Причем наиболее значимые механизмы появляются чаще всего в тех структурных элементах ноосферы, которые являются сущностными для нее, то есть связанными в первую очередь с функционированием разума и знания. Возникновение подобных инновационных по своей природе элементов стимулирует прогресс человеческого общества в масштабах планеты не только опосредовано. Они непосредственно

включаются в эволюционное развитие всей Земли, превращаются в одни из важнейших внутренних компонентов этого процесса. Можно сделать вывод о том, что ноосфера для обеспечения постоянного устойчивого функционирования вырабатывает внутренние механизмы саморегулирования и самосохранения.

Данное общетеоретическое положение прекрасно иллюстрируется на примере возникновения и развития глобальной телекоммуникационной компьютерной сети Интернет.

Итак, можно сделать вывод о том, что в рамках ноосферы, как реализация ее внутренних закономерностей, возникает компонент, объективно создающий возможность организации управления в планетарном масштабе, регулирования процессов в пределах всей Земли. В то же время сам этот элемент достаточно быстро показывает, что для его полноценного функционирования также требуются соответствующие по масштабам и полномочиям механизмы управления. Таким образом, постепенное вызревание в рамках ноосферы глобальных проблем достаточно быстро порождает (на основе реализации ее собственных, именно ей присущих внутренних законов) механизм, дающий возможность их разрешения. А сформировавшись, сам этот механизм в свою очередь требует соответствующих ему по масштабу и возможностям глобальных инструментов, четко демонстрирует их объективную необходимость. Все это опять-таки стимулирует дальнейшее развитие процессов общепланетарной эволюции.

Можно сказать, что в настоящее время информационное общество как новый этап в развитии человечества (и ноосферы) вступило в очередную стадию – сформировалась система информационно-коммуникационных (инфокоммуникационных) технологий как необходимый, «собственно познавательный и разумный» структурный компонент современной цивилизации. Они представляют собою глобальную по масштабам систему получения (производства), обработки, хранения, передачи, распределения, обмена и потребления (использования) информации. И в ней постепенно начинают проявляться качества, не наблюдавшиеся у ранее создаваемых человечеством искусственных систем.

Во-первых, возникновение системы информационно-коммуникационных технологий является именно необходимым и закономерным этапом в развитии ноосферы. Новая «разумная» оболочка Земли объективно требовала наличия всеохватывающей системы, которая выполняла бы функцию носителя общечеловеческого знания.

Без сформировавшихся на современном этапе информационно-коммуникационных технологий ноосфера не может функционировать целостно. Как сама ноосфера генетически следует из развития биосферы, так и сфера инфокоммуникационных технологий логически завер-

шает формирование ноосферы. С появлением сферы инфокоммуникационных технологий компонент «ноос» (разум) окончательно формируется как структурный элемент ноосферы, как некая нервная система, действительно, всей человеческой цивилизации. Он начинает реально функционировать не только как совокупность «персонифицированных разумов». Инфокоммуникационные технологии позволяют каждому индивиду, независимо от места нахождения, времени, уровня образования и т. д., непосредственно, активно, в режиме реального времени включаться в общепланетарный мыслительный процесс не только потенциально, но и реально. (Очевидно, что при осуществление данного процесса не все результаты являются, бесспорно, положительными. Здесь имеются и негативные стороны.) Возникает подлинно обобществленный разум, одновременно охватывающий всю поверхность Земли, одновременно вовлекающий сотни миллионов и миллиарды людей в свое функционирование. Он превращается в, действительно, «планетарную сферу» по своим масштабам, по уровням присутствия (от литосферы до космоса), по глубине воздействия на процессы, происходящие на Земле, и по скорости передачи этих воздействий.

В-вторых, информационно-коммуникационные технологии являются, на наш взгляд, самым динамичным компонентом ноосферы. Как функционирование самого человеческого общества (по сравнению с остальными компонентами природы) наименее ограничено внешними факторами, так и функционирование человеческого разума самое быстрое, наиболее динамичное, наименее ограниченное внешними факторами.

В-третьих, система информационных технологий является эволюционирующим элементом ноосферы. Закономерности, которыми ноосфера обладает, приводят к появлению новых механизмов, необходимых для ее функционирования на определенном этапе. Наблюдаются процессы, во многом подобные эволюционному отбору в живой природе. В этом смысле инфокоммуникационные технологии, как нервная система ноосферы, выступают в первую очередь активным регулятором протекающих трансформаций. Помимо этого, они также выполняют функцию инициации соответствующих преобразований во всех сферах человеческого общества.

Таким образом, инфокоммуникационные технологии в современных условиях все более демонстрируют внутренне присущие им системообразующие свойства и активно распространяют их на остальные структурные компоненты жизни человеческого общества. На нынешнем этапе функционирования человеческой цивилизации система данных технологий уже перестает быть вспомогательной структурой (пусть и очень важной), обеспечивающей просто передачу информации внутри ноосферы. Информационно-коммуникационные технологии к

началу XXI в. достигли такого уровня развития, что сами начинают задавать новые параметры системной организации остальных структурных компонентов человеческой цивилизации – экономических, социальных, политических, духовных. В результате происходят трансформации данных элементов в соответствии с теми нормами, процедурами и правилами построения, которые определяются инфокоммуникационной сферой.

УДК 004.42

И.Д. Пацкевич, Р.В. Кислинский

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В КИБЕРНЕТИЧЕСКОМ ПРОСТРАНСТВЕ

Современный этап развития общества характеризуется бурным развитием и внедрением средств связи, вычислительной техники и новых информационных технологий практически во все сферы человеческой деятельности. Все это привело к формированию так называемого кибернетического пространства, впитавшего в себя не только общечеловеческие культурные ценности, но, к сожалению, и все присущие обществу пороки.

Так, пользователь информационной сети может свободно получить рецепты производства наркотиков, способы изготовления из доступных материалов самодельных взрывных устройств, переписать на свой компьютер порнографические изображения или мультимедийные журналы сомнительного содержания, получить полные тексты доктрин идейных руководителей нацизма и мирового терроризма, принять участие в электронной конференции хакеров, на которой обсуждаются вопросы несанкционированного проникновения в автоматизированные системы органов государственного управления, военных структур и т. п.

Основной целью интернет-преступников является обман пользователей глобальной паутины и кража конфиденциальной информации, которая используется после в личных целях преступника. В результате такой деятельности миллионы людей во всем мире несут значительные убытки каждый год.

Почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры, направленные на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению.

К группе мер предупреждения компьютерных преступлений, прежде всего, относятся нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере. Первым шагом в этом направлении можно считать Закон Республики Беларусь «О повышении компьютерной безопасности», а также Закон «Об информатизации». В ноябре 2010 г. в нашей стране была принята Концепция национальной безопасности Республики Беларусь. В ней сказано, что мир вступил в стадию кардинальных экономических, общественных, военно-политических и иных изменений, характеризующихся высокой интенсивностью и динамичностью. Предпринимаются попытки формирования и навязывания идеологии глобализма, призванной подменить или исказить традиционные духовно-нравственные ценности народов.

Но одних мер профилактики недостаточно. В целях обеспечения информационной безопасности в Республике Беларусь были созданы специальные органы по борьбе с киберпреступностью. Так, 21 апреля 2008 г. создан Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ). ОАЦ является государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь, или иные сведения, охраняемые в соответствии с законодательством от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

Как дополнительные меры борьбы с преступностью в киберпространстве, в стране созданы отделы по раскрытию преступлений в сфере высоких технологий. Это современные, хорошо оснащенные, боеспособные подразделения, которые занимаются раскрытием и профилактикой преступлений против информационной безопасности, преступлений в сфере телекоммуникаций; противодействием хакерам, кардерам, а также распространению детской порнографии, кражам финансовых средств частных лиц и организаций путем использования компьютерной техники; оперативной и технической поддержкой служб правоохранительных органов при раскрытии тяжких и особо тяжких преступлений. Подразделения оснащены самыми современными техническими средствами раскрытия интернет-преступлений – как универсальным, так и специальным программным обеспечением. Универсальные программы общего назначения (информационно-поисковые системы, редакторы, электронные таблицы и т. п.) не только повышают производительность труда и эффективность работы по выявлению, раскрытию и расследованию преступлений, но и поднимают их на качественно новый уровень. Специализированные программы могут быть ориентированы на непосредственное их применение при осуще-

ствлении оперативно-розыскных мероприятий в направлении борьбы с информационной (в том числе компьютерной) преступностью.

В настоящее время существует программы, которые позволяют:

контролировать процесс попыток взлома компьютерной системы или сети;

определять индивидуальный почерк работы программиста и идентификационные характеристики разработанных им программ;

определять перечень электронных адресов и сайтов интернета, с которыми работал пользователь;

негласно регистрировать перечень программ, с которыми работает пользователь;

определять путь, а в некоторых случаях и конкретный адрес исходящей угрозы для компьютерных систем;

осуществлять негласный контроль над программистом, определяя характер разрабатываемых продуктов;

обнаруживать латентную и закодированную информации в компьютерной системе;

проводить идентификацию компьютерных систем по следам применения на различных материальных носителях информации;

осуществлять исследование следов деятельности оператора в целях его идентификации;

осуществлять диагностику устройств и систем телекоммуникаций на возможность осуществления несанкционированного доступа к ним;

исследовать материальные носители с целью поиска заданной информации;

осуществлять исследование компьютерных технологий для установления возможности решения конкретных преступных задач (крекинг, хакинг, фрикинг и т. п.);

исследовать программы ЭВМ и базы данных с целью определения их возможного предназначения для преступных действий (при наличии программных закладок, подпрограмм класса «троянский конь» и т. п.).

Поисковые программные средства могут найти широкое применение в оперативно-розыскной деятельности (непроцессуальная форма), в том числе и до возбуждения уголовного дела. Факт обнаружения объектов (программы закладок, программное обеспечение для изготовления вирусов или для осуществления взлома компьютерных сетей и т. п.) может послужить основанием для возбуждения дела и производства расследования. В процессуальной форме поисковые программные средства могут найти применение при проведении следственных действий, таких как следственный осмотр (все его виды), выемка предметов, документов и электронной почтовой корреспонденции, следственный эксперимент, выполняемый с целью опытной проверки показаний.

В оперативно-розыскной деятельности при расследовании компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и преступного группового поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Полезную информацию могут дать и анализ платежей клиентов за телефонные услуги. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения определенных криминогенных контингентов. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм оперативно-розыскной деятельности (поиск, профилактика, разработка). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные технологии.

Таким образом, мы видим, что почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать не только различные профилактические меры, но и активные меры по борьбе с данными преступлениями. Профилактические меры следует воспринимать как деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению, а в целях борьбы следует создавать специальные подразделения, которые будут заниматься раскрытием интернет-преступлений. Для этого сотрудникам правоохранительных органов необходимо получить знания по основам учебных дисциплин в области кибернетики и вычислительной техники.

УДК 006.07

С.В. Пашковский

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Начав обсуждение вопроса о совершенствовании законодательства в области информационной безопасности, необходимо отметить, что в рамках текущего доклада под информационной безопасностью пони-

мается состояние, достигаемое применением организационных, правовых и технических мер по защите информации, а также систематическим повышением уровня подготовки специалистов, реализующих названные меры. Изменение каждого из этих элементов неизбежно оказывает влияние на остальные. Так, стремительное развитие сферы информационно-коммуникационных технологий требует своевременного редактирования отдельных нормативных правовых актов и технических правовых актов. Учитывая указанное обстоятельство, ОАЦ осуществляет систематическую работу по совершенствованию законодательства в сфере защиты информации.

В ближайшее время развитие названной отрасли законодательства будет определяться тремя основными факторами.

Во-первых, подготовкой и принятием Закона Республики Беларусь «О персональных данных», который позволит однозначно определить понятийный аппарат, категории персональных данных, принципы работы и основы правового регулирования порядка обработки и защиты персональных данных, права субъектов персональных данных и обязанности операторов при их обработке, порядок трансграничной передачи персональных данных, а также установить контроль и ответственность в сфере работы с персональными данными.

Вторым фактором будет выступать принятие новой редакции стандарта Республики Беларусь 34.101.30 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация». В основе новой классификации объектов информатизации лежат такие признаки, как вид информации в зависимости от категории доступа, наличие подключения к открытым каналам передачи данных, а также конкретный тип информации, распространение и (или) предоставление которой ограничено. Избранный подход формирует множество классов, что позволяет предъявлять более дифференцированные требования по защите информации существующих и перспективных информационных систем.

Третьим фактором является разработка серии стандартов на специализированные средства защиты информации (DLP, SIEM, IPS/IDS), принятие которых позволит существенно снизить стоимость и время прохождения процедуры подтверждения соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР2013/027/BY), так как исключит необходимость разработки и оценки заданий по безопасности.

УДК 342.951; 351.9; 34:002

Д.В. Перевалов

ПРОБЛЕМНЫЕ ВОПРОСЫ ФУНКЦИОНИРОВАНИЯ СПЕЦИАЛЬНОГО КОМПЛЕКСНОГО АДМИНИСТРАТИВНО-ПРАВОВОГО РЕЖИМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Должное обеспечение безопасности критически важных объектов информатизации (КВОИ) в современных условиях может быть реализовано только в рамках соответствующего специального комплексного административно-правового режима (СКАПР). Формирование такого административно-правового режима обусловлено следующими обстоятельствами.

Во-первых, СКАПР позволяет построить эффективную охрану и защиту соответствующих объектов от различного рода угроз. Во-вторых, он обеспечивает необходимый уровень охраны и защиты соответствующих объектов, что возможно только при наличии должного государственно-управленческого воздействия: общественные отношения, возникающие, изменяющиеся и прекращающиеся в процессе обеспечения безопасности КВОИ, носят преимущественно административно-правовой характер. В-третьих, СКАПР обеспечивает безопасности КВОИ комплексно, так как при его функционировании реализуются нормы сразу нескольких отраслей права – конституционного, международного, административного, уголовного, трудового, а также права технического регулирования; требования и правила данного режима затрагивают различные по характеру права и обязанности субъектов режимного регулирования.

Вместе с тем для СКАПР при обеспечении безопасности КВОИ определяющими являются нормы административного права, поскольку складывающиеся отношения, хоть и относятся к другим правовым отраслям, но в рамках очерчиваемой СКАПР сферы облекаются в административно-правовую форму и становятся объектом административно-правового регулирования.

Однако в виде СКАПР система обеспечения безопасности КВОИ в настоящее время урегулирована нормативно не в должной степени. В то же время в связи с увеличением числа и изменением характера информационных угроз, возрастанием значения КВОИ в жизнедеятельности государства и общества все более актуальной становится потребность в более широком правовом регулировании данной сферы.

Исходя из сложившихся подходов к сущности и содержанию административно-правовых режимов и основываясь на результатах прове-

денных исследований, можно определить, что содержание СКАПР при обеспечении безопасности КВОИ должны составлять следующие элементы.

1. Нормативно-правовая основа СКАПР при обеспечении безопасности КВОИ.

Нормативно-правовую основу рассматриваемого СКАПР составляет совокупность следующих групп правовых норм:

1) нормы специального законодательного акта в области обеспечения безопасности КВОИ, которые определяют правовой статус КВОИ; субъектов государственного управления в этой сфере и их функции; систему и содержание мер обеспечения безопасности КВОИ, порядок их применения и др.;

2) нормы законодательных актов, постановлений Правительства Республики Беларусь, а также предписания нормативных правовых актов уполномоченных государственных органов и собственников (владельцев) КВОИ, детализирующие вопросы реализации мер обеспечения безопасности КВОИ;

3) нормы актов законодательства, непосредственно не регламентирующие обеспечение безопасности КВОИ, но создающие условия по реализации мер обеспечения их безопасности, а также определяющие полномочия государственных органов и иных организаций по реализации таких мер.

В настоящее время вопросы обеспечения безопасности КВОИ регламентируются Указом Президента Республики Беларусь от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» (далее – Указ № 486), постановлением Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации», а также приказами Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ) и техническими нормативными правовыми актами.

Вместе с тем при осуществлении правового регулирования обеспечения безопасности КВОИ возникает ряд проблем, основной из которых является сопряжение технических аспектов обеспечения безопасности КВОИ и закономерностей правовой регламентации данной сферы общественных отношений.

Наличие данной проблемы обусловлено следующими обстоятельствами:

1) вовлечение деятельности по обеспечению безопасности КВОИ в сферу правового регулирования имеет определенные последствия:

подчинение этой деятельности принципам правового регулирования (использование правовых дефиниций, определение правового статуса субъектов, определение вида и характера действий, установление процедурного порядка осуществления действий);

определение пределов осуществления деятельности по обеспечению безопасности КВОИ (осуществление действий только по технической защите информации или иных действий);

установление при осуществлении деятельности по обеспечению безопасности КВОИ общеобязательных и унифицированных правил поведения (невыполнение этих действий влечет административную или уголовную ответственность – например, нарушение правил защиты информации (ст. 22.7 Кодекса Республики Беларусь об административных правонарушениях) или умышленное нарушение правил эксплуатации компьютерной системы или сети (ст. 355 Уголовного кодекса Республики Беларусь);

2) деятельность по обеспечению безопасности КВОИ имеет свою специфику:

такая деятельность в большинстве своем регулируется различными техническими нормативными правовыми актами;

функционирование программно-аппаратных средств невозможно урегулировать нормативными правовыми актами.

В связи с этим требуется принятие законодательного акта (внесение изменений в Указ № 486), который бы в полном объеме регулировал отношения в сфере обеспечения безопасности КВОИ.

2. Субъекты режимной деятельности, осуществляемой в рамках СКАПР при обеспечении безопасности КВОИ.

К таким субъектам относятся ОАЦ и его уполномоченные должностные лица. Вместе с тем существует объективная потребность в расширении субъектов рассматриваемого СКАПР, в частности при осуществлении в отношении КВОИ режимной деятельности по обработке информации, содержащей государственные секреты.

3. Объекты, на которые направлена режимная деятельность, осуществляемая в рамках СКАПР при обеспечении безопасности КВОИ.

Режимная деятельность, осуществляемая в рамках рассматриваемого СКАПР, должна быть направлена:

1) на критические элементы КВОИ, т. е. его структурные компоненты, полное или частичное разрушение, выход из строя или невозможность действовать которых с неизбежностью приводят к нарушению или прекращению функционирования КВОИ в целом (аппаратные и программные средства, руководство и отдельные специалисты КВОИ и т. п.);

2) уязвимые места КВОИ – те его участки, зоны или сегменты критических элементов КВОИ, в отношении которых в силу их недостаточной устойчивости или низкого уровня защищенности могут быть успешно реализованы незаконные действия (электрокабели, провода связи, мотивация и здоровье персонала объекта и т. п.);

3) деяния, совершаемые в отношении критических элементов или уязвимых мест КВОИ, либо иные деяния, создающие угрозу безопасности КВОИ.

Адекватная и эффективная режимная деятельность должна основываться на знании и прогнозировании возможных действий лиц, создающих угрозы безопасности КВОИ, – нарушителей безопасности КВОИ.

4. Режимная деятельность уполномоченных субъектов по установлению, поддержанию и прекращению действия СКАПР при обеспечении безопасности КВОИ.

Целью осуществления режимной деятельности субъектов СКАПР при обеспечении безопасности КВОИ является охрана и защита, обеспечивающие соблюдение интересов государства и общества, а также нормальное функционирование объекта или поддержание его функционирования в случае выхода из строя его компонентов.

Установление СКАПР осуществляется принятием соответствующего законодательного акта, который регламентирует отношения в рассматриваемой области, определяет критическую информационно-коммуникационную инфраструктуру с выделением КВОИ и включением таких объектов в Государственный реестр КВОИ. Рассматриваемый СКАРП фактически установлен принятием Указа № 486. Одновременно сформирован соответствующий Государственный реестр.

Содержанием деятельности субъектов рассматриваемого СКАПР по поддержанию данного режима должна стать реализация соответствующих правовых, организационных, инженерно-технических, аппаратно-программных и специальных мер обеспечения безопасности КВОИ. Вместе с тем очевидно, что система мер обеспечения безопасности КВОИ сформирована еще не в полной мере, так как основной упор пока делается на аппаратно-программные и инженерно-технические меры.

Действия по прекращению действия СКАПР при обеспечении безопасности КВОИ будут заключаться в выводе соответствующих объектов из числа критически важных и в исключении их из Государственного реестра КВОИ.

УДК 343

Д.Г. Полещук

НЕЗАКОННЫЙ ОБОРОТ ПАРОЛЕЙ, КОДОВ ДОСТУПА К КОМПЬЮТЕРНОЙ СИСТЕМЕ, СЕТИ ИЛИ МАШИННОМУ НОСИТЕЛЮ: ПЕРСПЕКТИВЫ КРИМИНАЛИЗАЦИИ

Общество XXI в. характеризуется скоростными темпами развития информационных технологий, повышением значения информации и подавляющим воздействием глобальной компьютерной сети Интернет на повседневную жизнь большинства людей. На рабочих местах, в домашних условиях, в транспорте используются компьютеры, планшеты, смартфоны и иные устройства, позволяющие осуществлять быстрый доступ к различным информационным системам или сетям (в том числе социальным). В основном такой доступ носит санкционированный характер, то есть для его осуществления требуется идентификация пользователя путем введения его логина и пароля (кода) доступа, только пароля (кода) доступа либо использования дополнительных средств защиты от незаконного доступа (например, подтверждение доступа посредством SMS-информирования). Одновременно на многих машинных носителях (компьютеры, мобильные устройства и др.) также устанавливаются пароли (коды) доступа и даже сканеры отпечатков пальцев с целью ограничения доступа к таким устройствам посторонних лиц. Осуществление указанных технических мер обусловлено необходимостью защиты хранящейся в компьютерной системе, сети или на машинных носителях информации, ценной для их пользователей, владельцев и собственников.

Вместе с тем попытки несанкционированного доступа к защищенной информации приобрели маштабность мирового значения, а борьба с ними стала одной из ключевых проблем в сфере обеспечения информационной безопасности.

В то же время вопросам оборота паролей, кодов доступа к компьютерной системе, сети или машинному носителю (далее – пароли), полученным незаконным путем, в национальном охранительном законодательстве и в юридической литературе особого внимания не уделяется. С точки зрения действующего законодательства незаконные действия с паролями (продажа, отчуждение в иной форме, приобретение и др.) теоретически не могут рассматриваться как приготовление к преступлению (ст. 349 УК Республики Беларусь) или административному правонарушению (ст. 22.6 КоАП Республики Беларусь), поскольку КоАП не выделяет приготовление к административному правонарушению как основание наступления административной ответственно-

сти, а приготовление в рамках УК возможно только к умышленному преступлению, кроме преступлений, не представляющих большой общественной опасности.

Что касается возможности квалификации незаконного оборота паролей по ст. 353 УК «Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети», по нашему мнению, она является некорректной, поскольку предмет указанного преступления по своему смысловому содержанию пароли не охватывает.

Таким образом, меры правового воздействия на лиц, занимающихся незаконным оборотом паролей, в Республике Беларусь отсутствуют.

Общественная опасность рассматриваемого деяния заключается в возможности неконтролируемого использования паролей, добытых незаконным путем, для подготовки и совершения более тяжких преступлений. При этом миллионы паролей ежедневно похищаются и передаются хакерами друг другу в сети Интернет. Особую роль при их незаконной передаче играет даркнет (частная сеть, соединения которой устанавливаются только между доверенными участниками, нередко с применением специального программного обеспечения).

Случаи масштабных похищений и продаж паролей непосредственно затрагивают и граждан государств – членов СНГ. Так, в мае 2016 г. на одном из специализированных форумов молодой русскоязычный хакер похвастался массивом из 1,17 млрд взломанных учетных записей (большинство из них аккаунты Mail.ru), который он готов продать. В июне 2016 г. в средствах массовой информации сообщалось о том, что хакер под ником Peace на одной из онлайн-платформ выставил на продажу пароли 70 млн пользователей «Вконтакте» за 1 биткоин (примерно $1300), полученные в результате кибератаки на сайт в период между 2011 и 2013 гг. Уже в марте 2017 г. в даркнете были выставлены на торги 5 млн паролей к почтовым ящикам Gmail и Yahoo.

Международные основы борьбы с незаконным оборотом паролей установлены Конвенцией Совета Европы от 23 ноября 2001 г. «О преступности в сфере компьютерной информации» (ETS № 185) (далее – Конвенция). Пункт 1 ст. 6 Конвенции предусматривает необходимость установления уголовной ответственности за умышленное производство, продажу, приобретение для использования, импорт, оптовую продажу или иные формы предоставления в пользование компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения противозаконного доступа, неправомерного перехвата, воздействия на данные или воздействия на функционирование системы. Кроме того, Конвенция ориентирует на принятие законодательных мер, необходимых для того, чтобы квалифицировать в качестве преступления владение одним или несколькими паролями с намерением использовать их для совершения указанных выше преступлений.

Уголовная ответственность за рассматриваемые действия не наступает, если они связаны с разрешенным испытанием или защитой компьютерной системы.

Следует отметить, что сторона, присоединяющаяся к Конвенции, может сохранить за собой право не применять положения об уголовной ответственности за незаконные действия с паролями при условии, что такая оговорка не будет касаться продажи, оптовой продажи или иных форм предоставления в пользование паролей, кодов доступа или иных аналогичных данных.

Многие уголовные законы зарубежных государств содержат специальные нормы об уголовной ответственности за незаконный оборот паролей.

В частности, ст. 260-4 УК Молдовы предусматривает ответственность за неправомерные производство, импорт, продажу или предоставление паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к информационной системе в целом или ее части с целью совершения одного из преступлений, предусмотренных ст. 237, 259, 260-1–260-3, 260-5 и 260-6, если эти действия повлекли причинение ущерба в крупных размерах.

Статья 285 УК Грузии устанавливается уголовная ответственность за самовольные изготовление, хранение, продажу, распространение пароля, кода допуска, необходимого для проникновения в компьютерную систему, или иных подобных данных либо иное обеспечение доступа к ним с целью совершения киберпреступления либо нарушения тайны личной переписки, телефонных переговоров или сообщений.

Согласно ст. 231 УК Чехии подлежит уголовной ответственности тот, кто с намерением совершить нарушение тайны переписки или неавторизованный доступ к компьютерной системе и компьютерной информации производит, вводит в оборот, импортирует, экспортирует, перенаправляет, предлагает, предоставляет, продает или иным образом предоставляет, приобретает для себя или для другого лица либо обрабатывает пароль компьютера, код доступа, данные, процесс или любые другие аналогичные средства, с помощью которых можно получить доступ к компьютерной системе или ее части.

В ст. 615-4 УК Италии также предусмотрена ответственность за незаконную закупку, воспроизведение, распространение, передачу или предоставление кодов, паролей либо других средств доступа к компьютерной или телекоммуникационной системе.

Учитывая мировые тенденции консолидации усилий всех государств в борьбе с преступлениями против информационной безопасно-

сти и унификации норм материального уголовного права с положениями Конвенции, полагаем целесообразным рассмотреть вопрос установления уголовной ответственности за отдельные незаконные действия с паролями и в Республике Беларусь.

Предложенный подход будет иметь следующие результаты:

установление уголовной ответственности за незаконный оборот паролей будет способствовать вовлечению Республики Беларусь в борьбу с транснациональной киберпреступностью и позволит реагировать на рассматриваемые незаконные действия, совершенные на ее территории;

для возможного присоединения к Конвенции положения национального уголовного права будут приведены в соответствие с ее требованиями;

признание рассматриваемого деяния преступлением позволит предупредить совершение иных преступлений против информационной безопасности (ст. 349–352 УК Республики Беларусь).

На основании изложенного и принимая во внимание особенности действующего уголовного закона, предлагаем дополнить гл. 31 УК Республики Беларусь статьей следующего содержания:

«Статья 353^1. Незаконные изготовление, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных

Незаконные изготовление с целью сбыта, приобретение либо сбыт паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к защищенному машинному носителю, защищенной компьютерной системе или сети в целом или любой их части для совершения преступлений, предусмотренных ст. 349, 350, 351 и 352 настоящего Кодекса, –

наказываются штрафом, или арестом, или ограничением свободы на срок до двух лет».

УДК 004:34

Ю.В. Полковниченко, Т.Г. Чудиловская

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время фиксируется все больше случаев использования информационно-коммуникационных технологий в целях нарушения работоспособности информационных систем и информационно-коммуникационных сетей, а также нарушения права граждан на неприкосновенность частной жизни, личной и семейной тайны, осуществления промышленного шпионажа, нарушения прав интеллектуальной собственности. Обеспечение информационной безопасности является актуальной проблемой ввиду наличия многообразных факторов и угроз. В обращении с ежегодным Посланием к белорусскому народу и Национальному собранию 21 апреля 2017 г. Президент Республики Беларусь А.Г. Лукашенко отметил: «Обеспечение национальной безопасности невозможно без надежной защиты от деструктивных информационных атак, которые стали средством вмешательства во внутренние дела суверенных государств».

Вопросы обеспечения информационной безопасности государства, наряду с организационными и программно-техническими мерами, должны регулироваться нормами права. Правовое обеспечение информационной безопасности в Республике Беларусь включает в себя огромный комплекс норм, содержащихся в различных нормативных правовых актах Республики Беларусь и международных договорах.

Правовое регулирование в области информационных отношений в Республике Беларусь осуществляется Законом Республики Беларусь «Об информации, информатизации и защите информации». Основной функцией Закона является регулирование отношений, возникающих в процессе жизненного цикла информации, при создании и использовании информационных технологий, систем, сетей, ресурсов, а также при организации и обеспечении защиты информации. Этот Закон устанавливает требования по защите информации, а также ссылается на иные законодательные акты Республики Беларусь, в которых закреплена ответственность за нарушение законодательства об информации, информатизации и защите информации.

Составы правонарушений в информационной сфере находят свое отражение в Кодексе Республики Беларусь об административных правонарушениях, в котором данному аспекту посвящена гл. 22 «Административные правонарушения в области связи и информации».

Одними из важнейших правовых средств обеспечения информационной безопасности являются нормы уголовного законодательства, устанавливающие преступные деяния, посягающие на отношения в различных сферах информационной безопасности и определяющие санкции за их совершение. Они представлены в Уголовном Кодексе Республики Беларусь в разделе XII «Преступления против информационной безопасности» (одноименная гл. 31, ст. 349–355). Преступления, посягающие на состояние защищенности жизненно важных интересов физических и юридических лиц в информационной сфере, содержатся и в других разделах и главах УК. С целью единообразного применения законодательства об ответственности за совершение преступлений против информационной безопасности целесообразно было бы принять

постановление Пленума Верховного Суда Республики Беларусь «О судебной практике по делам о преступлениях против информационной безопасности».

Важным документом, определяющим политику Республики Беларусь в сфере информационной безопасности, является Концепция национальной безопасности Республики Беларусь. В документе определены национальные интересы Республики Беларусь, внутренние и внешние источники угроз безопасности в информационной сфере, основные направления обеспечения информационной безопасности.

Принципы государственной политики Республики Беларусь в сфере информатизации и основные направления развития информационного общества с учетом совокупности факторов, влияющих на его прогресс, указаны в Стратегии развития информатизации в Республике Беларусь на 2016–2022 годы. Так, с учетом цифрового доверия, защиты информационных ресурсов и информационно-коммуникационной инфраструктуры Стратегия определяет основные направления обеспечения информационной безопасности:

организация научных исследований, разработка и производство собственных аппаратных и программных средств защиты информации, ключевых элементов информационно-коммуникационной инфраструктуры, совершенствование системы их стандартизации, сертификации и аттестации в целях создания «цифрового суверенитета» Республики Беларусь;

совершенствование нормативной правовой и нормативно-технической базы для доступного, эффективного и беспрепятственного информационного взаимодействия государства, бизнеса и граждан;

организация хранения персональных данных граждан Республики Беларусь исключительно в центрах обработки данных и дата-центрах на территории Республики Беларусь;

создание необходимого уровня защиты информации, содержащейся в государственных информационных ресурсах;

резервирование информационных сетей республиканских органов государственного управления;

активное использование возможностей белорусского спутника связи и вещания для увеличения информационного присутствия страны в мировом информационном пространстве.

В связи с постоянным ростом преступности в области информационной безопасности, масштабностью причиненного ею ущерба для физических и юридических лиц такие преступления представляют серьезную угрозу для общества, а борьба с ними является серьезной проблемой для правоохранительных органов, особенно в части, касающейся оперативного установления злоумышленников, самого факта и места совершения преступления. Для противодействия данным преступлениям в 2001 г. в Министерстве внутренних дел Республики Беларусь создано управление по раскрытию преступлений в сфере высоких технологий (УРПСВТ, или управление «К»). Приоритетной задачей управления является координация деятельности подразделений МВД Республики Беларусь при выявлении ими преступлений против информационной безопасности. Также управление «К» осуществляет международное сотрудничество по оперативному обмену информацией в рамках противодействия преступлениям в сфере высоких технологий посредством международной сети НКП (Национальный контактный пункт), функционирующей под эгидой Римско-Лионской подгруппы «Группы Восьми». Наиболее эффективное взаимодействие осуществляется с Российской Федерацией.

Следует отметить, что Следственный комитет Республики Беларусь выступил с инициативой создания в Республике Беларусь центра противодействия киберпреступности. Центр передового опыта с целью решения теоретических и практических проблем противодействия киберпреступлениям предлагается создать на базе одного из учебных заведений Республики Беларусь. В центре должны будут работать как преподаватели вузов, так и сотрудники правоохранительных органов, специалисты в области расследования таких преступлений. Предполагается, что будут осуществляться исследования в области уголовного права, уголовного процесса, криминалистики, будут проводиться регулярные встречи ученых, представителей правоохранительных органов и частного сектора для обмена опытом и поиска решений существующих проблем, выработки стратегических подходов в борьбе с киберпреступностью, создания учебных и образовательных программ по данной тематике. Создание центра противодействия киберпреступности, несомненно, повысит уровень информационной безопасности в стране.

Таким образом, для обеспечения информационной безопасности в Республике Беларусь осуществляется эффективное правовое регулирование в информационной сфере, работают специальные подразделения для борьбы с преступлениями в области информационной безопасности, ведется взаимодействие с правоохранительными органами разных стран.

Приоритетными направлениями в развитии обеспечения информационной безопасности является совершенствование нормативной правовой базы, завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования дея-

тельности в этой сфере. При этом важное значение отводится усилению деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

УДК 343.8

А.Е. Сушко

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита граждан, их прав и свобод, интересов общества и государства являются основными задачами, стоящими перед правоохранительными органами Республики Беларусь.

На современном этапе столь динамичного развития и применения информационных технологий неизбежно возникает проблема защиты от их использования в преступных целях. Преступность в сфере высоких технологий не имеет границ и составляет угрозу международной безопасности.

Киберпреступность является проблемой мирового уровня, так как подобные преступления совершаются, как правило, транснациональными организованными преступными группами, члены которых, используя возможности сети Интернет, виртуально пересекают границы между государствами и пользуются несовершенством законодательства различных государств. Преступления против информационной безопасности приобретают транснациональный и организованный характер. Преступление с использованием компьютерной техники и ресурсов интернета может быть совершено на территории другой страны и даже нескольких государств одновременно. При этом злоумышленник потратит на его совершение всего несколько минут, общаясь с представителями различных организаций (банковские учреждения, интернет-магазины, платежные системы, различные сервисы интернета) не выходя из своего дома.

Концепция национальной безопасности Республики Беларусь определяет информационную безопасность как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере и выделяет ее в самостоятельную составляющую национальной безопасности. К таким угрозам относятся и преступления против информационной безопасности, впервые отраженные в Уголовном кодексе Республики Беларусь

1999 г. Статистика последних лет свидетельствует об увеличении количества этих преступлений.

В 2016 г. в сравнении с 2015 г. количество выявленных преступлений в сфере высоких технологий увеличилось на 1,3 % (с 2 440 до 2 471), притом прирост преступлений против информационной безопасности (гл. 31 УК Беларуси) составил 63,6 % (с 404 до 651). Количество же фактов несанкционированного доступа к компьютерной информации возросло на 152,9 % (со 102 до 258).

Национальными интересами России в сфере информационных технологий является обеспечение прав и свобод граждан, а также неприкосновенность частной жизни, как определено в Доктрине информационной безопасности Российской Федерации.

Информационная безопасность приобрела особое значение в условиях глобализации и интенсивного информационного обмена в мировом масштабе. Дело бывшего сотрудника ЦРУ и агентства национальной безопасности США Эдварда Сноудена, хакерские атаки на серверы Демократической партии США, серверы Европейской комиссии подтверждают это.

Практически каждый белорус в настоящее время активно использует множество высокотехнологичных устройств (Smart TV, компьютеры, планшеты, мобильные телефоны и иные электронные устройства, банковские карточки). Международный союз электросвязи отметил, что Беларусь в 2016 г. улучшила позиции в рейтинге развития информационно-коммуникационных технологий (ИКТ) и заняла 31-е место среди 175 стран.

Очевидно, что в настоящее время подлежит защите любая информация, имеющая отношение к физическому лицу, которая включает его персональные данные, сведения о регистрации на различных сайтах в сети Интернет или в социальных сетях, сведения о покупках в интернет-магазинах. Минимизировать риски в указанной сфере, в частности со стороны операторов персональных данных, позволит принятие Закона «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Так как проблема информационной безопасности не носит региональный характер, а охватывает все государства мира, при разработке указанного Закона целесообразно ориентироваться на европейское и российское законодательства в данной сфере.

Управлением Следственного комитета по Минской области в январе 2017 г. завершено расследование уголовного дела в отношении группы лиц, занимавшихся хищениями денежных средств граждан.

Расследованием установлено, что трое граждан Российской Федерации, арендуя дом в Минском районе с ноября 2015 г. по февраль 2016 г., с целью завладения денежными средствами граждан использовали вредоносное программное обеспечение и от имени Министерства внутренних дел Республики Беларусь рассылали электронные уведомления о наложении административного взыскания за якобы имевший место просмотр видеоматериалов, содержащих элементы порнографического характера. Для оплаты штрафа предлагалось перевести денежные средства на счета абонентских номеров одного из белорусских операторов сотовой связи. В результате противоправных действий фигуранты дела произвели блокирование компьютерной информации более 900 граждан. Причиненный ущерб составил свыше 136 тыс. белорусских рублей.

Главным следственным управлением Следственного комитета Республики Беларусь в 2016 г. при поддержке Европола, Секретной службы и ФБР США, полиции Кипра пресечена деятельность организованной преступной группы, жертвами которой стали более 130 тыс. держателей платежных карт из 29 стран. Преступная группа занималась компрометацией кредитных карт с использованием компьютерных технологий и вредоносных программ. Для этих целей были созданы несколько подставных онлайн-магазинов и фиктивная компания по разработке программного обеспечения. Киберпреступники связывались с легальными платежными онлайн-сервисами и имитировали проведение многочисленных международных транзакций. В дальнейшем похищенные средства переводились на банковский счет на Кипре. Благодаря большому числу транзакций с маленькими суммами преступникам несколько месяцев удавалось быть незамеченными. Сумма нанесенного ими ущерба составляет более 8 млн евро. Четыре участника группы, включая лидера, были установлены и задержаны Следственным комитетом Беларуси.

Европейский центр по борьбе с киберпреступностью, начавший свою работу в 2013 г., играет ведущую роль в борьбе с киберпреступностью на территории Европейского Союза, занимаясь созданием оперативных и аналитических мощностей, необходимых для обеспечения быстрого реагирования на киберпреступления, а также организацией взаимодействия официальных ведомств ЕС и стран-членов с международными партнерами. Сотрудники центра разрабатывают методы пресечения преступлений в сфере информационных технологий, в том числе завладения данными кредитных карточек, защищают от хакеров пользователей социальных сетей. Кроме того, центр обеспечивает безопасность стратегически важных интернет-ресурсов и коммуникационных систем ЕС, действует против распространения детской порнографии, занимается сбором и обработкой данных, оказанием информационной, технической и криминалистической поддержки соответст-

вующим подразделениям правоохранительных органов стран – членов ЕС, координацией совместных расследований, обучением и подготовкой специалистов. Европейский центр по борьбе с киберпреступностью содействует проведению необходимых исследований и созданию программного обеспечения, занимается оценкой и анализом существующих и потенциальных угроз, составлением прогнозов и выпуском заблаговременных предупреждений.

Так, 30 ноября 2016 г. был дан старт глобальной операции, получившей кодовое названия Avalanche («Лавина»). Для ликвидации огромной киберпреступной сети были объединены усилия правоохранительных органов и специалистов в области информационной безопасности из более чем 40 стран мира (Европол, ФБР, Интерпол, ICANN, Symantec, Shadowserver Foundation, Registrar of Last Resort и др.). Операцию предваряли расследования и другая подготовительная работа на протяжении четырех лет. В ходе проведения Avalanche прошли обыски в 37 местах и были арестованы пять подозреваемых, более 800 тыс. доменов перешли под контроль властей или были заблокированы, 39 серверов были изъяты и еще 221 сервер ушел в офлайн, после того как хостинг-провайдеров уведомили о нарушениях. Инфраструктура Avalanche использовалась для хостинга и распространения более чем 20 семейств различных вредоносных программ, в том числе таких известных, как GozNym, Marcher, Dridex, Matsnu, URLZone, XSWKit, Pandabanker, Cerber и Teslacrypt. Кроме того, злоумышленники занимались рассылкой спама, а также отмыванием денег, поиском и наймом так называемых денежных мулов. Огромный ботнет насчитывал как минимум 500 тыс. устройств по всему миру, которые за прошедшие годы успели атаковать более 40 крупных финансовых организаций, а также пользователей в более чем 180 странах мира. Суммарный ущерб от деятельности киберпреступников оценивается в сотни миллионов евро.

Указанные преступления, совершенные как на территории Республики Беларусь в отношении граждан Беларуси, так и на территории десятков государств организованными группами злоумышленников, подчеркивают опасность, исходящую от киберпреступников, и требуют от правоохранительных органов разных стран надлежащего уровня взаимодействия.

В настоящее время, на наш взгляд, необходимо:

провести мероприятия для присоединения Республики Беларусь к международным правовым инструментам в сфере информационной безопасности, в том числе к Конвенции о защите физических лиц при автоматизированной обработке персональных данных, к Конвенции Совета Европы о борьбе с киберпреступностью, одними из участников которой являются члены СНГ – Азербайджан, Армения, Молдова, к Соглашению между правительствами государств – членов Шанхайской

организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности;

разработать и принять Стратегию обеспечения кибербезопасности (информационной безопасности) Республики Беларусь, в которой следует отразить основные современные угрозы интересам Беларуси, ее граждан и бизнес-сообщества в киберпространстве, определить основные мероприятия, направленные на защиту объектов критической инфраструктуры, прав граждан и государства, совершенствование национального законодательства в области информационной безопасности, закрепление статуса национального координатора, который объединит специалистов в сфере информационной безопасности из различных государственных органов и представителей частного сектора. Также целесообразно разработать Закон «Об обеспечении информационной безопасности» и Закон «О персональных данных»;

продолжить сотрудничество Следственного комитета Республики Беларусь с правоохранительными органами Российской Федерации, Европы и США, в частности с ФСБ, Европолом, полицией Нидерландов, ФБР, Секретной службой США, для организации борьбы с международными преступлениями против информационной безопасности, для обмена информацией с целью успешного раскрытия и расследования таких преступлений;

продолжить работу над реализацией инициативы Следственного комитета в создании национального киберцентра, который должен стать платформой сотрудничества и координации действий по вопросам расследования и профилактики преступлений, связанных с использованием сети Интернет, объединить экспертные знания правоохранителей, ученых, представителей частного сектора. Центром будут проводиться научные исследования, вырабатываться стратегические подходы в борьбе с преступностью, создаваться учебные и образовательные программы по данной тематике, раскрываться и расследоваться киберпреступления.

УДК343.54

О.О. Топорикова

СЕКСУАЛЬНОЕ КИБЕРВЫМОГАТЕЛЬСТВО (SEXTORTION)

Происходящие изменения форм социальной коммуникации, связанные с развитием функционально совместимых информационно-коммуникационных технологий, стимулируют возникновение новых форм сексуальной эксплуатации, в том числе путем модификации преступлений, которые традиционно относились к категории совершаемых только посредством личного (реального) контакта (например, преступления против половой свободы и половой неприкосновенности). К числу таких преступлений можно отнести сексуальное кибервымогательство (sextortion).

Сексуальное вымогательство относится к одной из новых форм сексуальной эксплуатации. Т.М. Лопатина отмечает, что для интернет-вымогательства как явления в целом характерны две тенденции: стремление придать требованиям правомерный вид и гиперлатентность.

Сексуальное кибервымогательство реализуется посредством информационно-коммуникационных технологий и нефизических форм принуждения с целью получения сексуальных услуг либо приватных материалов (изображения, видео сексуального содержания) от жертвы. При этом чаще всего физического контакта преступника и жертвы не происходит. Жертва совершает иные действия сексуального характера либо половые сношения с третьими лицами, которые транслируются преступнику в режиме реального времени с использованием web-камеры.

Сексуальное вымогательство может быть сопряжено с совершением таких преступлений, как изготовление и распространение порнографии (ст. 343 УК) и незаконное распространение информации о частной жизни (ст. 179 УК). В большинстве таких случаев, зарегистрированных на территории Республики Беларусь, преступник и жертва ранее были знакомы, состояли в супружеских отношениях либо проживали совместно. Мотивом распространения приватных материалов была либо месть из-за расставания либо принуждение к восстановлению отношений. Анализ правоприменительной практики показал, что чаще всего в таких случаях жертвы не подают заявления о привлечении виновного лица по ст. 179 УК. Кроме того, имеют место мотивированные примирения с преступниками, попытки потерпевших прекратить уголовное производство по ст. 343 УК.

Анализ национальной правоприменительной практики и зарубежного опыта позволил выделить две формы сексуального кибервымогательства, особенности которых влияют на квалификацию деяния по УК Республики Беларусь.

Например, может иметь место следующая картина преступления. Используя для общения социальные сети либо иные средства коммуникации, преступник устанавливает доверительный контакт с жертвой, после чего просит выслать изображение, видео сексуального характера либо осуществить сексуальные действия с трансляцией на web-камеру в режиме реального времени. Получив данный материал, он начинает шантажировать им жертву.

Далее возможно два варианта развития событий, влияющие на квалификацию деяний.

Первый вариант – выражаются материальные требования, требования о перечислении денежных сумм. Такое сексуальное кибервымогательство имеет признаки классического вымогательства (ст. 208 УК). Согласно данным Главного управления внутренних дел Мингорисполкома в 2016 г. зарегистрировано 8 подобных случаев вымогательства денег с угрозой распространения информации сексуального характера.

Второй вариант – преступник понуждает жертву продолжать совершать иные действия сексуального характера либо выражает требование о вступлении в половые отношения с третьими лицами, которые будут транслироваться в режиме реального времени с использованием средств телекоммуникации (Skype, Viber и др.), требует высылать более откровенные сексуальные материалы.

Вторая форма преступного поведения также зафиксирована на территории Республики Беларусь. При этом однозначной практики квалификации указанного деяния в настоящее время не сформировано. В некоторых случаях уголовные дела возбуждаются по ст. 343 УК либо по иным статьям, связанным с использованием информационных технологий, в других случаях деяния квалифицируются по ст. 170 УК. Так, например, К., «формально знакомый по интернету» с Н., понуждал ее совершать иные действия сексуального характера и транслировать их ему по Skype. При попытке Н. прекратить подобные отношения К. заблокировал ее компьютер, разослал видеозаписи интимного характера с ее участием родственникам Н., а также ее знакомым в социальной сети «Одноклассники» (более 100 человек). Уголовное дело в этом случае было возбуждено по ч. 2 ст. 351 УК.

В случае если аналогичные действия совершаются лицом, с которым жертва была знакома в реальной жизни (например, состояли в супружеских отношениях либо проживали совместно), то виновные привлекаются к ответственности по ч. 1 ст. 170 и ч. 2 ст. 343 УК. Так, например, В. встречался и поддерживал с Т. интимные отношения. На протяжении данного периода времени он неоднократно осуществлял фотовидеосъемку Т., которая либо была в обнаженном виде, либо участвовала в сценах половых актов. После того как они расстались, В. неоднократно искал общения с Т. и требовал вступить с ним в половое сношение и совершить иные действия сексуального характера, высказывая ей угрозы о распространении в сети Интернет фотографий и видеозаписей, содержащих изображения Т. в обнаженном виде и сцены половых актов с ее участием. С целью подтверждения реальности угроз В. создал в социальной сети «Вконтакте» анкету, содержащую персональные данные В., в которой разместил указанные материалы в от-

крытом доступе. После чего В. оповестил пользователей о возможности просмотра данных материалов. Решением суда Барановичского района и г. Барановичи Брестской области В. был признан виновным по ч. 2 ст. 343 УК (изготовление и хранение с целью распространения и рекламирования, распространение и рекламирование порнографических материалов), а также в понуждении к половому сношению и совершению иных действий сексуального характера путем шантажа потерпевшей (ч. 1 ст. 170 УК) и осужден к 2 годам лишения свободы с применением отсрочки исполнения наказания.

Очевидно, что последние два примера в целом характеризуются идентичностью объективных и субъективных признаков преступления, предусмотренного ст. 170 УК. Вместе с тем в случаях сексуального кибервымогательства правоприменители, мотивируя свое решение отсутствием физического взаимодействия между преступником и жертвой, зачастую не усматривают признаков понуждения к совершению действий сексуального характера.

Подобные противоречия создают сложности в обеспечении противодействия данной форме эксплуатации половой свободы. Кроме того, определенной проблемой квалификации является то, что понуждение лица к изготовлению порнографии, как форма эксплуатации половой свободы, выходит за пределы диспозиции ст. 170 УК.

В заключение можно сделать следующие выводы.

Сексуальное кибервымогательство следует относить к преступлениям против половой неприкосновенности и половой свободы и квалифицировать как преступление, предусмотренное ст. 170 УК. Подобный подход позволяет четко определить объект правовой охраны, обеспечить уголовно-правовую защиту личности от новых форм посягательств.

Так как приватные изображения граждан и иная информация о сексуальных отношениях относятся к числу сведений о частной жизни, при наличии признаков собирания подобной информации о потерпевшем без его согласия действия виновного должны также квалифицироваться по ст. 179 УК. Под собиранием информации в данном случае полагаем целесообразным понимать осуществление записи трансляций, на которых потерпевший совершает иные действия сексуального характера при условии, что последнему неизвестно, что трансляция записывается.

В целях обеспечения уголовно-правовой защиты прав и законных интересов личности, а также противодействия распространению новых форм преступного поведения, совершаемого с использованием информационных и телекоммуникационных технологий, полагаем целесообразным ч. 2 ст. 170 УК дополнить квалифицирующим признаком «совершенное с использованием глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования либо выделенной сети электросвязи».

УДК 004:34

А.В. Фурманов, Т.Г. Чудиловская

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Современные информационные технологии не только открывают безграничные возможности, но и порождают новые проблемы развития общества, несут новые опасности, вызовы и угрозы его безопасности, одной из важнейших составляющих которой является информационная безопасность. Практически все страны с развитой экономикой на уровне государственных органов, предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности.

В силу трансграничности угроз информационной безопасности эффективное противодействие правонарушениям, совершаемым с использованием информационных технологий, может быть обеспечено на основе тесного взаимодействия государств – участников Содружества Независимых Государств между собой и с другими государствами.

Одним из основных направлений сотрудничества государств – участников СНГ является выработка рекомендаций и предложений по совершенствованию правового обеспечения информационной безопасности.

В феврале 1996 г. был принят модельный Уголовный кодекс для государств – участников СНГ (далее – модельный УК), который содержит отдельную главу 30 «Преступления против информационной безопасности», состоящую из семи статей (ст. 286–292). Принятие данного документа обратило внимание государств – участников СНГ на необходимость уголовно-правовой защиты отношений, складывающихся в сфере обеспечения информационной безопасности.

На сегодняшний день все государства СНГ включили в принятые после обретения независимости уголовные кодексы самостоятельные главы, предусматривающие уголовную ответственность за компьютерные преступления. Однако необходимо заметить, что в уголовных законах государств – участников СНГ отсутствует единство подходов к определению терминов, что не способствует унификации уголовного законодательства стран СНГ в рассматриваемой области.

Для укрепления правовой основы борьбы с преступностью в информационной сфере 1 июня 2001 г. было подписано Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, которое является правовой

основой сотрудничества правоохранительных и судебных органов государств – участников СНГ в области обеспечения эффективного предупреждения, выявления, пресечения, раскрытия и расследования компьютерных преступлений.

Важным нормативным актом по сближению национальных законодательств, регулирующим информационные отношения, является модельный Закон «Об информатизации, информации и защите информации», принятый 18 ноября 2005 г. на 26-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ.

В рамках СНГ также принята Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности, утвержденная Решением Совета глав государств Содружества Независимых Государств 10 октября 2008 г. В документе определены основные цели и принципы сотрудничества в сфере обеспечения информационной безопасности, угрозы информационной безопасности, методы и основные направления сотрудничества, план мероприятий. Концепция явилась основанием для Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, которые приняты на 38-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ.

В настоящее время преступления, совершаемые с использованием информационных технологий, приобретают транснациональный и организованный характер, создают угрозу национальной безопасности государств – участников СНГ; происходит сращивание различных видов преступности, главным образом за счет использования средств компьютерной техники и информационных сетей. В связи с этим была принята Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, одобренная Решением Совета глав государств СНГ 25 октября 2013 г. Концепция определяет принципы, задачи, основные направления, формы и систему обеспечения сотрудничества.

Для осуществления взаимодействия при выполнении положений Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности с учетом важности совместного и эффективного использования новейших информационно-коммуникационных технологий для усиления противодействия угрозам информационной безопасности 20 ноября 2013 г. заключено Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности. Целью документа является проведение совместных скоординированных мероприятий, направленных на обеспечение информационной безопасности.

Для обеспечения решения задач устойчивого развития информационных отношений, надежной защиты от реализации угроз жизненно важным интересам личности, общества и государства в информационной сфере 28 октября 2016 г. Советом глав правительств СНГ утверждена Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и План действий по ее реализации.

В документе определены основные направления взаимодействия государств – участников СНГ в области информационной безопасности:

разработка и обоснование предложений по структуре и задачам коллективной системы информационной безопасности государств – участников СНГ;

поощрение дальнейшего укрепления доверия и основ безопасности посредством дополняющих и взаимоукрепляющих инициатив в области безопасности при использовании информационно-компьютерных технологий;

защита национальных и межгосударственных информационных систем от несанкционированного доступа, от утечки защищаемой информации по техническим каналам и от внешнего электромагнитного воздействия;

защита баз данных и информационных ресурсов;

защита персональных данных и прав субъектов информации;

обеспечение безопасности информационных и коммуникационных технологий, сетей и систем;

создание защищенных систем межведомственного электронного документооборота;

развитие механизмов мониторинга и противодействия киберпреступности;

обеспечение взаимодействия национальных центров реагирования на компьютерные инциденты;

выявление и оперативное реагирование на случаи нарушения информационной безопасности, обмен информацией и техническими средствами борьбы с нарушениями;

формирование систем мониторинга ресурсов национальных сегментов интернета в целях своевременного выявления угроз, а также поиска оптимальных средств их нейтрализации;

создание инфраструктуры, необходимой для внедрения электронной цифровой подписи;

подготовка и реализация совместных мероприятий и проектов по формированию культуры обеспечения информационной безопасности.

Краткий обзор документов в сфере обеспечения информационной безопасности показывает, что нормотворческий процесс на пространстве СНГ протекает довольно динамично. Информационная политика государств – участников СНГ направлена на установление общих подходов к правовому регулированию обеспечения информационной безопасности, укреплению сбалансированности национальных правовых систем в условиях информатизации общества; на развитие международного информационного обмена; на обеспечение безопасности информационных условий экономического и таможенного сотрудничества; на стимулирование использования информационно-коммуникативных технологий во всех сферах жизни общества.

Однако принимаемые в рамках СНГ документы не в полной мере согласованы между собой. Для решения задач правового регулирования отношений в сфере обеспечения информационной безопасности исключительно важным является вопрос проработки правовых дефиниций с целью однозначного их толкования. Унификация основных терминов и понятий в нормативной правовой базе государств – участников СНГ – важное направление совершенствования законодательства.

Актуальным является и решение вопроса о юридической силе правовых актов СНГ для Республики Беларусь и иных государств – участников СНГ, так как на уровне учредительных документов отсутствует четкая система международно-правовых актов, принимаемых органами СНГ, – их виды, соотношения между собой по юридической силе и степени обязательности.

УДК 341.24:342.97

С.А. Чернышева

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПЛЕНОСТЬЮ

Компьютерная преступность (киберпреступность или кибертерроризм), являясь принципиально новым видом нарушений в информационной сфере, характеризуется способностью быстро приспосабливаться к новым условиям и проникать во все сферы жизни общества.

Компьютерная преступность превратилась в целую криминальную отрасль. Возможности быстро развивающихся информационно-компьютерных технологий (ИКТ) все активнее используются в преступных целях, о чем свидетельствует статистика компьютерных преступлений как в Республике Беларусь, так и в зарубежных странах.

Так, в Республике Беларусь в 2016 г. число выявленных преступлений в сфере высоких технологий увеличилось на 1,3 % в сравнении с 2015 г., а общий уровень раскрываемости составил 56,5 % (в 2015 г. – 55,5 %).

Увеличение количества компьютерных преступлений произошло за счет прироста преступлений против информационной безопасности на 63,6 % (с 404 до 651). Только количество фактов несанкционированного доступа к компьютерной информации возросло на 152,9 % (с 102 до 258).

Столкнувшись с компьютерной преступностью, органы уголовной юстиции зарубежных стран начали борьбу с ней путем применения к злоумышленникам традиционных норм о хищениях или злоупотреблениях. Однако такой подход оказался неудачным. Компьютерные преступления не укладывались в диспозиции норм об ответственности за названные преступления. В них не был учтен способ совершения преступлений (использование высоких технологий), личность преступника и общественно опасные последствия, которые исчислялись миллиардами долларов США.

Стали возникать новые нормы уголовного права, предусматривающие ответственность за новый вид преступности – компьютерные преступления.

Впервые закон о компьютерных преступлениях был принят 2 апреля 1973 г. в Швеции. В начале 1990-х гг. Уголовный кодекс Швеции был дополнен нормами, предусматривающими ответственность за деяния с использованием компьютерной информации и технологий.

В 1979 г. на конференции Американской ассоциации адвокатов впервые в США была сформирована система компьютерных преступлений, ставшая затем основой для уголовного законодательства штатов.

Вопросами борьбы с компьютерными преступлениями стали заниматься и международные организации.

С 1983 по 1985 г. Комитет Организации экономического сотрудничества и развития (ОЭСР) обсудил возможность международной гармонизации уголовного законодательства отдельных государств в целях борьбы с экономическими компьютерными преступлениями. В 1986 г. Комитетом был предложен единый перечень действий, которые должны рассматриваться в законодательстве государств – членов организации как компьютерные преступления.

В период с 1985 по 1989 г. над проблемой компьютерных преступлений работал Отдельный комитет экспертов по компьютерным преступлениям Совета Европы.

Развитие законодательства об ответственности за компьютерные преступления в ряде стран Европы происходило следующим образом. В 1986 г. Уголовный кодекс ФРГ был дополнен нормами, предусматривающими ответственность за компьютерные преступления. В августе 1990 г. вступил в силу Закон о злоупотреблениях компьютерами в

Великобритании. В 1993 г. Уголовный кодекс Нидерландов был дополнен новыми составами преступлений и т. д.

Особого внимания заслуживает опыт борьбы с компьютерной преступностью в Японии, которая в дополнение к нормам Уголовного кодекса о компьютерных преступлениях приняла 3 февраля 2000 г. Закон «О несанкционированном проникновении в компьютерные сети».

В первой половине 1990-х гг. законы об ответственности за компьютерные преступления были приняты и в других государствах мира.

Однако борьба с транснациональной организованной компьютерной преступностью требовала выработки более эффективных мер. Различия в правовых системах при недостаточно развитом международном сотрудничестве усложняли проведение расследований киберпреступлений и преследование за их совершение.

Эксперты ООН на XI Конгрессе (Бангкок, 2005) подчеркивали особый характер компьютерной преступности и указывали на необходимость применения комплексных подходов в борьбе с ней, а также на неотложность обновления уголовного законодательства всех развитых стран, в том числе введение норм, касающихся новых видов компьютерной преступности.

В настоящее время разработаны и действуют следующие международно-правовые основы сотрудничества в области борьбы с компьютерной преступностью:

Конвенция Совета Европы о киберпреступности 2001 г.;

Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые на XI Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями в Бангкоке 25 апреля 2005 г.;

Глобальная программа кибербезопасности, утвержденная Международным союзом электросвязи в 2007 г.;

Окинавская Хартия глобального информационного общества, принятая 23 июля 2000 г. на Окинаве (Япония);

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, заключенное 1 июня 2001 г. и др.

Главным органом в области межгосударственной борьбы с преступностью является Организация Объединенных Наций, которая с 1950 г. на Конгрессах ООН уделяет серьезное внимание проблеме борьбы с компьютерными преступлениями, и эта деятельность включена в число приоритетов ООН.

В частности, на XII Конгрессе ООН (Бразилия, апрель 2010 г.) была рассмотрена рекомендация относительно необходимости тщательного

изучения и принятия решения по разработке глобальной Конвенции о борьбе с киберпреступностью.

Республика Беларусь принимает активное участие в деле международной борьбы с компьютерной преступностью. Наряду с Уголовным кодексом Республики Беларусь (гл. 31) приняты значимые нормативные документы. Правовая база Республики Беларусь в отношении правонарушений и преступлений в информационном пространстве значительно приближена к требованиям и стандартам, принятым на международном уровне, в том числе Конвенции Совета Европы о киберпреступности 2001 г.

В Республике Беларусь Министерство юстиции, Управление «К» Министерства внутренних дел, Комитет государственной безопасности в целях противодействия киберпреступности осуществляют оперативный обмен информацией через международную сеть национальных контактных пунктов (НКП).

Указанная сеть НКП имеется в 58 странах мира (Россия, Украина, США, Германия, Великобритания, Испания, Швеция, Бразилия и др.). Вступление Беларуси в конце 2008 г. в международную сеть НКП способствовало как повышению эффективности работы по противодействию киберпреступности, так и дальнейшему развитию международного сотрудничества МВД Республики Беларусь в целом.

Во многих странах все еще практически отсутствует законодательное обеспечение борьбы с преступностью в киберпространстве, или страны имеют во многом устаревшие законы и механизмы их реализации. При этом понимание масштабов компьютерной преступности приводит к выводу, что справиться с угрозами возможно только совместными усилиями.

Построение деятельности правоохранительных структур на основе внедрения информационных технологий дает совершенно новые возможности для координации совместной деятельности в международном масштабе. Только совместная деятельность и межгосударственное сотрудничество способны эффективно противостоять преступности.

В настоящее время наблюдается осознанная тенденция к унификации законодательства и координации правоохранительной деятельности в мировом масштабе. Вопросы юрисдикции должны решается путем сотрудничества государств.

Универсальным регулятором в сфере борьбы с компьютерной преступностью могла бы стать отдельная Конвенция ООН о компьютерных преступлениях. Значение принятия такой Конвенции необычайно велико.

УДК 343

С.А. Шарапов

О ТЕНДЕНЦИЯХ КРИМИНАЛИЗАЦИИ ДЕЙСТВИЙ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ

В современных условиях практически каждый пользователь компьютера сталкивался с действием вредоносных программ. По данным «Лаборатории Касперского» в 2016 г. при серфинге в интернете атакам вредоносных объектов подверглись 31,9 % компьютеров пользователей. Разработанными указанной компанией программными средствами отражено свыше 758 млн атак, веб-антивирусом обнаружено более 69,2 млн уникальных детектируемых объектов.

Приведенные сведения указывают на значительную актуальность вопроса ответственности за использование вредоносного программного обеспечения и важности его разрешения для общества и государства. Между тем четкие критерии, по которым программы должны относится к категории вредоносных, на законодательном уровне не определены, что влечет за собой формирование противоречивой правоприменительной практики.

В настоящее время в научной литературе активно высказываются предложения о необходимости повышения криминализации как самого понятия «вредоносные программы», так и действий с ними. Например, К.Н. Евдокимов в опубликованной в 2013 г. монографии «Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты», рекомендованной для использования преподавателями, аспирантами, студентами, слушателями юридических вузов, сотрудниками правоохранительных органов, утверждает, что вредоносную компьютерную программу необходимо рассматривать в широком смысле «как любую компьютерную программу, приводящую к уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации без согласия и уведомления ее владельца (пользователя). Тем самым вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния и достижения вредных последствий, указанных в статье 273 УК Российской Федерации».

Кроме того, К.Н. Евдокимов предлагает «в число преступных действий включить такое деяние, как приобретение компьютерных программ либо иной компьютерной информации, заведомо предназначен-

ных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации» (аналогичное предложение в 2008 г. высказывалось Е.А. Маслаковой в диссертации на соискание ученой степени кандидата юридических наук «Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты»).

В 2016 г. Д.И. Макушев в статье «О совершенствовании объективной стороны состава преступления, предусмотренного ст. 273 УК Российской Федерации», поддерживая мнение своего научного руководителя – вышеупомянутого К.Н. Евдокимова, утверждает, что «даже поверхностный взгляд на диспозицию ст. 273 УК РФ позволяет сделать вывод об отсутствии наказания за приобретение преступниками вредоносного программного обеспечения». В этой связи он предлагает ввести уголовную ответственность за приобретение вредоносных программ вне зависимости от преступных целей и мотивов. По мнению данного автора, вредоносные компьютерные программы так же, как и оружие, наркотики, взрывчатые вещества, должны считаться предметами, запрещенными к свободному гражданскому обороту, поскольку наносят ущерб информационной безопасности и могут использоваться как орудие либо средство для совершения других компьютерных преступлений. При этом, описывая вредоносные программы, автор относит к их числу компьютерные вирусы (черви, троянские кони, логические бомбы и др.), что не вполне объективно, поскольку они не имеют механизма самовоспроизведения путем внедрения своего кода в другую программу. Указанный в статье результат действия вредоносной программы – «уход от уплаты налогов» также представляется невозможным, хотя схожий тезис приводится, например, в комментарии к Уголовному кодексу Российской Федерации под редакцией А.В. Бриллиантова. Безусловно, при уклонении от уплаты налогов в современных условиях используются средства компьютерной техники и соответствующее программное обеспечение, но можно ли его рассматривать в качестве вредоносного?

В ходе расследования уголовных дел в сфере экономики и в финансово-кредитной системе автор сталкивался со случаями, когда в целях уклонения от уплаты налогов производились определенные манипуляции в программе «1С: Бухгалтерия» (таким образом значительная часть доходов коммерческой структуры была сокрыта от налогообложения), а для хищения денежных средств бухгалтером предприятия вносились изменения в программу для начисления заработной платы работникам.

Такие действия виновных были квалифицированы по соответствующим статьям Уголовного кодекса Республики Беларусь: за уклонение от уплаты налогов было предъявлено обвинение по ст. 243, а за хищение – по ст. 211 УК Республики Беларусь). При этом дополнительная квалификация таких действий по статье за использование вредоносных программ не требуется, несмотря на то, что они действительно совершены с использованием компьютерной техники, соответствующего программного обеспечения и ими причинен вред.

Вышеописанные юридические толкования понятия «вредоносные программы» и предложения по введению уголовной ответственности за их приобретение представляются не вполне оправданными, поскольку приведут к излишней криминализации действий в информационной сфере.

По нашему мнению, вредоносная программа должна предназначаться только для противоправных действий. В этой связи предложение о возможности оценки какой-либо легальной, лицензионной программы как вредоносной, полагаем, является неверным, ибо так можно, например, оценить операционную систему, поскольку она всегда используется при совершении преступлений против информационной безопасности или хищений с использованием компьютерной техники.

Таким образом, необходимо различать (по крайней мере, с точки зрения уголовного права) компьютерные программы, которые могут использоваться для совершения противоправных деяний: они могут быть как легальными и лицензионными, так и сами по себе вредоносными, являющимися таковыми изначально.

В части предложения о введении уголовной ответственности за приобретение вредоносных программ, полагаем, что такая мера будет излишней и чрезмерной, поскольку такое деяние не обладает уровнем общественной опасности, присущей преступлению. А кроме того, действующий уголовный закон позволяет привлечь виновных к ответственности за приобретение таких программ, как за приготовление к преступлению, если установлен умысел в использовании их в противоправных целях.

С учетом изложенного представляется, что любые предложения по ужесточению уголовной ответственности как за преступления против информационной безопасности, так и за иные категории преступлений должны быть качественно и всесторонне проработаны, научно обоснованы не только с точки зрения необходимости и целесообразности, но и с точки зрения последствий их введения.

УДК 343.534(476)(043.3)

Н.А. Швед

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ТЕРМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ

В юридической литературе неоднократно указывалось на тот факт, что одним из существенных недостатков гл. 31 Уголовного кодекса Республики Беларусь является перегруженность ее узкоспециальными техническими терминами, которые законодатель не раскрывает в УК. Уяснение терминов, использованных при конструировании ст. 349–354 УК, требует от правоприменителя познаний в области не только уголовного права, но и компьютерной техники. В противном случае это может повлечь неоднозначное применение указанных норм на практике. В частности, хотелось бы остановиться более подробно на ст. 349 УК, устанавливающей ответственность за несанкционированный доступ к компьютерной информации.

В этой связи необходимо выяснить, что представляет собой несанкционированный доступ вообще и в каких случаях он признается преступлением, а также в чем заключается различие между несанкционированным и неправомерным доступом. Для начала проанализируем понятие «доступ к информации», являющееся составной частью рассматриваемого термина.

Закон Республики Беларусь «Об информации, информатизации и защите информации» раскрывает содержание понятия доступа к информации в ст. 1 как возможность получения информации и пользования ею. Практически идентичное определение содержится и в Федеральном законе «Об информации, информационных технологиях и о защите информации». Е.А. Миндрова, критикуя законодательное определение, считает, что понятие необоснованно расширено, так как к доступу относится правомочие использования полученной информации, т. е. в понятии «доступ к информации» смешаны возможности получения и распространения.

В научной литературе определения понятия доступа в основном, по сути, схожи с нормативными. Например, И.А. Клепицкий понимает под доступом к компьютерной информации приобретение и использование лицом возможности получать, вводить, изменять или уничтожать информацию либо влиять на процесс обработки. Однако есть и иные. Так, В.Г. Степанов-Егиянц считает, что под доступом к компьютерной информации следует понимать получение возможности обращения к компьютерной информации, в результате которого лицо получает правомочия обладателя информации.

На основании анализа нормативных и литературных источников можно выделить две существующие позиции относительно содержания понятия «доступ к информации»: 1) только полномочие на ознакомление с информацией; 2) полномочие на ознакомление и использование информации. При этом толкование содержания данных полномочий позволяет говорить о том, что ознакомление заключается в получении сведений, а использование – в извлечении из этих сведений пользы, применение их.

Представляется, что доступ к информации – это комплексное понятие, включающее в себя оба правомочия, поскольку они взаимосвязаны. Ознакомление, как правило, предполагает возможность дальнейшего использования информации, соответственно, прежде чем воспользоваться информацией, нужно сначала с ней ознакомиться. Возможность ознакомления с информацией без использования ее не представляет общественной опасности – информация должна быть воспринята.

Если обратиться к УК государств – участников СНГ, то можно заметить, что в России, Туркменистане, Азербайджане, Казахстане и Таджикистане такой доступ к информации именуется неправомерным, а в Беларуси, Узбекистане и Армении – несанкционированным. Н.Ф. Ахраменка считает предпочтительным использование прилагательного «неправомерный», которое характеризует сущностный, а не организационный признак доступа. М.Ю. Демьянович полагает, что доступ к компьютерной информации возможен только при наличии определенных законных полномочий, т. е. правового основания, поэтому правильно называть его неправомерным. В то же время некоторые российские авторы определяют неправомерный доступ как несанкционированное собственником информации ознакомление лица с данными (подобное используется в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации).

Заслуживающую внимания точку зрения высказывает Д.А. Овсюков, рассматривая такое условие как неправомерность. В частности, он отмечает, что при проведении DdoS-атаки доступ к сайту/серверу является именно правомерным. Такое право дает сам владелец сайта в соответствии с п. 1 ч. 3 ст. 6 Федерального закона «Об информации, информационных технологиях и о защите информации», разрешив доступ к информации на своем сайте/сервере для любого пользователя интернета (неограниченного круга лиц). Единственным различием между обычным доступом и DdoS-атакой является количество и частота подключений к серверу для получения информации. Таким об-

разом, сам доступ является правомерным, преступник при DdoS-атаке злоупотребляет предоставленным правом на доступ к сайту-жертве. В этой связи автор предлагает для надлежащей уголовно-правовой защиты от данного вида кибератак внести изменения в ст. 272 УК Российской Федерации, убрав из объективной стороны такое обстоятельство, как неправомерность доступа, заменив его признаками несанкционированности и умышленности в отношении последствий.

Т.Л. Тропина считает, что понятие неправомерного доступа является оценочным. Неправомерность может означать как несоответствие нормам права, так и совершение действия при отсутствии прав на его совершение. Автор также предлагает заменить термин «неправомерный» термином «несанкционированный».

В Положении о технической и криптографической защите информации в Республике Беларусь, утвержденном Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, несанкционированный доступ к информации определяется как доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа. В п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» разъясняется, что несанкционированным при хищении с использованием компьютерной техники считается доступ к компьютерной информации лица, не имеющего права на доступ к этой информации либо имеющего такое право, но осуществляющего его помимо установленного порядка. Кроме того, в технической литературе употребляется именно термин «несанкционированный доступ». Также прилагательное «несанкционированный» по отношению к доступу используется и в государственных стандартах.

На наш взгляд, несанкционированное ознакомление означает, что у лица нет ни прав на ознакомление с информацией, ни разрешения (санкции) владельца информации. Ведь ситуацию, когда у лица имеется право на доступ к информации, но такой доступ осуществлен помимо установленного порядка, относят к несанкционированному доступу. Поэтому считаем традиционное использование прилагательного «несанкционированный» более приемлемым.

Таким образом, несанкционированный доступ к компьютерной информации состоит из представленных в единстве получения и реализации возможности – ознакомления и использования указанной информации, сопряженных с нарушением системы ее защиты. При этом действие осуществляется лицом, не имеющим права на ознакомление с информацией либо имеющим такое право, но осуществляющим его с

нарушением установленного порядка. В предметно-содержательном аспекте несанкционированный доступ состоит из ознакомления с полученной информацией и из возможного затем ее использования, независимо от фактической реализации этой возможности. В организационно-управленческом аспекте несанкционированный доступ – это нарушение установленных правил и порядка доступа, связанных с системой защиты.

УДК 504.75.05

С.Л. Яблочников, И.О. Яблочникова, М.С. Яблочникова

АЛЬТЕРНАТИВНЫЙ ВЗГЛЯД НА ПРОБЛЕМЫ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Как правило, научные публикации в сфере обеспечения информационной безопасности в первую очередь касаются вопросов разработки методов и средств защиты информации от несанкционированного доступа к ней, ее искажения, уничтожения, модификации или же создания условий гарантированного доступа для определенного круга пользователей. Мероприятия, связанные с защитой информации, реализуются при ее приеме, передаче, хранении, обработке, визуализации и т. д. Таким образом, в качестве объектов, на защиту которых направлены соответствующие действия в рамках выработанной политики безопасности, рассматриваются либо некоторые информационные ресурсы, либо совокупность информационных процессов, осуществляемых в сложных технических системах. Также речь идет об обеспечении бесперебойного функционирования программно-технических комплексов, непосредственно реализующих указанные выше защищаемые информационные процессы.

Упомянутые сложные технические системы, существующие для обеспечения информационных процессов, в большинстве случаев являются человеко-машинными. Конечная цель функционирования таких систем – информационная поддержка производственной, экономической, технологической, социальной и иной деятельности отдельных личностей, определенных групп людей или же социума в целом. При этом общая логика совокупности действий в рамках обеспечения информационной безопасности такова: необходимо защитить информационные ресурсы или информационные процессы, которые человек (общество), в конечном счете, использует себе во благо.

Фактически мало кто из исследователей задумывается о том факте, что кроме негативных, несанкционированных воздействий (внешних и

внутренних по отношению к информационной системе, естественных и искусственных, преднамеренных и непреднамеренных) на информационные ресурсы, процессы и программно-технические средства, вполне реально существует целый ряд существенных угроз для отдельных личностей и социальных групп, возникающих вследствие их взаимодействия с информационными ресурсами, оборудованием, а также вольного или невольного участия в процессах передачи, приемки, хранения, отображения, обработки и синтеза информации. В некотором роде такой подход определяет альтернативную трактовку сущности основ информационной безопасности, вполне имеющую право на существование.

В последнее время в ряде публикаций высказывается мнение о необходимости активного формирования теоретических основ нового направления в науке – информационной экологии. Отправная точка для обоснования ее сущности – признание того факта, что помимо природной и социальной сред обитания человека объективно существует также информационная среда, являющаяся агрессивной по отношению к нему. Роль и значение такой среды в современном информационном обществе и в условиях реализации так называемой четвертой промышленной революции постоянно возрастает по мере дальнейшего развития компьютерных технологий, средств массовой информации и современных телекоммуникаций.

Информационная среда оказывает на человека весьма активное воздействие. Она существенно влияет (в том числе и негативно) на формирование и функционирование личности, на его духовное, интеллектуальное и психическое развитие, состояние психического и физического здоровья. Таким образом, при использовании упомянутого выше подхода к рассмотрению роли информационных ресурсов и информационных технологий объектом защиты становится человек и как достаточно сложная биологическая система, и как необъемлемая часть (социальная подсистема) другой сложной и глобальной системы – социума.

Смещение акцентов в сторону информационной безопасности непосредственно конкретного человека, а не совокупности современных средств обеспечения его продуктивной жизнедеятельности позволяет рассматривать обсуждаемую проблему несколько в ином ракурсе, как и саму информационную безопасность, в классическом ее понимании, в качестве составной части комплексной безопасности жизнедеятельности.

Также вполне понятен тезис о том, что перед человечеством стоит следующая дилемма: активное использование информационных ресурсов и информационных технологий для эффективного достижения определенных целей с обеспечением защиты информации и функционирования средств ее обработки или же обеспечение с наименьшими затратами комплексной безопасности жизнедеятельности человека в процессе решения им глобальных и локальных задач, возникающих перед ним. Все зависит от того, как именно будет трактоваться понятие «эффективность жизнедеятельности»: как максимизация объемов обработки информации и обусловленное этим максимальное извлечение некоторой выгоды (в том числе и финансовой) или же как некоторое достаточное для обеспечения эволюционного развития человечества информационное взаимодействие при минимизации рисков возникновения негативных последствий в настоящем и будущем.

По нашему мнению, социум со временем в качестве приоритетного изберет для себя путь развития, при котором минимизируются всевозможные риски и подлежат максимизации возможности сохранения и непрерывной эволюции человеческого потенциала. Обеспечение физического и психического здоровья отдельной личности и общества в целом является более важной и глобальной проблемой, чем создание некоторого валового продукта, который со временем, может быть, позволит решить указанную выше задачу наряду со многими остальными. Таким образом, создание теоретических основ информационной экологии – это в некотором роде попытка изменить парадигму эволюции общества.

РАЗДЕЛ 2

СОВРЕМЕННЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

В.М. Алефиренко

ОЦЕНКА КАЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ ТЕХНИЧЕСКИХ СРЕДСТВ АКУСТИЧЕСКОЙ РАЗВЕДКИ

Технические средства получения информации по акустическому каналу имеют двойное назначение. Они могут использоваться как злоумышленниками для несанкционированного получения информации, так и легитимными органами для обеспечения безопасности. Одним из таких средств является направленный микрофон, который позволяет получать акустическую информацию на достаточно больших расстояниях. Поэтому определенный интерес представляет оценка качественных показателей направленных микрофонов, на основании которой можно определить наиболее лучшую модель для санкционированного использования или сделать вывод, какую модель направленного микрофона наиболее вероятно используют злоумышленники, чтобы выбрать адекватные меры и средства противодействия.

Для оценки качественных показателей направленных микрофонов предлагается использовать комплексный метод оценки качества изделий, который предполагает использование следующих комплексных показателей:

средневзвешенный арифметический $$K_K = \sum_{i=1}^{m} \alpha_{Hi} K_{Hi}; \quad (1)$$

средневзвешенный геометрический $$K_K = \sqrt[m]{\prod_{i=1}^{m} K_{Hi}^{\alpha_{Hi}}}; \quad (2)$$

средневзвешенный гармонический $$K_K = \frac{\sum_{i=1}^{m} \alpha_{Hi}}{\sum_{i=1}^{m} \frac{\alpha_{Hi}}{K_{Hi}}}, \quad (3)$$

где K_{Hi} – нормированный i-й единичный показатель; α_{Hi} – нормированный коэффициент, характеризующий вес (значимость, важность) i-го единичного показателя; m – количество единичных показателей, принятых во внимание.

Для получения нормированных (безразмерных) значений единичных показателей K_{Hi} может использоваться следующее выражение

$$K_{Hi} = \frac{K_i - K_{кр\ i}}{K_{opt\ i} - K_{кр\ i}}, \quad (4)$$

где K_i – исходное значение i-го единичного показателя; $K_{кр\ i}$ – критическое значение i-го единичного показателя; $K_{opt\ i}$ – оптимальное значение i-го показателя.

Коэффициенты значимости α_{Hi} для выражений (1) – (3) должны выбираться, соответственно, таким образом, чтобы обеспечивалось одно из условий:

$$\sum_{i=1}^{m} \alpha_{Hi} = 1; \quad \prod_{i=1}^{m} \alpha_{Hi} = 1. \quad (5)$$

В качестве единичных показателей использовались технические характеристики направленных микрофонов, представленные в справочно-рекламной литературе и на интернет-сайтах. После изучения особенностей и характеристик направленных микрофонов различных фирм для расчетов было отобрано 13 моделей: «Вереск», «НМ-СН», «ОДМ-01», «ОВМ-01», «НСМ-003», «CCS», «Супер Ухо-100», «Yukon», «Кейс», «АТ-89», «YKN», «UEM-88», «МП».

В качестве единичных показателей были выбраны следующие основные характеристики направленных микрофонов: диапазон рабочих частот, дальность действия, ширина диаграммы направленности, коэффициент усиления, наличие ветрозащищенности, габаритные размеры, вес.

Для оценки комплексных показателей качества направленных микрофонов необходимо выполнить следующие действия: провести преобразование параметров, выраженных несколькими числовыми значениями, в параметры, выраженные одним числовым значением (диапазон рабочих частот); выразить качественные значения параметров числовыми значениями (наличие ветрозащищенности); определить численные значения параметров моделей, по которым отсутствует информация в источниках; назначить параметрам коэффициенты значимости; выбрать значения параметров для нормирования; провести нормирование значений параметров по формуле (4); провести нормирова-

ние значений коэффициентов значимости с учетом выражений (5); провести расчет комплексных показателей качества по формулам (1) – (3); провести анализ и оценку полученных результатов.

Результаты расчетов комплексных показателей качества, проведенные для каждой модели направленного микрофона, представлены в таблице.

Таблица

Результаты расчетов комплексных показателей качества направленных микрофонов

Модель микрофона	Место	Сумма мест	Средневзвешенные показатели качества		
			арифметический	геометрический	гармонический
Вереск	2	6	0,59	0,42	0,26
НМ-СН	9–10	28	0,52	0,31	0,16
ОДМ-01	12	33	0,50	0,14	0,007
ОВМ-01	3–4	11	0,57	0,39	0,25
НСМ-003	3–4	11	0,52	0,39	0,26
CCS	11	32	0,47	0,28	0,18
Супер Ухо-100	9–10	28	0,47	0,31	0,22
Yukon	5	15	0,56	0,39	0,24
Кейс	13	38	0,25	0,06	0,008
АТ-89	6	19	0,48	0,35	0,26
YKN	8	26	0,48	0,32	0,22
UEM-88	7	22	0,52	0,34	0,20
МП	1	4	0,58	0,42	0,28

Как видно из таблицы, первые три места по комплексным показателям и по сумме мест занимают направленные микрофоны «МП», «Вереск», «ОВМ-01» и «НСМ-003».

Следует отметить, что использование численных значений комплексных показателей качества позволяет проводить только предварительную оценку уровня качества технических средств акустической разведки с целью дальнейшего принятия решения о его использовании. При этом если по каким-либо причинам модель с наивысшим показателем качества не может быть использована (например, модель имеет значение какого-либо параметра ниже требуемого или модель отсутствует в продаже), то по полученным значениям может быть выбрана другая модель с требуемым значением данного параметра и максимальным значением комплексного показателя среди остальных моделей с такими же значениями этого параметра.

УДК 519.876

Н.М. Бобович

МЕТОД МОДЕЛИРОВАНИЯ СТРУКТУРЫ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В докладе рассматривается задача математического моделирования структуры критически важных объектов информатизации для количественного анализа устойчивости функционирования и управления ею с использованием метода сопряжения случайных структур (систем) по производительности.

Современные критически важные объекты информатизации (КВОИ) принадлежат к широкому классу систем, обладающих целенаправленным поведением. В процессе функционирования вследствие воздействия дестабилизирующих факторов и изменения состояния отдельных элементов система фактически претерпевает случайные изменения своей структуры. Поэтому структурная устойчивость объекта к воздействию дестабилизирующих факторов представляет наибольший интерес при практическом изучении и создании моделей сложных систем в задачах количественного анализа их устойчивости функционирования.

Общей особенностью количественной оценки показателей устойчивости функционировании является статистический характер оцениваемых показателей на всех иерархических уровнях: элемент – подсистема – система в целом. Возможность представления производительности на высших уровнях в виде операторов сопряжения, представляющих собой ее функциональную зависимость от производительностей на более низких уровнях, позволяет свести задачу количественной оценки устойчивости функционирования по показателю «производительность» к задачам расчета статистических характеристик функций случайных аргументов.

Сложность и громоздкость функциональных зависимостей между производительностями элементов и образуемыми ими реальными системами существенно затрудняет прямое решение задачи. Поэтому предлагается использовать метод сопряжения случайных структур (систем) по производительности.

Использование метода анализа случайных структур (систем) по производительности для анализа сложных структур, расчета материального и функционального ущербов, показателя устойчивости функционирования КВОИ основывается на разработке следующего комплекса математических моделей: пространственно-временной модели объекта, структурно-функциональной модели объекта, пространственно-временной модели воздействий, модели потерь, модели восстановления, модели управления.

Среди перечисленных моделей особое место в анализе устойчивости функционирования занимает структурно-функциональная модель КВОИ, методика разработки и особенности, использования которой рассматриваются ниже.

Структурно-функциональная модель имеет многоуровневую систему отображения, одинаковую по математической структуре на всех уровнях. При переходе от уровня к уровню подсистема низшего уровня принимается элементом на следующем за ним уровне. Многоуровневая система может преобразовываться в одноуровневую путем развертывания подсистем каждого уровня до элементов самого низкого уровня.

Структурно-функциональная модель представляет собой аналитический алгоритм вычисления производительности системы через производительности входящих в него элементов. Разработанная для исследований устойчивости модель имеет графическую форму представления аналитического алгоритма.

Данная модель строится на основе двух элементарных структур:

бесструктурная совокупность (элементарное звено) – объединение однотипных взаимозаменяемых элементов. Оператор сопряжения по производительности – суммирование производительностей объединяемых элементов;

элементарная цепь – объединение невзаимозаменяемых элементов, каждый из которых абсолютно необходим для функционирования структуры. Оператором сопряжения по производительности является выбор элемента с наименьшей производительностью.

В исходном состоянии, характеризующем отсутствие воздействий, структура системы является неслучайной и оптимизирована по расстановке кадров и использованию технических средств.

На рисунке приведена структурно-функциональная модель элемента КВОИ, построенная по изложенным принципам.

Структурно-функциональная схема системы

Алгоритм вычисления производительности системы имеет вид

$$I = \min\{[\min(I_1, I_2 + I_3) + \min(I_4, I_5), I_6]\}.$$

Таким образом, метод представления системы в виде совокупности последовательно-параллельных связей между элементами позволяет установить взаимно-однозначное соответствие между аналитическим выражением оператора сопряжения и его графическим отображением и тем самым дает возможность упростить как задачу записи алгоритмов вычисления производительности, так и расчет ее статистических характеристик. Кроме того, такое представление в ряде случаев позволяет анализировать влияние структуры на устойчивость функционирования системы непосредственно, без ее количественных показателей.

УДК 004.056.5:004.75

Е.А. Дрыбин, В.С. Садов

ПРИМЕНЕНИЕ МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ В СОВРЕМЕННЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Стеганография как способ сокрытия информации используется с момента появления письменности и необходимости передачи секретных сообщений, и наряду с популяризацией средств обмена информацией с использованием компьютерных сетей передачи данных и глобальной сети Интернет растет востребованность стеганографических методов защиты конфиденциальных данных.

Текстовая стеганография предполагает использование текстового контейнера для сокрытия в нем секретного сообщения (в текстовом представлении или каком-либо ином виде). Использование кода HTML какой-либо веб-страницы в качестве текстового контейнера делает обнаружение секретного сообщения практически невозможным, поскольку веб-страницы с использованием гипертекстовой разметки являются фундаментальными строительными блоками глобальной сети Интернет.

Настоящие тезисы рассматривают общие принципы, которые лежат в основе большинства методов сокрытия информации в коде веб-страниц, написанном с использованием языков HTML и CSS.

Методы текстовой стеганографии.

Выборочное сокрытие. Символы секретного сообщения скрывают в одном из символов слов контейнера (в первом или любом предопределенном месте). Объединение этих символов позволяет извлечь скрытый текст. Для использования этого метода требуется большое количество обычного текста, который будет выступать в роли контейнера.

Веб-страницы HTML. Так как атрибуты тегов HTML не чувствительны к регистру, эти символы можно использовать для сокрытия и извлечения исходного текста.

Сокрытие с использованием пробелов. Биты исходного сообщения определяются количеством пробелов в стего, например меньшее количество пробелов может указывать на 0 и большее количество пробелов между словами может определять 1.

Семантическое сокрытие. Используются синонимы, чтобы скрыть исходное сообщение.

Два основных фактора определяют эффективность методов текстовой стеганографии с использованием HTML-страниц в качестве контейнера:

веб-страницы присутствуют в сети Интернет в огромном количестве, и обнаружить конкретную страницу, содержащую скрытую информацию, практически невозможно;

порядок тегов HTML, используемых для форматирования внешнего вида веб-страницы, не имеет значения, что может помочь скрыть один бит сообщения за тегами.

Текстовая стеганография с использованием HTML-документов.

Основная сложность в применении текстовой стеганографии заключается в присутствии в текстовых документах значительно меньшего количества избыточной информации в сравнении с изображениями или аудио. Теги HTML не чувствительны к регистру, т. е. <html>, <HTML> или <hTmL> определят абсолютно идентичный внешний вид документа. Биты сообщения могут быть скрыты в тегах путем изменения регистра символов (в зависимости от значения бита исходного сообщения). Кроме того, порядок следования атрибутов HTML также не влияет на внешний вид или другие характеристики веб-страницы.

Алгоритм встраивания сообщения в произвольный HTML-документ можно разделить на четыре шага.

Исходный текст необходимо зашифровать и затем преобразовать в двоичную форму представления.

Для генерации ключевого файла необходимо представить ключевые комбинации тегов выбранного HTML-документа (состоят из первичного и вторичного атрибутов) в виде строк и столбцов. Порядок расположения первичных и вторичных атрибутов в стего может скрывать один бит данных. Для всех пар атрибутов, которые встречаются в выбранном HTML-файле, определяется первичный и вторичный атрибут (любой атрибут может выступать в качестве первичного), выбирается ключевая комбинация. Правильный порядок расположения атрибутов в стего указывает на бит 1, обратный порядок расположения тегов указывает на бит 0.

После создания ключевого файла скрытое сообщение может быть встроено в произвольный HTML-документ путем нахождения ключевых комбинаций (пар HTML-тегов) и изменения в случае необходимости их взаимного расположения в соответствии с битами исходного сообщения.

Извлечение сообщения представляет собой обратный встраиванию процесс. Для каждой комбинации первичных и вторичных атрибутов определяют порядок при помощи ключевого файла и, сравнивая его со стего, извлекают биты исходного сообщения.

Безопасная текстовая стеганография с использованием криптографических систем с открытым ключом.

В основе метода лежит сокрытие текста в CSS-части веб-страницы с использованием свойств атрибута конца строки (EOL). В обмене участвуют две стороны. Получатель выполняет генерацию пары открытых и закрытых ключей с использованием схемы шифрования RSA. Открытый ключ передается другому участнику обмена, т. е. отправителю. Отправитель шифрует исходный текст, используя открытый ключ. Зашифрованное сообщение преобразуется в двоичную форму, которая будет встроена в содержимое веб-страницы следующим образом: в коде CSS находится точка с запятой (символ EOL), после которой дописывается пробел для битов со значением 1 или символ табуляции для битов со значением 0. Процесс извлечения требует выявления последовательности встроенных битов и ее расшифровки с использованием секретного ключа получателя.

Тезисы рассматривают некоторые методы текстовой стеганографии, которые могут применяться в современных сетях передачи данных и в глобальной сети Интернет для скрытого обмена секретными сообщениями. Сегодня стеганографические методы защиты информации все более востребованы физическими и юридическими лицами, в частности в странах, в которых использование средств криптографии регулируется на законодательном уровне.

Приведенные выше методы сокрытия информации в содержании веб-страниц являются очень эффективными с точки зрения вероятности обнаружения, поскольку веб-страницы, построенные с использованием технологий HTML и CSS, присутствуют в сети Интернет в огромном количестве. Безопасность информационного обмена также можно усилить за счет сокрытия сообщения в CSS-коде, поскольку листы каскадного стиля используются для форматирования и управления внешним видом веб-страниц. Кроме того, код CSS не виден со стороны клиента, что также увеличивает уровень защищенности информационного обмена с использованием кода CSS в качестве стеганографического контейнера.

УДК 004.934.056.5(083.74)(476)

П.П. Изотов, И.В. Муринов, А.М. Хананов

УСТРОЙСТВО ПАССИВНОЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ЦИФРОВЫХ ТЕЛЕФОННЫХ АППАРАТОВ ОТ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ И ВЫСОКОЧАСТОТНОГО НАВЯЗЫВАНИЯ

Во многих государственных и коммерческих организациях Республики Беларусь используются автоматические телефонные станции (АТС) с цифровыми телефонными аппаратами. Для обеспечения информационной безопасности в этих организациях необходимы устройства технической защиты цифровых телефонных аппаратов от утечки речевой информации по двухпроводным и четырехпроводным цифровым телефонным линиям путем акустоэлектрического преобразования и высокочастотного навязывания.

Имеющиеся устройства защиты для аналоговых телефонных аппаратов (например, «Гранит-8» – устройство защиты для аналоговой двухпроводной телефонной линии) позволяют осуществить защиту от утечки речевой информации в аналоговых телефонных линиях, но не могут быть использованы для цифровых линий, так как мешают работе цифровых телефонных аппаратов.

Имеющиеся устройства защиты для цифровых телефонных аппаратов (например, «Гвард», «МП-1Ц», «Топаз-ЦТ» – устройства защиты для цифровой двухпроводной телефонной линии) позволяют осуществить защиту от утечки речевой информации, но имеют свои особенности в работе.

В устройстве «Гвард» для перехода в режим защиты необходимо кнопкой отключить цепи микрофона и громкоговорителя от телефонного аппарата, а при разговоре по телефону подключить их обратно.

«МП-1Ц» является устройством активной технической защиты, т. е. в его состав входит шумогенератор, который выдает в цифровую телефонную линию определенный уровень шума, а при разговоре (трубка поднята) шумогенератор выключается. Выключение шумогенератора устройством происходит тогда, когда уменьшается напряжение питания в телефонной линии, что, как предполагается, должно происходить при поднятии телефонной трубки. Однако в цифровых телефонах Samsung (DS-5021D) и Panasonic (KX-DT321RU) при поднятии телефонной трубки напряжение питание телефона в линии не меняется и шумогенератор не выключается, что мешает работе цифрового телефона.

«Топаз-ЦТ» является устройством активной технической защиты, которое выдает в цифровую телефонную линию определенный уровень шума непрерывно, что также приводит к сбоям в работе в цифровых телефонах Samsung и Panasonic.

Как видно из вышеизложенного, для защиты двухпроводных цифровых телефонных аппаратов необходимо устройство, не оказывающее влияния на работу цифровых телефонных аппаратов, т. е. реализующее пассивные методы защиты. Согласно действующим техническим нормативным правовым актам пассивным методом защиты является подавление несущей частоты сигнала высокочастотного навязывания, или подавление информативного низкочастотного сигнала, или подавление результатов преобразования сигнала высокочастотного навязывания и информативного низкочастотного сигнала, или использование их в комбинации.

Для создания такого устройства были сформулированы следующие основные технические требования по назначению:

1. Устройство защиты не должно влиять на работу цифрового телефонного аппарата.

2. Устройство защиты должно обеспечивать в необходимом широком диапазоне частот высокую степень подавления сигналов. (Выполнение этого требования осложнено тем, что частоты информационных сигналов в цифровых АТС и телефонных аппаратах лежат в этом же диапазоне, и не могут быть отфильтрованы (подавлены). К тому же, построение схем ограничителей напряжения на пассивных элементах не обеспечивает высокую степень подавления сигналов ВЧ-навязывания.)

3. Электрическое питание устройства защиты должно осуществляться от сети 220 В, и устройство защиты должно формировать напряжение питания для цифрового телефонного аппарата.

С учетом технических требований устройство защиты было построено так, чтобы ослаблять сигнал со среднеквадратичным значением напряжения 0,1 В и ниже, даже при смещении этого сигнала положительным или отрицательным напряжением. Сигнал больше 0,1 В пропускается на выход в виде трех уровней напряжения: положительного, нулевого и отрицательного. Величина этих уровней зависит от типа АТС: для АТС Samsung +1,5; 0; -1,5 В; для АТС Panasonic +4; 0; -4 В.

Для построения устройства защиты используются активные элементы и источник питания. На рис. 1 представлена структурная схема устройства защиты без блока питания, где СП – согласующий преобразователь с цифровой двухпроводной телефонной линией связи; ВЧФ – высокочастотный фильтр; ПУ – преобразователь уровней; Кл – ключ отключения/включения канала передачи данных; УУК – устройство управления каналами передачи данных.

Как видно из рис. 1, устройство защиты состоит из двух каналов: канала передачи данных от АТС к цифровому телефону (ЦТ) и канала передачи данных от ЦТ к АТС. Объединяют эти два канала два СП: один со стороны АТС, второй со стороны ЦТ. Переключение каналов происходит поочередно таким образом, чтобы обеспечить прохожде-

ния информационного сигнала от АТС к ЦТ и от ЦТ к АТС, не оказывая влияния на работу ЦТ и АТС.

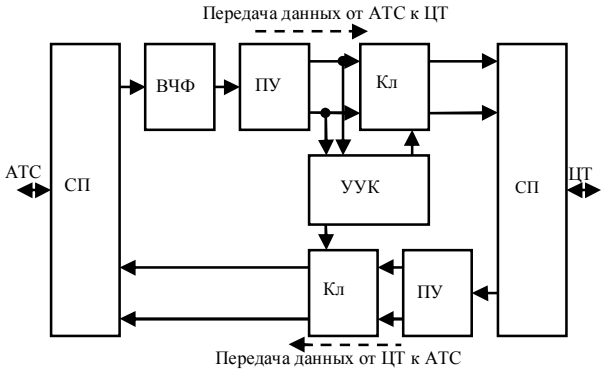

Рис. 1. Структурная схема устройства пассивной технической защиты цифровых телефонных аппаратов

В канал входят ПУ и Кл. ПУ отделяет положительное напряжение от отрицательного (рис. 2 б, в, г). Кл предназначен для переключения каналов и управляется УУК, которое синхронизируется от сигнала АТС.

Если сигнала АТС нет, то открыт канал от АТС к ЦТ, а второй канал закрыт. Это связано с тем, что передачу данных первой начинает АТС, а затем отвечает ЦТ. СП формирует из двух сигналов ПУ (рис. 2 в, г) выходной сигнал с тремя уровнями (рис. 2 д).

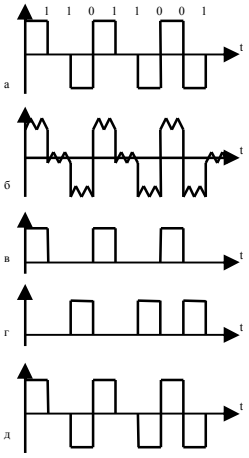

Рис. 2. Цифровой сигнал:
а – без помех (сверху – соответствующий сигналу бинарный код);
б – с помехой (вход ПУ);
в – и *г* – с помехой на выходе ПУ;
д – с помехой на выходе устройства защиты

На рис. 3 представлен внешний вид устройства пассивной технической защиты цифровых телефонных аппаратов.

Рис. 3. Внешний вид устройства пассивной технической защиты цифровых телефонных аппаратов

Опытная партия устройств защиты изготовлена в Гомельском филиале Научно-исследовательского института технической защиты информации и проходит сертификацию. Устройство защиты предназначено для работы с цифровыми телефонами Panasonic (KX-DT321RU и др.) и АТС KX-TDE600, KX-TDA100, 200 и др., в состав которых входит плата для работы с двухпроводными цифровыми телефонами KX-TDA0172. Устройство защиты изготавливается и для работы с цифровыми телефонами Samsung (DS-5021D и др.) и АТС iDCS 500 и др., в состав которых входит модуль расширения для работы с двухпроводными цифровыми телефонами 8DLI, 16DLI.

УДК 004.42

Е.М. Клачкевич, Р.В. Кислинский

СОВРЕМЕННЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Информация сегодня – важный ресурс, потеря которого чревата неприятными последствиями. Утрата конфиденциальных данных компании несет в себе угрозы финансовых потерь, поскольку полученной информацией могут воспользоваться конкуренты или злоумышленники. Для предотвращения столь нежелательных ситуаций все фирмы, учреждения используют методы защиты информации.

Безопасность информационных систем (ИС) как учебную дисциплину изучают программисты и специалисты в области построения ИС. Однако знать виды информационных угроз и технологии защиты должны все, кто работает с секретными данными.

Основным видом информационных угроз, для защиты от которых на каждом предприятии разрабатывается целая технология, является

несанкционированный доступ злоумышленников к данным. Злоумышленники планируют заранее преступные действия, которые могут осуществлять путем прямого доступа к устройствам или путем удаленной атаки с использованием специально разработанных для кражи информации программ.

Кроме действий хакеров, фирмы нередко сталкиваются с ситуациями потери информации по причине нарушения работы программно-технических средств. В данном случае секретные материалы не попадают в руки злоумышленников, однако утрачиваются и не подлежат восстановлению либо восстанавливаются слишком долго. Сбои в компьютерных системах могут возникать по следующим причинам: потеря информации вследствие повреждения носителей – жестких дисков, ошибки в работе программных средств, нарушения в работе аппаратных средств из-за повреждения или износа.

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется семь основных методов (способов) защиты: препятствие, маскировка, механизмы шифрования, регламентация, управление доступом, принуждение, побуждение. Все перечисленные методы нацелены на построение эффективной технологии защиты информации, благодаря которой исключаются потери по причине халатности персонала и успешно отражаются разные виды угроз.

Под препятствием подразумевается способ физической защиты информационных систем, который не позволяет злоумышленникам попасть на охраняемую территорию.

Маскировка как способ защиты информации предусматривает преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Механизмы шифрования – криптографическое закрытие информации. Этот метод защиты все шире применяется как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Управление доступом регулирует использование всех ресурсов ИС и информационных технологий и противостоит несанкционированному доступу к информации на всех возможных путях. Управление доступом включает следующие функции защиты:

идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

разрешение и создание условий работы в пределах установленного регламента;

регистрацию (протоколирование) обращений к защищаемым ресурсам;

реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т. п.) при попытках несанкционированных действий.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение как метод защиты обязывает пользователей и персонал ИС соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений используются следующие средства: физические, программные и аппаратные, организационные, законодательные, психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основными и наиболее старыми средствами физического препятствия являются прочные двери, надежные замки, решетки на окнах. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства защиты используются для охраны данных как на бумажных, так и на электронных носителях.

Программные и аппаратные средства – незаменимый компонент обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства – программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко

выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства защиты – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации. В Республике Беларусь в этом направлении активно ведется работа, результатом которой является Закон Республики Беларусь «Об информации, информатизации и защите информации».

Психологические средства защиты – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

Таким образом, мы можем сделать вывод, что защита информации является актуальной проблемой, особенно для силовых структур, так как попавшая «не в те руки» информация (даже не военного характера) может нести угрозу. Именно по этой причине было разработано много способов и средств защиты информации.

В заключение хотелось бы вспомнить выражение «Кто владеет информацией – владеет миром», так как в последнее десятилетие информация стала одним из самых ценных ресурсов.

УДК 681.3.05

А.Н. Коваленко

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ РАДИОЛУЧЕВЫХ СРЕДСТВ ОБНАРУЖЕНИЯ

Радиолучевыми средствами обнаружения (РЛСО) называют двухпозиционные датчики, в которых передатчик и приемник конструктивно размещены в различных устройствах с целью получения информации о нахождении в электромагнитном поле этих устройств перемещающегося объекта обнаружения.

Физический принцип функционирования радиолучевых средств обнаружения основан на преобразовании в сигнал тревоги изменений параметров электромагнитного поля на входе приемного устройства при появлении нарушителя в зоне обнаружения.

Передающее устройство (ПРД) генерирует электромагнитное поле сверхвысокой частоты и в виде радиоволн излучает его в сторону приемного устройства (ПРМ). Излучение производится в виде радиоимпульсов, имеющих постоянную амплитуду и частоту следования. Таким образом, в пространстве между передающим и приемным устройствами РЛСО создается зона обнаружения. Приемное устройство принимает радиоимпульсы, поступающие от передающего устройства, и осуществляет их обработку. До появления нарушителя в зоне обнаружения амплитуда принимаемых радиоволн практически постоянна. Сигнал тревоги РЛСО не подает.

Когда в зону обнаружения входит нарушитель, то в антенну ПРМ поступают дополнительные, отраженные от нарушителя радиоволны (рис. 1). В приемной антенне отраженные и прямые радиоволны либо складываются, либо вычитаются – все зависит от разности хода прямых и отраженных волн. Если разность хода радиоволн равна нечетному числу полуволн, то результирующая амплитуда радиоимпульса максимально уменьшается. Можно доказать, что в зоне обнаружения существуют области пространства, в которых появление нарушителя приводит к увеличению результирующей амплитуды. С ними соседствуют области, в которых нарушитель уменьшает результативную амплитуду. При идеально проводящей поверхности почвы и при отсутствии предметов на местности эти области имели бы форму чередующихся полуколец, как показано на рис. 1. В реальных условиях эта картина оказывается искаженной, но общая закономерность сохраняется.

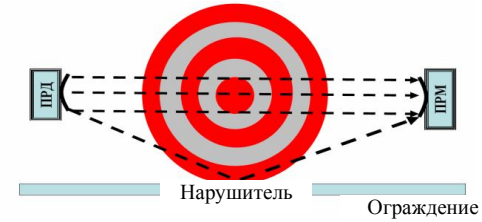

Рис. 1. Ход радиолучей между передающим и приемным устройством

Из приведенных рассуждений очевидно, что на пути нарушителя у границы зоны обнаружения может оказаться любая из указанных областей. Следовательно, амплитуда результирующих радиоимпульсов в приемной антенне с появлением нарушителя в зоне обнаружения может либо увеличиваться, либо уменьшаться. Изменения амплитуды радиоимпульсов в приемной антенне и является первичным электрическим сигналом о входе нарушителя в зону обнаружения.

Опыт эксплуатации радиолучевых средств обнаружения показывает, что для них характерна некоторая неустойчивость работы, которая проявляется в пропуске нарушителя без выдачи сигнала «Тревога» на отдельных участках зоны обнаружения.

Исследования позволяют сделать предположение, что основными причинами неустойчивой работы является нестабильность, изменчивость конфигурации зоны обнаружения и ее возможные искажения.

Форма зоны обнаружения зависит от направленных свойств передающей и приемной антенн и характеризуется их диаграммой направленности. На вид диаграммы направленности влияют отражения радиоволн от поверхности земли и ограждения, что приводит к ее изрезанности. Поэтому практические исследования были начаты с измерения диаграммы направленности и изучения характера ее искажений, приводящих к неустойчивой работе датчика. Экспериментальные данные свидетельствуют о том, что в сторону приемного устройства РЛСО может быть в один период времени направлен максимум излучения, а в другой – минимум:

$$E\max = \frac{r\cdot(2n+1)}{4h_1} \qquad (1)$$

$$E\min = \frac{r\cdot 2n}{4h_1}, \qquad (2)$$

где r – расстояние между приемником и передатчиком; n = 0, 1, 2…; h_1 – высота установки передатчика.

В результате этого уровень мощности поступающих в приемную антенну электромагнитных колебаний не является постоянным и изменяется в широком диапазоне, изменяется также в значительных пределах уровень поступающих в приемник сигналов. А при минимальном уровне сигналов средство обнаружения может работать неустойчиво, что и становится причиной пропуска нарушителя без выдачи сигнала «Тревога».

На рис. 2 показана зависимость направленности излучающей антенны РЛСО от диэлектрических свойств поверхности. Диэлектрическая проницаемость песка в сухую и сырую погоду соотносится как 1:10.

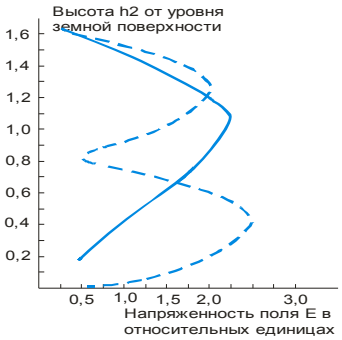

Рис. 2. Диаграмма направленности излучающей антенны РЛСО:
сплошная линия – значение в сухую погоду;
пунктирная линия – значение в сырую погоду;
h_2 – высота установки приемной антенны (от уровня земной поверхности)

Для повышения устойчивости работы датчика обнаружения требуется повысить средний уровень мощности сигналов и сосредоточить наиболее возможный поток энергии электромагнитного излучения от передающего устройства в приемник. Это достигается путем направления в сторону приемной антенны наиболее устойчивого лепестка диаграммы. Таким лепестком является самый нижний лепесток диаграммы излучения при горизонтальной поляризации волны, который благодаря явлению интерференции прямого луча с отраженным от поверхности земли сильно прижат к земле и может смещаться только вверх при любом изменении погодных условий.

Полученные характеристики направленности излучающей антенны дают возможность повысить эффективность применения существующих РЛСО.

УДК 004.056

В.В. Маликов, М.А. Бабич, Е.О. Перхальский

АКТУАЛЬНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В настоящее время, как правило, главными экономическими активами компаний и государств являются объекты интеллектуальной собственности, полученные в результате интеллектуальной деятельности, на которую затрачены значительные материальные и финансовые ресурсы. Несанкционированный доступ к таким активам приводит к их краже, что негативно влияет на экономику страны и приводит к банкротству компаний.

Обеспечение защиты от утечки конфиденциальной информации является сложной и многоуровневой задачей, которая включает в себя разграничение уровней доступа у сотрудников, составление документов о неразглашении, постоянное обучение сотрудников, внедрение технических средств и систем защиты информации.

Внедрение и использование DLP-системы позволяет эффективно автоматизировать ряд задач по защите конфиденциальной информации от утечки по технических каналам. Под DLP-системой (Data Loss Prevention) будем понимать программно-аппаратный комплекс, предназначенный для предотвращения утечек конфиденциальной информации за пределы корпоративной системы/сети на основе анализа потоков и входящих/выходящих данных.

Современная DLP-система, как правило, состоит из нескольких модулей, функционирующих на выделенных серверах, на рабочих местах

сотрудников компании (персональные компьютеры, рабочие станции и т. д.), а также на специализированных рабочих станциях службы безопасности.

Для оценки эффективности была выбрана DLP-система SecureTower российской компании Falcongaze, которая представляет собой программный продукт, позволяющий решать задачи по защите конфиденциальной информации от утечки по технических каналам.

В рамках исследования эффективности проведено:

1. Тестирование программной среды функционирования DLP-системы на предмет поддерживаемых операционных систем (ОС) (табл. 1). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО VMware Workstation Pro).

Таблица 1

Программная среда функционирования DLP-системы

Структурный компонент для инсталляции DLP-системы	Оперативная система	Результат тестирования
Серверное оборудование	Microsoft Windows Server 2008/2012/2016 (x64)	Соответствует заявленным данным
Клиентская часть (работа с консолью)	Microsoft Windows Vista/7/8/10/2008/2012/2016 (x86/x64)	Соответствует заявленным данным
Конечные точки (для агентской схемы)	Microsoft Windows XP SP3/Vista/7/8/10/Server 2003/2008/2012/2016 (x86/x64)	Соответствует заявленным данным

2. Тестирование эффективности перехвата данных DLP-системой в приложениях, использующих протоколы POP3, SMTP, HTTP и др. (табл. 2). Назначение портов приложений использовалось по умолчанию. Эффективность перехвата оценивалась в процентах от детекции сформированных тестовых баз из 20 файлов, сообщений в 2 режимах DLP-системы (настройки по умолчанию/специальная настройка параметров). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО VMware Workstation Pro).

3. Тестирование эффективности DLP-системой выявления стеганографических технологий модификации файлов (табл. 3). В качестве эксперимента 2 тестовых файла (формат doc, rar; объем до 50 КБ) с конфиденциальной информацией встраивались в файл-контейнер (формат png, jpg, pdf) с использованием стеганографического ПО OpenPuff (v.4.00, настройки качества по умолчанию, LSB-метод). Эффективность оценивалась в процентах от детекции сформированной тестовой базы из

6 файлов. Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО VMware Workstation Pro).

Таблица 2

Эффективность перехвата данных DLP-системой

Протокол	Порт (по умолчанию)	Поддержка протокола	Эффективность перехвата, файла, сообщения, %	
			настройки по умолчанию	с настройкой параметров
POP3	110	да	90	95
SMTP	25	да	95	100
IMAP	143, 993	да	90	95
OSCAR	5190	да	90	95
HTTP	80, 8080	да	95	100
FTP	20, 21	да	90	95
XMPP	5222	да	95	100
Mail.Ru Агент	2041, 2042, 443	да	95	100
Yahoo	23,80	да	95	100
MAPI	1024-65535	да	90	100

Таблица 3

Эффективность выявления стеганографических технологий модификации файлов DLP-системы

Технология детектирования DLP-системы	Эффективность, %
«Цифровой отпечаток» (Digital Fingerprints)	0
Контрольная сумма (хэш)	0

На основании проведенного исследования эффективности работы DLP-системы по защите конфиденциальной информации от утечки по технических каналам можно сделать следующие выводы.

1. Программная среда функционирования DLP-системы SecureTower компании Falcongaze поддерживает все основные ОС семейства Windows корпорации Microsoft.

2. Внедрение и использование DLP-системы позволяет эффективно автоматизировать задачи по защите конфиденциальной информации от утечки по технических каналам. Эффективность перехвата данных DLP-системой по заданному перечню протоколов и портов составила от 90 до 100 %.

3. Использование DLP-системы не позволяет детектировать стеганографические технологии модификации файлов.

УДК 004.056

А.Р. Мацылевич

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СЕТИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ КАК ОБЪЕКТ УПРАВЛЕНИЯ

Среди информационных сетей различного назначения можно выделить информационные сети специального назначения (ИССН), которые функционируют в интересах ведомств и органов, входящих в состав сил обеспечения национальной безопасности Республики Беларусь. Специфика ИССН определена назначением, условиями функционирования, природой угроз безопасности информации, а также тяжестью последствий их реализации. Реализация данных угроз может нанести ущерб не только владельцу ИССН, но и национальной безопасности Республики Беларусь.

В своем развитии информационные системы и сети, в том числе ИССН, достигли такого уровня, что человек по своим психофизиологическим возможностям уже не в состоянии адекватно и оперативно противодействовать угрозам безопасности информации, существенно снижая эффективность защиты информации. Необходимость использования ресурсоемких интерфейсов («машина – человек – машина») обуславливает зависимость процессов защиты информации от таких характеристик человека, как мотивация, профессиональная подготовленность, усталость, отвлеченность, эмоциональность и др., которые могут способствовать блокированию системы защиты информации в ИССН (влияние так называемого человеческого фактора). Более того, неквалифицированные действия человека по управлению защитой информации являются внутренней угрозой безопасности информации в ИССН.

Максимально возможное исключение человеческого фактора из процессов защиты информации достигается при применении программно-технических средств, реализующих функции управления защитой информации (средства и системы управления защитой информации). Автоматизация процессов управления защитой информации позволяет наиболее эффективно решать задачи как единого управления защитой информации, так и защиты информации в ИССН.

В настоящее время концептуально и методологически наиболее изучены вопросы применения средств защиты информации, в меньшей мере вопросы применения средств контроля эффективности защиты информации. Концептуальные положения создания и применения средств управления защитой информации и, более того, систем автоматизированного управления защитой информации в ИССН разработаны недостаточно полно.

ИССН являются сложными организационно-техническими системами, в которых объединены элементы различной природы (антропогенной и техногенной). Поэтому, несмотря на тщательное изучение технических и организационных систем, возникла необходимость автоматизированного управления новыми типами систем – организационно-техническими. Наличие человека как элемента в системе, элемента в подсистеме управления (лицо, принимающее решение по защите информации) не позволяет в полной мере применять традиционные методы формирования управляющих воздействий (касающихся исключительно организационных или технических систем).

По причине недостаточной изученности вопросов управления защитой информации подсистема защиты информации в ИССН традиционно рассматривается в основном как организационная система. Поэтому в защите информации преобладают меры правового или организационного характера. Применение технических мер, связанных с внедрением средств вычислительной техники, в первую очередь касается криптографического преобразования информации и защиты информации от утечки по техническим каналам.

В настоящее время созданы подходы и условия для формирования эффективно функционирующих систем управления организационно-техническими процессами, к классу которых относится защита информации. Основополагающим при этом является адекватное представление о защите информации как об объекте управления, то есть определены назначение, цели функционирования, структура, основные параметры (характеристики), способы управления, критерий оптимальности и эффективности управления.

Задачу адекватного представления о защите информации как об объекте управления целесообразно решать в рамках системного анализа, наиболее конструктивного направления, используемого для практических приложений теории систем к задачам управления. Описание защиты информации как объекта управления и в то же время как системы осуществляется в понятиях системного анализа.

Описание защиты информации как объекта управления позволяет провести дальнейшее исследование управления защитой информации в рамках теории автоматического управления (ТАУ). Теория автоматического управления входит в состав дисциплин, образующих науку об управлении. Изначально ТАУ предназначалась для исследования процессов управления техническими объектами. В последнее время ТАУ используют для изучения статики и динамики не только технических объектов, но и организационных, организационно-технических.

Основой ТАУ является метод пространства состояний, с помощью которого отдельные системы описываются во времени в виде векторных дифференциальных уравнений.

Применение научно-методологического аппарата ТАУ позволяет:

определить статические и динамические свойства системы;

описать основные законы управления в виде математических зависимостей, в соответствии с которыми вырабатываются управляющие воздействия;

исследовать переходные процессы в системе, их качество и влияние на дальнейшее поведение управляемой системы;

исследовать устойчивость и управляемость системы;

наглядно представить процессы функционирования системы методом фазовой плоскости (пространства).

Таким образом, представление и исследование процесса защиты информации в ИССН как объекта управления в рамках системного анализа – теории автоматического управления позволит определить его параметры (характеристики) и выявить присущие ему особенности, которые должны в полной мере учитываться при создании автоматизированных средств и систем управления защитой информации в ИССН. Это необходимо для проведения моделирования процессов защиты информации в ИССН в различных условиях их функционирования в целях определения оптимальности и эффективности применения различных способов управления защитой информации посредством программно-технических средств (средств автоматизации).

УДК 339

М.С. Маскина, О.В. Степанова

О БЕЗОПАСНОСТИ БЕСКОНТАКТНЫХ ПЛАТЕЖЕЙ

На сегодняшний день в мире существуют разные способы оплаты услуг, наиболее новым из которых является бесконтактный платеж. Самыми известными бесконтактными системами оплаты в России являются: MasterCard PayPass, Visa PayWave, Apple Pay, Samsung Pay. Их создатели заявляют, что технология бесконтактных платежей не только является прогрессивной, но и считается самой безопасной. В данной статье попытаемся разобраться, действительно ли бесконтактные платежи настолько безопасны.

Все вышеперечисленные системы оплаты работают на технологии связи, действующей на малых расстояниях, – NFC (Near Field Communication). Это высокочастотная, беспроводная связь малого радиуса,

работающая на частоте 13,56 МГц при скорости передачи данных 424 кбит/с на расстоянии до 10 см, предназначена для бесконтактного обмена информацией. В бесконтактные карты MasterCard PayPass и Visa PayWave встроен чип NFC, который позволяет провести операцию оплаты, если банковскую карточку поднести к считывающему устройству на близкое расстояние. Это очень удобно, так как процесс оплаты занимает немного времени, так как подтверждение платежа не требуется, если сумма покупки не превышает 1 000 рублей.

На данный момент Apple Pay поддерживает технологию NFC пока лишь с картами платежной системы MasterCard. Достаточно лишь сфотографировать или внести данные карты на смартфон iPhone, чтобы он стал платежным средством. Безопасность Apple Pay базируется на трех составляющих: биометрическом сенсоре Touch ID, чипе NFC и чипе Secure Element, который хранит в себе, не передавая и не копируя, информацию о банковских картах. Каждая транзакция получает уникальный код – токен, который передается терминалу вместо индивидуального номера карты. Чтобы произвести оплату, ее нужно подтвердить PIN-кодом или срабатыванием Touch ID независимо от суммы покупки. В случае кражи или потери смартфона iPhone все платежи можно запретить через программу Find My iPhone.

В отличие от Apple Pay платежный сервис Samsung Pay обеспечивает и работу по бесконтактной технологии, и связь по магнитной полосе. В смартфон Samsung помимо чипа NFC встроен магнитный чип MST (Magnetic Secure Transmission), который создает сигнал, идентичный сигналу пластиковой карты при ее взаимодействии с терминалами оплаты. Смартфоны с сервисом Samsung Pay создают магнитное поле, сходное с сигналом магнитной полосы банковской карты, и поддерживают обе ведущие платежные системы Visa и MasterCard.

Система безопасности Samsung Pay имеет также два принципа действия. На магнитных терминалах при каждом соединении чип генерирует индивидуальный код – токен, чтобы терминал считывал именно его, а не уникальный номер карты. При работе с NFC программа использует потоковое шифрование данных и алгоритм Serpent (змея), который оперативно распознает несанкционированный доступ. Samsung Pay использует безопасную среду Samsung Knox, которая проверяет смартфон на наличие уязвимостей и при их нахождении автоматически отключает Samsung Pay. В случае кражи или потери смартфона можно запретить проводить платежи через программу Samsung Find My Mobile.

В теории безопасность бесконтактных платежных технологий обеспечена вполне, но так ли это в действительности? Рассмотрим подробнее уровни защиты.

Первый уровень защиты – физический, суть которого заключается в том, что при совершении оплаты посредством NFC карту или смартфон нужно поднести на достаточно близкое расстояние (до 10 см) к считывающему устройству. Это условие действия бесконтактных технологий удалось обойти исследователям из британского Университета Суррея. Они продемонстрировали возможность считывания данных по технологии NFC на расстоянии до 80 см с помощью компактного сканера, которых позволяет таким образом незаметно забирать деньги в местах большого скопления людей. Другим путем пошли испанские хакеры Риккардо Родригес и Хосе Вилла, которые создали концепт вируса для операционной системы Android, превращающий смартфон в ретранслятор NFC-сигнала. При нахождении бесконтактной карты рядом с таким смартфоном злоумышленнику поступает сигнал о возможности проведения транзакции, создается мост между банковской картой и телефонами жертвы и хакера посредством связи сети Интернет. Таким образом, мошенник может расплатиться на ближайшем терминале со своего телефона, используя чужую карту.

Второй уровень защиты – криптография. Бесконтактные транзакции защищены стандартом EMV (Europay MasterCard Visa). Если магнитную дорожку можно просто скопировать, то с чипом аналогичные действия не совершаются. При каждом запросе терминала микросхема генерирует одноразовый ключ, который можно перехватить, но он уже не подойдет для следующего платежа.

Третий уровень защиты – сумма покупки. Существуют ограничения максимальной суммы единовременного списания денежных средств с бесконтактных карт, которые задает банк-эквайер. В России этот предел равен 1 000 рублей, при превышении его терминал просит ввести PIN-подтверждение для совершения покупки. К Apple Pay и Samsung Pay это не относится: для проведения платежа всегда требуется подтверждение. Британские исследователи Ньюкаслского университета сообщили, что обнаружили в платежной системе Visa недостаток: если запросить платеж в иностранной валюте, то пороговое ограничение не действует, хотя представители Visa позднее опровергли эту информацию.

Из вышесказанного следует, что существует возможность снятия посторонним лицом денег с банковских карт через бесконтактные платежи. Технологии Apple Pay и Samsung Pay являются самыми безопасными, так как предусматривают запрос PIN-кода или срабатывание Touch ID при проведении любой транзакции, независимо от суммы покупки. Но и эти технологии не обеспечивают полной безопасности бесконтактных платежей, ибо существует вирус, который автоматически устанавливает в операционной системе телефона приложения злоумышленников. На сегодняшний день более защищенной считается Apple Pay из-за существования некоторых ограничений: оплата принимается лишь в немногих учреждениях, система работает с одной платежной системой.

Судя по темпам внедрения бесконтактных платежных систем, все эти возможные угрозы не слишком пугают банки – очевидно, выгода превышает потери. Точнее, потери при бесконтактном мошенничестве пока незначительны, и банки могут компенсировать их безболезненно для себя. Таким образом, можно сказать, что самый простой и доступный способ безналичной оплаты является достаточно небезопасным. Так что о сохранности своих денежных средств лучше позаботиться самому, а не надеяться на обещания разработчиков новых систем.

УДК 343.32

А.М. Пановицын

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ ПРЕСЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ РАДИКАЛЬНЫХ ПОЛИТИЗИРОВАННЫХ ФОРМИРОВАНИЙ

Доступный мобильный интернет не только способствует социально-политическому и экономическому развитию общества, но и несет вполне реальные угрозы. Так, поиск кандидатов в радикальные группировки, их вербовка и соответствующая идейная и психологическая обработка все чаще осуществляются посредством сети Интернет. Ресурсы глобальной сети позволяют радикальным организациям оказывать массовое пропагандистское воздействие, особенно на молодое поколение, которое, являясь основным потребителем интернет-контента, еще не имеет твердых социальных позиций, политических взглядов и убеждений. Об эффективности данной работы свидетельствует статистика возраста лиц, задерживаемых при проведении политических акций за совершение противоправных действий на территориях нашего и сопредельных государств.

Сегодня в сети Интернет достаточно оппозиционных сайтов и информационных ресурсов, исключающих терпимость и толерантность, призывающих к публичному выражению своих политических и общественных взглядов путем проведения уличных акций, несанкционированных массовых мероприятий и других провокационных действий возле зданий государственных органов, посольств и консульских учреждений, крупных промышленных предприятий и организаций, в других местах массового скопления граждан. Члены радикальных формирований не собираются вести диалог с властями, не признают

компромиссов и не видят безопасных способов решения возникающих социальных и политических проблем, поэтому неизменной целью данных мероприятий является дестабилизация социально-политической обстановки в стране и организация массовых беспорядков, как показали события, предшествующие несанкционированным массовым мероприятиям, запланированным на 26 марта 2017 г. в Минске.

Проведение таких акций требует от органов внутренних дел Республики Беларусь и внутренних войск Министерства внутренних дел Республики Беларусь усиленных мер по охране общественного порядка и обеспечению общественной безопасности, а также поиска новых эффективных мер пресечения деятельности радикальных политизированных формирований.

В настоящее время в целях ограничения влияния радикальных политизированных формирований проводятся профилактические мероприятия, в том числе направленные на ограничение свободного доступа к ресурсам, содержащим социально-опасный контент. Данная работа, хоть и является эффективной, не может устранить имеющуюся угрозу, так как вместо удаленного контента появляется новый, адреса ссылок на материалы пропагандистского характера периодически меняются, информация размещается на серверах частных зарубежных компаний, напрямую не связанных с радикальным организациями, но уклоняющихся от взаимодействия с государственными службами.

Наряду с применяемыми методами профилактики сегодня предпринимаются дополнительные меры по ликвидации радикальных формирований путем выявления и привлечения к ответственности лиц, непосредственно занимающихся как вербовкой, подготовкой и организацией политических провокаций, так и поиском спонсоров и покровителей. В этих целях используются имеющиеся в распоряжении правоохранительных органов Республики Беларусь специализированные программно-технические комплексы UFED компании Celebrite, предназначенные для проведения криминалистических исследований устройств сотовой связи.

Устройства мобильной связи из-за своей компактности и функциональности являются наиболее распространенными средствами поиска информации и коммуникации в сети Интернет. Поэтому благодаря данным, находящимся в них, можно установить лиц, являющихся членами радикальных организаций и несущих потенциальную и реальную угрозу обществу. Следовательно, при задержании активных участников радикальных формирований, подозреваемых в совершении преступных действий, целесообразно изымать имеющиеся у них средства мобильной связи для проведения криминалистического исследования в целях получения вещественных доказательств преступной деятельности и установления соучастников, заказчиков и организаторов преступлений.

При проведении исследований средств связи особая роль должна отводиться сведениям, полученным из электронной почты, мобильных браузеров, интернет-мессенджеров, социальных сетей, специализированных форумов и чатов, навигационных приложений и других коммуникационных программ. Абоненты сетей сотовой связи, используя веб-браузеры, читают новости, посещают веб-сайты, совершают финансовые операции, следят за социальными сетями и т. д. При этом любая их сетевая активность оставляет следы в операционной системе и приложениях мобильного устройства. Проведение экспертного исследования мобильных веб-браузеров позволяет узнать: историю браузера, историю поиска; проанализировать закладки, временные файлы; изучить содержание сохраненных страниц и файлов, cookies; установить сохраненные пароли и имена пользователя; определить геолокационные данные местонахождения абонента.

Исследование интернет-мессенджера, в свою очередь, способствует установлению: истории групповых и приватных бесед (включая неавторизованные контакты, группы контактов); списка контактов с фотографиями, полями и заметками; полной информации о звонке посредством IP-телефонии: имени адресата или владельца телефонного номера, длительности разговора; текста отправленных сообщений, номера телефона получателя, временной метки и стоимости; деталей учетной записи: имени, адреса, телефонного номера, адреса электронной почты, даты рождения, другой пользовательской информации; геоданных события.

Кроме того, оперативный интерес при исследовании устройств сотовой связи могут представлять временные файлы, сохраненные фото, видео- или аудиозаписи, сделанные владельцем телефона, которые приняты другими абонентами или переданы им либо разыскиваются в сети Интернет подозреваемым. К примеру, мультимедийный контент может быть посвящен изготовлению простейших зажигательных гранат, взрывных устройств или тактике противодействия правоохранительным органам. Анализ навигационных приложений мобильного устройства дает возможность изучить маршруты и поисковые запросы пользователя, определить места, которые разыскивал или посещал подозреваемый.

Определенный интерес с точки зрения получения фактических сведений представляет возможность восстановления удаленных сообщений. В изъятых устройствах в большинстве случаев можно восстановить SMS- и MMS-переписку, сообщения электронной почты и другие сообщения в зависимости от типа устройства. Кроме того, используя специальные утилиты для просмотра данных, эксперты могут анализировать вложения и технические данные сообщений. В результате подобного исследования появляется возможность установить полный круг общения подозреваемого за счет сведений, полученных из элек-

тронной почты, социальных сетей, приложений IP-телефонии, чатов, форумов, SMS- и MMS-сообщений и т. п. Возможность восстановления переписки позволяет выявить возможных соучастников и организаторов проводимых акций, установить лиц, осуществляющих руководство и финансирование радикальных организаций.

Кроме того, извлеченные из мобильных устройств геолокационные сведения, совмещенные с данными операторов электросвязи, позволяют определить места проживания и подготовки членов радикальных организации, расположение возможных схронов оружия и боеприпасов.

Все вышеизложенное свидетельствует о возможности повышении качества работы правоохранительных органов по пресечению деятельности радикальных политизированных формирований за счет внедрения современных информационных технологий и технических средств.

УДК 621.391.01

А.С. Поляков, Д.В. Белый

ПРОСТОЙ СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ОШИБОК ПРИ ПЕРЕДАЧЕ ПО ЛИНИЯМ СВЯЗИ

Несмотря на серьезные достижения в области создания надежных каналов связи, проблема зашиты информации от ошибок при ее передаче остается достаточно актуальной. В настоящее время для решения этой задачи используются различные методы кодирования/декодирования информации, которые достаточно сложны, трудоемки при реализации и не всегда соответствуют требованиям по производительности (быстродействию). Наиболее простой способ обнаружения и исправления ошибок основан на операции вычисления четности единичных символов в строках и столбцах бинарной матрицы, представляющей собой передаваемую информацию. При кодировании двухмерных кодов этот способ позволяет определять адреса ошибок, но при условии, что и в столбцах, и в строках бинарной матрицы имеются только одиночные ошибки.

Предлагаемый ниже способ устранения ошибок основан на использовании результатов проверок четности по четырем координатам бинарной матрицы: строкам, столбцам, главным диагоналям и вспомогательным диагоналям.

Под главными диагоналями понимается как основная главная диагональ матрицы, так и все параллельные ей диагонали, рассматриваемые как непрерывные цепочки элементов матрицы, начинающиеся в первой строке и проходящие в направлении «сверху – вниз – направо» через все строки матрицы до достижения крайнего правого элемента

предыдущей строки с переходом на левый элемент следующей строки. Нумерация элементов новой строки начинается с номера, который был последним в предыдущей строке. На рисунке 1 элементы основной главной диагонали обозначены цифрой 1, а номера остальных главных диагоналей – цифрами, расположенными в верхних левых углах элементов матрицы.

Под вспомогательными диагоналями подразумеваются основная вспомогательная диагональ матрицы и все параллельные ей диагонали, проходящие в направлении «сверху – вниз – налево», начиная с первой строки матрицы и заканчивая последней строкой. С крайнего левого элемента строки происходит переход на крайний правый элемент следующей строки. Номера вспомогательных диагоналей на рисунке выделены курсивом и размещены в нижних правых углах элементов матрицы. Номера диагоналей на рисунке соответствуют номерам столбцов в первой строке матрицы: *b* – номера главных диагоналей в прямом направлении, *b̲* – номера вспомогательных диагоналей, *d* – номера главных диагоналей (расположены в верхних левых углах элементов матрицы), *d̲* – номера вспомогательных диагоналей (расположены в правых нижних углах элементов матрицы), *a* – номера строк матрицы.

		d						n	d		
b		1	2	3	4	5	6	7	8	9	10
b̲		9	8	7	6	5	4	3	2	1	Ln
a	1	1 9	2 8	3 7	4 6	5 5	6 4	7 3	8 2	9 1	
	2	9 8	1 7	2 6	3 ▼ 5	4 4	5 3	6 2	7 1	8 9	■
	3	8 7	9 6	1 5	2 4	3 3	4 2	5 1	6 9	7 1	
	4	7 ▼ 6	8 5	9 4	1 3	2 2	3 1	4 9	5 8	6 7	■
	5	6 5	7 4	8 ▼ 3	9 2	1 1	2 9	3 8	4 ▼ 7	5 6	
m	6	5 4	6 3	7 2	8 1	9 9	1 8	2 7	3 6	4 5	
MD	7	4 ■ 3	5 2	6 1	7 ■ 9	8■ 8	9 7	1 6	2 5	3■ 4	
AD̲	8	2	1	9	8	■7	■6	■ 5	4	■ 3	
Cln	9	■		■	■				■		

Размещение номеров диагоналей и проверочных символов четности

Результаты подсчета четности отображаются в дополнительно вводимых в матрицу столбце *Ln* и строках *MD*, *AD, Cln*, представляющих значения четности по строкам, главным диагоналям, вспомогательным диагоналям и столбцам матрицы соответственно.

Передаваемая информация разбивается на строки длиной n бит каждая. Из m последовательно следующих строк формируется бинарная матрица размером $(m \times n)$ бит, $m \le n$, в которой выполняются операции подсчета четности по строкам, столбцам и диагоналям. Получается бинарная матрица размером $(m + 3) \times (n + 1)$ бит. После передачи информации в полученной матрице производится проверка четности по всем упомянутым выше направлениям и по результатам проверок формируются списки номеров: ошибочных строк – *SX,* ошибочных столбцов – *SY,* ошибочных главных диагоналей – *SD* и ошибочных вспомогательных диагоналей – *SD*. Предположим, что в матрице (рисунок) после ее передачи по каналу связи появились ошибки (отмечены символом ▼), соответственно, после подсчета четности были выявлены ошибочные координаты (отмечены символом ■) и сформированы списки ошибочных координат: *SX* = 2, 4; *SY* = 1, 3, 4, 8; *SD* = 3, 4, 7, 8; *SD* = 3, 5, 6, 7.

Предлагаемый способ поиска ошибок предусматривает формирование множества строк $S = \{S_1, S_2, S_3, S_4\}$, где S_1 и S_2 – номера ошибочных строк и столбцов из списков *SX* и *SY*, а S_3 и S_4 – номера ошибочных диагоналей из *SD* и *SD*, соответствующие элементам матрицы, адреса которых указаны в S_1 и S_2. Множество S представляет собой множество возможных вариантов размещения ошибок. Формирование S производится на основе двух списков, например *SX* и *SY*, из элементов которых составляются все возможные пары, которые записываются в столбцы S_1 и S_2. Значения остальных столбцов в строках множества S вычисляются с помощью уравнений: $d\,(a,b) = (n - a + b + 1)\,MDn$, $b\,(a,d) = (a + d - n - 1)\,MDn$, $a\,(b,d) = (b + n - d + 1)\,MDn$, $\underline{b} = n - b + 1$, $\underline{d}\,(a,\underline{b}) = (2n - a - b + 2)\,MDn$.

Производится анализ множества S с целью исключения строк, представляющих адреса несуществующих (ложных) ошибок. Принцип выявления ложных ошибок достаточно прост: из S удаляются строки, в которых значение хотя бы одного столбца отсутствует в соответствующем списке (*SX*, *SY*, *SD*, *SD*).

Рассмотрим применение способа на примере представленной выше матрицы, в строках которой имеются ошибки: двойная – (5, 3), (5, 8) и две одиночные – (2, 4) и (4, 1). Процесс формирования множества S и анализа его элементов показан в нижеприведенной таблице. На основании списков *SX* и *SY*, формируется множество S_I, т. е. составляются

пары из элементов этих списков: 2 и 1, 2 и 3, 2 и 4, …, 4 и 8 (выделены курсивом) и записываются в столбцы S_1 и S_2 соответственно. С помощью приведенных выше формул вычисляются номера главных и вспомогательных диагоналей и записываются в столбцы S_3 и S_4. Из S_I удаляются строки, в которых значения столбцов S_3 и S_4 отсутствуют в списках *SD* и *SD* (отмечены --). Остались две строки (отмечены +), которые представляют собой адреса ошибок (2, 4) и (4, 1). Из списков *SX*, *SY*, *SD*, *SD* удаляются элементы, присутствующие в оставшихся строках.

Поскольку в *SX* нет элементов, множество S_{II} составляется на основе списков *SY* и *SD*. Из S_{II} удаляются строки, в которых столбцы S_3 и S_4 содержат номера диагоналей, отсутствующие в списках *SD* и *SD* (отмечены символами --). Оставшиеся две строки представляют собой адреса двойной ошибки (5, 3) и (5, 8). После удаления из списков ошибочных координат номеров, представленных в этих строках, списки *SX*, *SY*, *SD* и *SD* оказались пустыми. Это свидетельство того, что все ошибки обнаружены.

Таблица

Списки ошибочных координат				Множество строк S_I					Множество строк S_{II}				
SX	*SY*	*SD*	*SD*	S_1	S_2	S_3	S_4	Ошибки в строках	S_1	S_2	S_3	S_4	Ошибки в строках
До анализа множества S				*2*	*1*	9	8	--	9	*3*	*4*	8	--
2	1	3	3	*2*	*3*	2	6	--	5	*3*	*8*	3	+
4	3	4	5	*2*	*4*	3	5	+	5	*8*	*4*	7	+
–	4	7	6	*2*	*8*	7	1	--	1	*8*	*8*	2	--
–	8	8	7	*4*	*1*	7	6	+					
После анализа множества S_1				*4*	*3*	9	4	--					
–	3	4	3	*4*	*4*	1	3	--					
–	8	8	7	*4*	*8*	5	8	--					
После анализа множества S_2													
–	–	–	–										
–	–	–	–										

Эффективность способа повышается с увеличением соотношения «число столбцов/число строк» (n/m) бинарной матрицы, представляющей собой содержание передаваемой по каналу связи информации.

УДК 378.046

Е.А. Свирский

ИНФОРМАТИЗАЦИЯ ОБЩЕСТВА И ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Внедрение информационных технологий во все сферы деятельности общества стало нормой. И очевидно, что обратного пути нет. Темпы развития и внедрения информационных технологий очень высоки. С одной стороны, это радует, поскольку эти высокие темпы свидетельствуют об устойчивом движении общества к развитию и самосовершенствованию, а со второй, создает проблемы, связанные с освоением технологий и безопасностью информационных ресурсов.

Инновационные технологии далеко не всегда доводятся до совершенного состояния, очень часто информационные инновационные технологии изобилуют большим количеством ошибок, в том числе и уязвимостями, которые позволяют злоумышленникам получить несанкционированный доступ к информационным ресурсам. Изменить что-нибудь в этом практически невозможно, поскольку в условиях рыночной экономики необходимо как можно скорее выводить продукт на рынок, что сказывается на качестве разработки продукта.

Риски несанкционированного доступа к информационным ресурсам при внедрении инновационных информационных технологий всегда велики. Это вынуждает создавать избыточные системы защиты информационных ресурсов, поскольку защищаться нужно, но неизвестно от чего. Можно упростить систему информационной безопасности, защищаясь от конкретных угроз. Но такая система информационной безопасности не в состоянии предотвратить вновь возникающие угрозы, связанные с внедрением инновационных информационных технологий, а это значит, что система безопасности может бороться только со следствиями, т. е. с уже известными угрозами, что не позволяет обеспечить безопасность информационных ресурсов с заданной надежностью. Аналогом таких систем безопасности являются антивирусные программные комплексы, которые эффективно борются с уже известными вирусами, когда их сигнатуры занесены в антивирусную базу.

Построение систем информационной безопасности с заданным уровнем доверия возможно на основе международных стандартов по информационной безопасности. Но анализ базы технических нормативных правовых актов по информационной безопасности показывает, что она недостаточна для решения этой задачи: в Республике Беларусь приняты только отдельные из уже имеющихся у ISO стандартов по информационной безопасности. Также складывается впечатление, что

логика основных международных стандартов в республике не воспринята: даже сегодня, через 15 лет после перевода на русский язык стандарта ISO/IEC 15408, все еще идут дискуссии, а нужен ли он нам.

Опыт работы курсов повышения квалификации по информационной безопасности в государственном учреждении образования «Институт повышения квалификации и переподготовки в области технологий информатизации и управления» Белорусского государственного университета показывает, что сегодня не хватает как стандартов, так и методических материалов для проектирования и разработки систем информационной безопасности. Специалисты, непосредственно обеспечивающие защиту информации в информационных системах, не в состоянии применять стандарты по информационной безопасности, и в частности национальную версию ISO/IEC 15408, как в силу специфики самого стандарта, так и из-за отсутствия стандартов, расширяющих его границы применения, а также методических материалов по практике применения международных стандартов.

Для исправления сложившейся ситуации со стандартами в сфере информационной безопасности необходимо:

создать специализированный технический комитет по стандартизации – ТК «Защита информации»;

разработать и издать информационные материалы, раскрывающие концепцию (логику) основных международных стандартов;

разработать концепцию развития системы стандартов в сфере информационной безопасности;

провести ревизию существующей базы стандартов в сфере информационной безопасности;

признать необходимым разработку методических материалов по применению международных стандартов с учетом национального законодательства;

решить вопросы финансирования разработки и актуализации стандартов по информационной безопасности;

решить вопросы регистрации и сопровождения профилей защиты, отказавшись от практики регистрации их как стандартов;

решить вопросы финансирования разработки методических материалов и их сопровождения (создание интернет-ресурса для размещения методических и иных руководящих и информационных материалов по применению стандартов) и др.

Эти вышеперечисленные мероприятия должны, во-первых, поддерживать систему стандартов в актуальном состоянии и, во-вторых, способствовать квалифицированному применению стандартов по информационной безопасности практикующими специалистами.

Для разработки методических и иных руководящих и информационных материалов по применению стандартов необходимо будет привлекать высококвалифицированных экспертов.

Обширная нормативная и специальная литература позволит существенно повысить культуру управления информационной безопасностью информационных систем и создаст предпосылки для построения информационных систем с заданным уровнем доверия.

УДК 621.391

В.О. Сидорович

АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОМЕХОЗАЩИЩЕННОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ УПЛОТНЕНИЕМ

Практика построения современных систем передачи информации (СПИ) показывает, что наиболее дорогостоящими звеньями трактов передачи являются линии связи (кабельные, волоконно-оптические, сотовой мобильной радиосвязи, радиорелейной и спутниковой связи и т. д.). Поскольку экономически нецелесообразно использовать дорогостоящую линию связи для передачи информации единственной паре абонентов, то возникает необходимость построения многоканальных СПИ, обеспечивающих передачу большого числа сообщений из различных источников информации по общей линии связи.

В многоканальной СПИ по общему высокочастотному тракту передаются сообщения от нескольких источников информации. На передающей стороне многоканальной системы сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику канальные сигналы. Затем промодулированные канальные сигналы объединяются по тому или иному правилу, в результате чего формируется суммарный (групповой) сигнал. Данная операция называется уплотнением каналов. Полученный групповой сигнал затем модулирует несущее колебание, которое поступает на передачу. При использовании общей несущей канальные сигналы иногда называют поднесущими колебаниями. В ряде случаев, когда источники информации территориально сосредоточены, общая несущая не используется и канальные сигналы формируются непосредственно на несущих частотах. На приемной стороне многоканальной радиолинии после демодуляции несущей осуществляется операция, обратная операции уплотнения, – из группового сигнала выделяются сигналы отдельных каналов. Данная операция называется разделением (селекцией) каналов.

Тракт связи по способности передавать информацию характеризуется объемом $V_{MP}: V_{MP} = F_{MP} \times T_{MP} \times D_{MP}$, где F_{MP} – полоса частот тракта связи, T_{MP} – время использования тракта связи, D_{MP} – динамический диапазон тракта связи.

Передаваемый по тракту связи сигнал также имеет три измерения, т. е. тоже имеет объем $V_C = F_C \times T_C \times D_C$. Для передачи сигнала по тракту связи с допустимыми искажениями необходимо выполнить условие, чтобы $V_{MP} \geq V_C$.

Возможные методы уплотнения каналов можно классифицировать на линейные и нелинейные. К линейным относятся такие, при которых уплотнение сигналов отдельных каналов производится линейными устройствами с постоянными или переменными параметрами. В противном случае методы уплотнения являются нелинейными.

Если объем тракта связи намного больше объема передаваемого сигнала, то возможно уплотнение тракта связи n каналами передачи информации. В зависимости от того, какой из параметров тракта связи делится по отдельным каналам, различают методы: частотного и временного уплотнения, а также уплотнения по уровню (кодовое). Указанные методы уплотнения тракта связи являются линейными.

При использовании линейных методов операция уплотнения каналов сводится к суммированию канальных сигналов. В кодовом линейном уплотнении в качестве ансамбля канальных сигналов используются ортогональные системы тригонометрических функций, функций Радемахера – Уолша, полиномы Лежандра, Чебышева и др. Групповой сигнал представляется в виде суммы ортогональных канальных сигналов. Разделение сигналов на приемной стороне осуществляется n линейными избирательными устройствами (по числу каналов), каждое из которых выделяет соответствующий канальный сигнал из группового. Для линейного разделения каналов при линейном уплотнении необходимым и достаточным условием является линейная независимость канальных сигналов, при которой ни один из них нельзя представить линейной комбинацией других канальных сигналов.

Общая теория нелинейного уплотнения и разделения каналов к настоящему времени еще недостаточно разработана. Поэтому ограничимся рассмотрением так называемого комбинационного метода, который является одним из примеров нелинейного уплотнения и разделения каналов.

Пусть имеется $L_{\text{т}}$ каналов, в которых сообщения, подлежащие передаче, представлены в цифровой форме, например двоичным кодом. Символы кода «0» и «1» из всех каналов одновременно поступают на

устройство уплотнения. Поскольку в каждом из каналов возможно появление как «0», так и «1», то, очевидно, в любой фиксированный момент времени на устройство уплотнения от всех каналов поступает одна из $2^{L_У}$ возможных комбинаций «0» и «1». В общем случае при представлении сообщения в каждом из каналов с помощью кода с основанием b (шестиричного кода, где $b \geq 2$) в любой фиксированный момент времени на устройство уплотнения от всех $L_{т}$ каналов будет поступать одна из возможных комбинаций символов 0, 1, ... , $b-1$. Устройство уплотнения каждой из поступивших комбинаций ставит в соответствие свой номер (однозначно соответствующее этой комбинации число), который и является групповым сигналом. Таким образом, при данном методе уплотнения групповой сигнал не является линейной комбинацией канальных сигналов, а представляет собой однозначное отображение возможных комбинаций канальных символов, чем и объясняется название данного метода уплотнения. Групповой сигнал может кодироваться различными способами. На приемной стороне по принятому групповому сигналу восстанавливаются символы кодов сообщений в каждом из каналов, т. е. осуществляется разделение каналов. Данное разделение возможно, потому что любая комбинация символов кода сообщения однозначно соответствует групповому сигналу. В общем случае разделение каналов осуществляется нелинейными устройствами, хотя возможны модификации комбинационного уплотнения, при которых разделение осуществляется линейными устройствами.

На выбор того или иного типа кода группового сигнала существенное влияние оказывает сложность реализации соответствующей операции нелинейного преобразования (операции уплотнения) и обратной операции (операции разделения каналов). В этой связи большой интерес представляет один из частных случаев комбинационного уплотнения – логическое, или мажоритарное, уплотнение каналов. В результате данного уплотнения каждой комбинации двоичного кода с блоковой длиной $П_С$ в параллельной форме поступившей от уплотняемых источников, в устройстве уплотнения ставится в однозначное соответствие комбинация двоичного кода группового сигнала с блоковой длиной $П$, представленного в последовательной форме. При этом значение каждого двоичного символа кодовой комбинации группового сигнала определяется в соответствии с логической функцией абсолютного большинства, т. е. мажоритарно, что и определяет название данного метода уплотнения.

Двоичный код группового сигнала, получаемый при мажоритарном уплотнении, удобен для дальнейших преобразований на передающей стороне и обработки на приемной стороне и имеет минимально возможный пикфактор, что позволяет полностью использовать потенциальные возможности радиопередающего устройства. При этом нелинейность группового тракта не приводит к появлению междуканальных помех. Кроме того, при данном методе уплотнения оказывается возможным линейное разделение каналов, реализуемое полностью цифровым устройством разделения.

На сегодняшний день важнейшими достоинствами кодового уплотнения являются эффективное использование выделенной полосы частот (все каналы занимают одну и ту же полосу частот в одном временном интервале), обеспечение высокой потенциальной помехоустойчивости (за счет ортогональных функций) и высокая помехозащищенность, возможность обеспечить энергетическую и структурную скрытность передаваемой информации.

УДК 004.42

В.А. Тарасенко, Р.В. Кислинский

ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ГОСУДАРСТВЕННЫХ ОРГАНОВ

«Кто владеет информацией – тот владеет миром» – это, наверно, одно из самых известных высказываний, выражающее суть самой острой проблемы в мире. Актуальность данной работы связана с необходимостью защиты конфиденциальных данных, информации и сведений, утеря, разглашение или искажение которых может повлечь за собой негативные последствия для организации, предприятия и государства, а также необходимость соответствия информационной системы требованиям нормативно-правовых документов. Создание технологий и индустрии сбора, переработки, анализа информации и ее доставки конечному пользователю порождает ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях, а также безопасность самих систем и технологий.

Безопасность информационных систем является одной из важнейших составляющих проблем обеспечения безопасности государственного органа. Переход к новым формам государственного и хозяйственного управления в республике в условиях дефицита и противоречивости правовой базы породил целый комплекс проблем в области защиты данных, информации, знаний и самих информационно-коммуникационных технологий. Развитие информатизации в Республике Беларусь в течение 2011–2015 гг. осуществлялось в соответствии со Стра-

тегией развития информационного общества на период до 2015 года, утвержденной постановлением Совета Министров Республики Беларусь от 9 августа 2010 г. № 1074, и Законом Республики Беларусь «Об информации, информатизации и защите информации». Данные правовые акты определяют основные требования по защите информации: обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям. Любой государственный орган, получающий ресурсы, в том числе и информационные, перерабатывает их в продукты своей деятельности, порождая специфическую внутреннюю среду, которая формируется совокупностью структурных подразделений, персоналом, техническими средствами и технологическими процессами, экономическими и социальными отношениями как внутри органа, так и во взаимодействии с внешней средой.

Внутри государственного органа информационные потоки поступают в соответствующие модули корпоративной системы для структурирования, систематизации, обработки, анализа и практического использования. Большая часть этой информации является свободно используемой в процессе реализации деятельности государственного органа, однако в зависимости от особенностей внутренней деятельности и взаимодействия с внешним миром часть информации может быть предназначенной для служебного пользования, строго конфиденциальной или секретной. Такая информация является, как правило, закрытой и требует соответствующих мер защиты.

Программно-аппаратные средства для работы с охраняемой информацией либо встраиваются в соответствующие модули корпоративной информационной системы, либо используются локально в системах, указанных в политике информационной базы. Средства противодействия угрозам информационной базы и утечкам данных и информации являются, по сути, программно-аппаратным слоем в существующей ИТ-инфраструктуре государственного органа, в которой не только обрабатываются конфиденциальные данные, но и работают сотрудники с этими данными. Защитный комплекс состоит как из технических устройств и программного обеспечения, так и из совокупности организационных мер по реализации политики внутренней безопасности – целостное решение связывает воедино инфраструктуру, информацию и персонал.

К мерам по защите информации относится обеспечение особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации.

Государственные органы и юридические лица, осуществляющие обработку информации, распространение и (или) предоставление которой ограничено, определяют соответствующие подразделения или должностных лиц, ответственных за обеспечение защиты информации.

Целостные программные продукты осуществляют контроль и управление рисками внутренней безопасности и минимизируют утечки конфиденциальной информации за счет соответствующих технологических составляющих, глубоко интегрированных в информационную структуру органа. К ним относятся программно-аппаратные устройства:

отслеживания перемещения конфиденциальной информации по информационной системе;

управления контролем утечки данных через сетевой трафик по сетевым протоколам;

шлюза, через который идет трафик из внутренней сети во внешнюю сеть;

сервера, обрабатывающего определенный тип трафика;

рабочей станции;

внутренних каналов почты и др.;

управления контролем утечки охраняемой информации с рабочих станций, периферийных и мобильных устройств посредством контроля действий авторизованных пользователей с конфиденциальными данными: с файлами, внешними устройствами, сетью (локальной, беспроводной), буфером обмена, приложениями, устройств печати (локальные, сетевые);

теневого копирования информационных объектов в единую базу контентной фильтрации по единым правилам для всех каналов.

УДК 004.315.5

Н.С. Уваров

ВВЕДЕНИЕ В КОМБИНИРОВАННУЮ АРИФМЕТИКУ НА ОСНОВЕ АЛГЕБРЫ КВАТЕРНИОНОВ И ЛОГАРИФМИЧЕСКОЙ СИСТЕМЫ СЧИСЛЕНИЯ

Известно обобщение из действительной и комплексной арифметики (два вещественных числа), которое распространяется далее на более неясную арифметику кватернионов (четыре вещественных числа),

применяемой в обработке сигналов, аэрокосмических приложениях, графике и виртуальной реальности. Умножение кватернионов реализуется 3D-вращением, но оно затратное (обычно 16 умножений с плавающей запятой и 12 сложений). В работе предполагается альтернативное представление кватернионов с использовании логарифмов в целях уменьшения затрат умножения.

Как логарифмы, так и кватернионы – почтенные математические понятия. После открытия каждый из них произвел революцию и правил вековой наукой и техникой и с теоретической, и с практической точки зрения (ручное вычисление). В этой работе рассматривается возможность объединения кватернионов с логарифмической системой счисления. Потребность такого подхода имеет место в различных приложениях, таких как анимационная графика, виртуальная реальность, робототехника и системы управления.

Альтернативный способ, известный как конструкция Кэли – Диксона, заключается в том, что, чтобы определить кватернион, необходимо начать с пары комплексных значений: $\overline{Q}_0 = Q_{00} + Q_{01}i$ и $\overline{Q_1} = Q_{10} + \zeta$, каждое из которых содержит половину информации кватерниона. Такое представление Кэли – Диксона было использовано для построения умножителя кватернионов в прямоугольной форме и использовалось, чтобы предложить альтернативное полярное представление одного угла (с помощью комплексного угла, а не действительных углов, используемых в нашей работе): $Q = \overline{Q}_0 + \overline{Q}_1 j = (Q_{00} + Q_{01}i) + (Q_{10} + Q_{11}i) = Q_{00} + Q_{01}i + Q_{10}j + Q_{11}k.$ Как известно, $ij = k$ дает четвертый элемент прямоугольного представления кватернионов. Для формирования сопряженного кватерниона Q в этом представлении требуется комплексное сопряженное число $\overline{Q}_0^*$ и комплексное отрицательное $-\overline{Q}_1^*$. Для формирования отрицательного требуется отрицание обеих частей: $-\overline{Q}_0$ и $-\overline{Q}_1$. Если два кватерниона представлены парой комплексных значений Q и аналогично $P = \overline{P}_0 + \overline{P}_1 j,$ то результат умножения P на Q может быть описан в виде набора комплексных операций: $\overline{R}_0 = \overline{P}_0\overline{Q}_0 - \overline{P}_1\overline{Q}_1^*;$ $\overline{R}_1 = \overline{P}_0\overline{Q}_1 + \overline{P}_1\overline{Q}_0^*$ За исключением присутствия сопряженных операций, этот алгоритм похож на прямоугольный алгоритм умножения.

Новая концепция, которую называют кватернионная комплексная ЛСЧ (ККЛСЧ), заключается в замене прямоугольного представления для комплексных переменных: $\overline{Q}_0 = Q_{00} + Q_{01}i,$ $\overline{Q}_1 = Q_{10} + Q_{11}i,$

$\overline{P}_0 = P_{00} + P_{01}i,$ $\overline{P}_1 = P_{10} + P_{11}i,$ с представлением КЛСЧ при тех же значениях: $\overline{Q}_0 = \beta^{q_{00}} cis(q_{01}),$ $\overline{Q}_1 = \beta^{q_{10}} cis(q_{11}),$ $\overline{P}_0 = \beta^{p_{00}} cis(p_{01}),$ $\overline{P}_1 = \beta^{p_{10}} cis(p_{11}).$ Другими словами, $P_i = \beta^{p_{00}} cis(p_{01}) + \beta^{p_{10}} cis(p_{11}) j,$ $Q_0 = \beta^{q_{00}} cis(q_{01}) + \beta^{q_{10}} cis(q_{11}) j.$

Было доказано, что два самых естественных способа, которые можно было бы попытаться использовать в ЛСЧ для умножения кватернионов, не эффективны: во-первых, функция кватернионного логарифма не поможет упростить умножения, потому что умножение кватернионов не коммутативно, хотя сложение кватернионов коммутативно; во-вторых, с помощью ЛСЧ для двенадцати сложений/вычитаний, участвующих в прямоугольном определении умножения кватернионов, гораздо дороже, чем при использовании плавающей запятой. Чтобы преодолеть это, было предложено новое представление ККЛСЧ. Для кватерниона Q используется пара комплексных чисел в конструкции Кэли – Диксона, в котором каждое комплексное число представляется в КЛСЧ в логарифмическо-полярной форме. Для простой реализации с этим представлением нужны четыре КЛСЧ умножителя и два КЛСЧ сумматора, а так как ККЛСЧ сумматоры имеют общие подвыражения, оборудование может быть оптимизировано до эквивалента около по 5,5 ЛСЧ сумматоров и один ЛСЧ сумматор/вычитатель. Эти особенности могут извлечь выгоду во встраиваемых системах, которые интенсивно используют кватернионы в различных приложениях.

УДК 004.056:061.68

А.В. Федорцов

ПОРЯДОК ФОРМАЛИЗАЦИИ МОДЕЛИ ПОЛЬЗОВАТЕЛЯ ПРОГРАММНО-ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ДЛЯ ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ НА ОСНОВЕ АППАРАТА НЕЧЕТКОЙ ЛОГИКИ

Влияние человеческого фактора на процессы, протекающие в информационных системах различных организаций, нельзя недооценивать. Вместе с тем отсутствие четкого представления об источнике угроз (внутреннем нарушителе), ассоциируемом с указанным фактором, а также о последовательности и результатах его злоумышленных и незлоумышленных действий не позволяет осуществлять адекватное руководство защитой информации и приводит, в свою очередь, к ощутимым для организации негативным последствиям. По этой же причине

невозможно обеспечить тесную корреляцию между защитными мерами и исходящими от человека угрозами, вследствие чего проектируемые либо ранее введенные в эксплуатацию системы защиты информации не способны эффективно функционировать, как планировалось ранее. Поэтому формализация модели пользователя программно-техническими средствами организации будет способствовать достижению высокой степени уверенности в том, что поведение персонала при определенных условиях, как и потенциальные серьезные последствия (ущерб) для информационной системы, в основном прогнозируемы, что есть возможность управлять складывающейся обстановкой.

Установление параметров характеристик принимаемого на работу в организацию сотрудника является начальным этапом формализации модели пользователя программно-техническими средствами информационной системы. В качестве основы предлагается использовать модель DISC для классификации людей по типам. В общем виде DISC – четырехсекторная поведенческая модель для исследования поведения людей в окружающей их среде или в определенной ситуации. DISC позволяет рассмотреть стили поведения и предпочтения в поведении. Так как DISC не оценивает умственных способностей человека (IQ), эмоционального интеллекта (EQ), не является инструментом выявления мотивов человека, не оценивает образования, способностей и опыта, дополнительно следует использовать профильные опросные листы и тесты. После определения поведенческих типов (тип D – доминирующие, тип I – влияющие, тип S – постоянные, тип C – соответствующие) принимаемых на работу сотрудников, оценке их первичных способностей (качеств) полученные сведения обобщаются, ранжируются с применением функций принадлежности к определенным уровням представляемой для организации опасности и сводятся в таблицу. Для получения наглядного представления количественного и качественного соотношения тех или иных характеристик пользователей программно-техническими средствами целесообразно построить их портреты в виде графиков (диаграммы, рисунки), применив данные из таблицы.

Второй и последующий этапы формализации модели пользователя программно-техническими средствами, направленные на уточнение (дополнение) таблицы первоначальных характеристик сотрудников организации и исходящей от них опасности, наступают:

после назначения на различные должности (определяется выполняемая роль, категория выполняемых обязанностей и имеющихся при этом возможностей);

предоставления доступа к программно-техническим средствам (устанавливается группа пользователей, вид доступа, категория и класс

используемых программно-технических средств, категория обрабатываемой информации);

проведения контрольных мероприятий или переподготовки, повышения квалификации (выявляется фактический порядок исполнения обязанностей, реальный уровень навыков в работе, особенности поведения и мотивация совершения атаки);

перемещения на другую должность или увольнения (фиксируется уровень накопленных знаний об информационной системе и опыт продвижения по карьерной лестнице).

Полученные на каждом этапе данные, предварительно дополнив их численными значениями ущерба информационной системе в случае реализации атаки на используемые пользователем объекты, как наиболее уязвимые по отношению к нему, следует по определенным в организации правилам сопоставить с критериями внутреннего нарушителя.

Внутренние нарушители, как правило, имеют более высокий потенциал для реализации угроз информационной системе по сравнению с внешним нарушителем. Данное утверждение основывается на таких обстоятельствах, как наличие у внутренних нарушителей прав доступа, дополненных определенными полномочиями, знание обстановки (например, предпринимаемые меры и достоверно выполняемые процедуры для обеспечения информационной безопасности). Кроме того, внутренние нарушители, пользуясь доверием в соответствии с выполняемыми должностными обязанностями, имеют возможность причинять ущерб методами, которыми не располагают внешние нарушители, вынужденные дополнительно преодолевать элементы системы защиты информации. Кроме того, внутренние нарушители не ограничены в выборе цели атаки и благоприятного времени для ее совершения.

Таким образом, накопленная при формализации модели база знаний о пользователях программно-техническими средствами позволяет выявлять потенциальных внутренних нарушителей и в целом осуществлять руководство защитой информации с применением аппарата нечеткой логики, реализовывать на практике более взвешенную политику управления подчиненными должностными лицами из соображений информационной безопасности. Также полученная модель пользователя может быть использована при разработке технологии адаптивного управления программно-техническими комплексами и средствами защиты информации от атак.

УДК 621.391

В.М. Чертков, В.К. Железняк

СПОСОБ ПОЛУЧЕНИЯ ИДЕНТИФИКАЦИОННОГО ПОРТРЕТА РАДИОЭЛЕКТРОННЫХ СРЕДСТВ ПЕРЕХВАТА ИНФОРМАЦИИ МЕТОДАМИ НЕЛИНЕЙНОЙ РАДИОЛОКАЦИИ

Важными требованиями, предъявляемыми к средствам обнаружения, являются высокая вероятность обнаружения и достоверность идентификации. Несмотря на совершенство средств обнаружения радиоактивных средств (РЭС), достигнутая достоверность не удовлетворяет порогу обнаружения. Высокая достоверность определяется обнаружением РЭС в активных и пассивных режимах их работы.

Нелинейный локатор (НЛ) является одним из самых эффективных технических средств по выявлению радиоэлектронных средств перехвата информации как в активном, так и в пассивном режимах работы. Существует несколько методов обнаружения и локализации скрытых устройств.

Традиционный метод обнаружения и локализации основывается на изменении разницы уровней на второй и третьей гармониках переизлученного зондирующего сигнала от РЭС перехвата информации. Основным недостатком этого метода является большое количество ложных срабатываний, вызванных сложными металлическими предметами, не содержащими электронных компонентов. Вероятность правильного обнаружения в основном будет зависеть от опыта и квалификации оператора НЛ.

Другим методом является способ обнаружения РЭС с распознаванием типа нелинейности, основанного на излучении зондирующего сигнала, промодулированного по пилообразному закону в направлении на нелинейный объект, и на приеме и регистрации сигнала отклика по двум каналам на второй и третьей гармониках частоты вторичного электромагнитного поля. Идентификация типа нелинейности производится по соотношению уровней амплитуд канальных сигналов. Дополнительная модуляция позволяет определить зависимость амплитуды сигнала отклика от амплитуды зондирующего сигнала и по ее виду уточнить тип нелинейности. Основным недостатком приведенного метода является сложность технической реализации, в частности высокие требования к линейности передающего каскада.

Третий метод предложен авторами на основе использования амплитудно-модулированного сигнала (АМ-сигнал) с подавленной несущей, который основывается на управлении уровнем спектральных составляющих и на высокой точности измерения и обработки статистических значений уровней на второй, третьей и удвоенной восстановленной несущей гармониках, образованных из-за нелинейности вольт-амперной характеристики (ВАХ) РЭС. Данный метод позволяет за несколько измерений, выполненных под одним углом ориентации на НЛ, определить ВАХ РЭС перехвата информации.

Учитывая факт того, что современные РЭС состоят из несколько тысяч полупроводниковых p-n-переходов, результирующая ВАХ будет образовываться исходя из суперпозиции ориентации отклика всех его p-n-переходов. Данная теория проверялась во время экспериментов с макетным образцом НЛ и расположенными в области его излучения двух диодов с разными ВАХ. Полученные результаты полностью подтвердили развитую теорию.

В ходе анализа результатов экспериментов при оценке нелинейности ВАХ простых объектов (состоящих из одного p-n-перехода) отмечено, что при разных углах наведения НЛ на нелинейный элемент полученные данные отличаются только мощностью принимаемых уровней, при этом закон распределения значений остается постоянным. Это свидетельствует о том, что эффективная площадь рассеивания (ЭПР) простых нелинейных объектов (одиночных диодов) по форме совпадает при различных углах, что дает возможность рассматривать ЭПР в виде вектора данных, полученных только при одном угле излучения.

Авторами предложено в качестве идентификационного портрета (ИП) исследуемого объекта совместно рассматривать его ЭПР и вид нелинейности ВАХ. ЭПР, по сути, определяет характер изменения уровней на второй, третьей и удвоенной восстановленной несущей гармониках в зависимости от угла облучения зондирующим сигналам. Следовательно, ИП будет определяться как характер изменения уровней на второй, третьей и удвоенной восстановленной несущей гармониках и как расчетные изменения коэффициентов уравнения аппроксимации в зависимости от угла.

Построение ИП сводится к следующему алгоритму действий:

обнаружение нелинейного объекта по наличию отклика на второй и третьей гармониках переизлученного зондирующего сигнала;

определение необходимого уровня излучения для более качественного приема и регистрации данных. На данном этапе происходит регулирование мощности излучения и оптимальных подбор расстояния до объекта;

получение вида нелинейности ВАХ на основе разработанного алгоритма, который по полученным данным значений уровней комбинационных гармоник определяет коэффициенты аппроксимирующего полинома;

повторное получение ВАХ после смены угла облучения по азимуту на 1–5 градусов (дискретность может варьироваться) с помощью датчика гироскопа;

повторение всего цикла измерений по азимуту по достижении 360 градусов, т. е. после полного круга азимута со сменой угла места на 1–5 градусов.

В результате полученные данные можно представить в виде трех графиков для каждого коэффициента полинома, аппроксимирующего ВАХ нелинейного объекта, которые и будут составлять ИП. Пример такого ИП в виде трехмерного графика для квадратичного коэффициента полинома, аппроксимирующего ВАХ диода Д220, представлен на рис. 1. По осям X и Y отложены соответственно градусы угла азимута и угла места, по оси Z значение квадратичного коэффициента. На рис. 2 представлен тот же ИД, но в виде изображения, на котором номера строк и столбцов – это углы места и азимута, а яркость соответствует числовому значению расчетного квадратичного коэффициента.

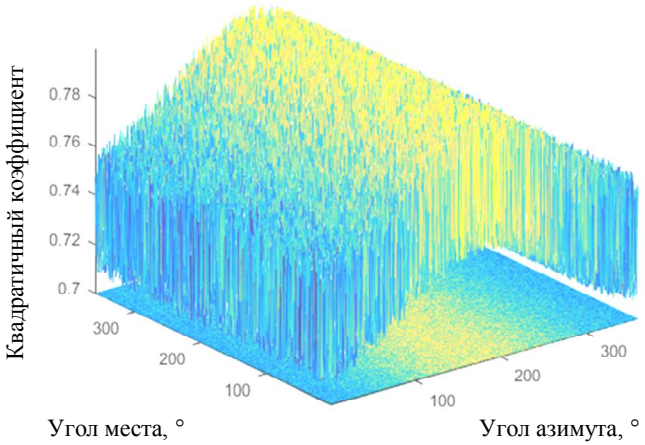

Рис. 1. Идентификационный портрет диода Д220
по квадратичному коэффициенту в виде графика

В результате цифровой обработки данных, полученных при оперативном обследовании, алгоритм поиска определяет степень подобия идентификационных портретов и принимает решение по отнесению исследованного объекта к определенному классу РЭС, который визуализируется в графическом интерфейсе пользователя на персональном компьютере в режиме реального времени, что снижает нагрузку на

оператора, повышает уровень обнаружения и достоверности идентификации, а следовательно, снижает вероятность объявления ложной тревоги.

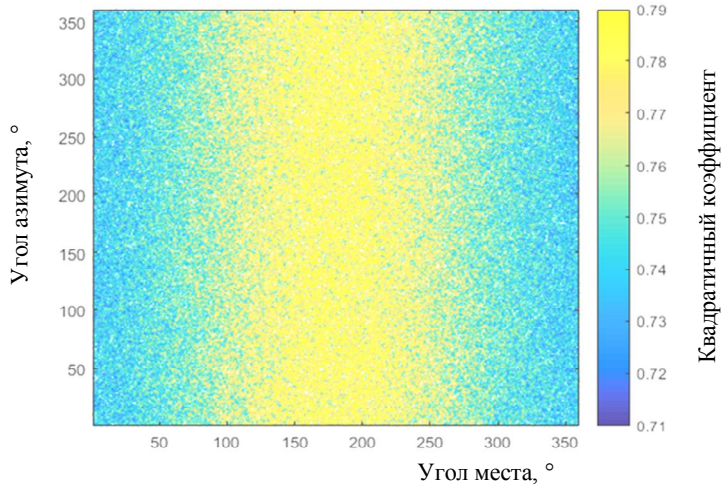

Рис. 2. Идентификационный портрет диода Д220
по квадратичному коэффициенту в виде изображения

УДК 004:34

Т.Г. Чудиловская

ОБЛАЧНЫЕ СЕРВИСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последние годы стремительно развиваются технологии облачных вычислений (англ. cloud computing), которые предлагают удаленный (в том числе через интернет) доступ пользователей к хранилищам данных, вычислительным ресурсам и программным приложениям.

Национальный институт стандартов и технологий США выделяет три модели облачных вычислений: IaaS (инфраструктура как сервис), PaaS (платформа как сервис) и SaaS (программное обеспечение как сервис).

Среда облачных вычислений – это совокупность вычислительных ресурсов в виде виртуальной машины, предоставляемых пользователю с помощью общих сервисов доступа. Физический уровень облачной системы состоит из аппаратных ресурсов, которые необходимы для

обеспечения предоставляемых сервисов, и, как правило, включает серверы, системы хранения и сетевые компоненты.

Использование облачных технологий обладает весомыми преимуществами: возможностью передавать в аутсорсинг высокотехнологические работы по эксплуатации ИТ-инфраструктуры; доступностью широкого набора информационных технологий и ресурсов без приобретения специализированного программного обеспечения и оборудования, а также затрат на обучение и содержание персонала.

Вместе с тем использование облачных технологий имеет и свои недостатки. Система облачных вычислений может подвергаться различным видам угроз безопасности, включая угрозы целостности, конфиденциальности и доступности ее ресурсов, данных и виртуальной инфраструктуры, которые могут быть использованы нецелевым образом, например в качестве площадки для распространения новых атак.

Фактически задачу защиты облака можно разделить на две составляющие: обеспечение безопасности функционирования оборудования и обеспечения безопасности данных. Провайдер должен реализовать защиту своего аппаратно-программного комплекса от несанкционированного вторжения, модификации кода, взлома ИТ-системы, чтобы обеспечить защиту данных клиента. Клиент, в свою очередь, при необходимости размещения каких-либо важных и секретных данных может использовать технологии шифрования для защиты от несанкционированного доступа к ценной информации.

При этом важно учитывать, что возможности пользователя по управлению системой безопасности зависят от выбора сервисной модели. В модели IaaS провайдер контролирует лишь физическую и виртуальную среду, в которой работают виртуальные машины клиентов; он не занимается обслуживанием операционных систем и приложений, функционирующих внутри самих виртуальных машин. На стороне заказчика можно построить свои собственные технические средства обеспечения безопасности. Клиент может иметь полный контроль над реальной конфигурацией сервера, что гарантирует ему больший контроль рисков безопасности окружения и данных. В PaaS поставщик управляет лишь аппаратной платформой и операционной системой, что ограничивает способности предприятия заказчика в управлении рисками на этих уровнях. В модели SaaS провайдер облачной услуги полностью контролирует физическую и логическую инфраструктуру, занимается его разработкой и обслуживанием, оставляя пользователю лишь возможность загружать свои данные и работать с ними.

В сложившихся условиях специалистами все большее внимание уделяется вопросам разработки средств защиты, позволяющих противодействовать угрозам информационной безопасности со стороны злоумышленников, на основе единого концептуального подхода, сочетающего в себе преимущества разных методов защиты информации.

Активное распространение облачных сервисов и очевидная выгода от работы на этом направлении привела к появлению концепции «всё как сервис» (Everything as a Service, XaaS). Среди набора услуг, предоставляемых провайдерами, в последнее время набирают популярность облачные сервисы для информационной безопасности, или безопасность как услуга (Security as a Service, SecaaS). Безопасность как сервис – это обеспечение безопасности, осуществляемое удаленно на базе системы, находящейся в собственности поставщика услуги, с оплатой по факту использования.

Преимуществами сервисов безопасности являются:

быстрое развертывание. Чтобы начать пользоваться сервисом, не требуется дополнительного программного обеспечения или аппаратных устройств;

аутсорсинг административных задач;

использование лицензионного программного обеспечения;

стабильное обновление антивирусов, black-list (черных списков) и других ресурсов защиты;

снижение издержек на поддержание работоспособности аппаратного и программного обеспечения;

гибкая система оплаты за потребленные ресурсы;

отсутствие необходимости содержать штат специалистов определенной квалификации в области информационной безопасности;

доступность при наличии подключения к сети Интернет;

надежность и устойчивость сервиса благодаря технологии отказоустойчивости и уровня надежности.

В зависимости от выбора программного продукта Security as a Service включает в себя целый набор программ и сервисов для обеспечения комплексной безопасности: антиспам-защиту, антивирусную защиту, защиту от атак «отказ в обслуживании» (DoS/DDoS), оценку безопасности, защиту мобильных устройств (поддержка IOS/Android), управление, обнаружение и предотвращение вторжений.

Кроме основных сервисов услуга может предоставить и дополнительные, к которым можно отнести: шифрование данных, непрерывность бизнеса и восстановление после катастроф (предотвращение потери данных), управление учетными записями и доступом, управление событиями информационной безопасности, предотвращение утечек данных.

В настоящее время лидирующими продуктами Security as a Service являются McAfee Security-as-a-Service, Panda Security Cloud Protection, Symantec.cloud и Zscaler Cloud Services.

Задача обеспечения информационной безопасности становится все более сложной и ресурсоемкой. Грамотно применяя облачные сервисы для информационной безопасности, клиенты получают выстроенные процессы защиты, возможность оперативно подключать или отключать услугу, оплачивая только тот объем сервисов, который необходим в конкретный момент времени.

УДК 355.4

А.Н. Шедько

СОЗДАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В настоящее время проблема обеспечения безопасности критически важных объектов информатизации (КВОИ) в каждом государстве приобретает все более актуальный характер. И в Республике Беларусь, и в Российской Федерации также уделяется значительное внимание этой проблеме. В частности, отмечается, что информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Также определяется, что угрозы информационной безопасности предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Создание системы безопасности (СБ) КВОИ предлагается рассматривать на примере стационарной цифровой автоматической телефонной станции (АТС) узла электросвязи сети общего пользования, обеспечивающей предоставление услуг в населенном пункте Республики Беларусь с численностью не менее 20 тыс. человек (далее – районный центр).

Объекты информатизации (ОИ) данной АТС размещены в пределах области действия одного комплекса безопасности (КЗ) и используются как критичные активы, так и обрабатывается общедоступная (открытая) информация, хотя одно или несколько средств вычислительной техники из совокупности имеют открытые каналы обмена информацией за пределами КЗ с другими ОИ. Так как при этом обеспечивается доступность и целостность критичных активов путем реализации мер,

направленных на предотвращение умеренного ущерба, то данным КВОИ присвоен класс В2-у.

Согласно перечню показателей уровня ущерба национальным интересам Республики Беларусь в социальной и демографической сферах в случае возникновения угроз различного характера в отношении ОИ (его составляющих элементов) уровень ущерба определяется с учетом того, что АТС размещена в районном центре, и оценивается как умеренный при прекращении функционирования на период от 48 до 72 ч более одной сети электросвязи (стационарная или сотовая подвижная электросвязь, передача данных, в том числе с доступом в сеть Интернет).

Если АТС в целом невозможно отнести к КВОИ, то приказом ее руководителя создается комиссия по отнесению отдельных ОИ АТС к КВОИ, утверждается ее председатель и состав. Комиссией составляется перечень ОИ АТС с их описанием (состав комплекса технических средств (средств электронной вычислительной техники), структура используемого программного обеспечения (перечень), общая функциональная схема (схема сети), наличие и характер взаимодействия с другими объектами и т. д.), который утверждается руководителем АТС. Для каждого из перечня ОИ АТС комиссия устанавливает отраслевые критерии отнесения ОИ к КВОИ методом экспертных оценок: определяются отраслевые критерии, перечень которых утвержден, и соответствие данных ОИ отраслевым критериям отнесения ОИ к КВОИ в соответствии с методикой, также утвержденной.

Руководителю АТС представляется отчет по результатам оценки соответствия ОИ АТС отраслевым критериям отнесения ОИ к КВОИ и составляются заключения о соответствии отдельных ОИ АТС отраслевым критериям отнесения их к КВОИ по утвержденной форме. В частности, к КВОИ комиссией может быть отнесена локальная информационная сеть АТС. Указанные заключения с описанием ОИ прилагаются к мотивировочному ходатайству и направляются по подчиненности в вышестоящую организацию для принятия решения об отнесении ОИ АТС к КВОИ.

При рассмотрении практических аспектов создания СБ КВОИ уже упоминалось о том, что в рамках создания СБ КВОИ разрабатывается и внедряется система менеджмента информационной безопасности.

Кардинальной мерой повышения защищенности сетей связи могла бы стать замена телекоммуникационного оборудования иностранного производства на «доверенное» отечественное, сертифицированное. Однако данное мероприятие сложное в организационно-техническом плане, требует больших затрат. Приемлемой альтернативой является оснащение существующего оборудования связи специализированными техническими средствами защиты.

В мировой практике в качестве основных технических средств для обнаружения и исключения злоумышленного воздействия через каналы внешнего доступа к телефонной сети используются защитные межстанционные экраны. С точки зрения алгоритма анализа и обработки информации экраны для АТС являются более сложными устройствами по сравнению с аналогичными решениями для компьютерных сетей.

УДК 004.087.5

А.И. Шемаров

СОЗДАНИЕ ИДЕНТИФИКАЦИОННЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ГИБРИДНЫХ МЕТОДОВ ЗАЩИТЫ НА ПРИМЕРЕ МИКРОКОНТРОЛЛЕРОВ ATMEL AVRMEGA

При создании идентификационных устройств существует проблема считывания кодов, записанных на этих устройствах, с последующей их эмуляцией. Получение кодов доступа для стандартных устройств, как правило, не вызывает значительных технических трудностей. Идентификационные карты на базе микроконтроллеров существенно усложняют задачу злоумышленников.

Проблема может быть решена с помощью гибридных методов защиты, не использующих записанный в идентификационной карте цифровой код, который является главной целью атаки злоумышленников. Это связано в первую очередь с доминированием цифровых технологий и математических криптографических алгоритмов. В качестве гибридной технологии целесообразно использовать объединение цифровых и аналоговых методов защиты информации. Применение таких гибридных методов заключается в создании и использовании дополнительного канала передачи кодированных аналоговых данных на базе физического интерфейса, применяемого для передачи цифрового кода. Передача аналогового кодированного сигнала сопровождается нарушением стационарных вероятностных характеристик аналоговых сигналов цифрового интерфейса. Реальный сигнал, несущий код, формируется в пределах допустимых отклонений физических параметров для конкретного интерфейса. Многообразие параметров физических сигналов, их вероятностные отклонения существенно усложняют задачу сканирования. Использование дополнительных каналов позволяет существенно упростить задачу идентификации оригинального устройства от его эмуляции, выполненной с помощью специальных технических средств.

Для иллюстрации метода рассмотрим возможную реализацию дополнительного канала передачи данных на базе широко распространенных микроконтроллеров фирмы ATMEL AVRmega. Эти контроллеры

используют RISC-архитектуру и отличаются развитой системой команд, позволяющих создавать эффективный быстродействующий код; имеют большое количество встроенных интерфейсов, которые можно использовать для решения практически любых задач при сопряжении микроконтроллера с другими средствами вычислительной техники и периферийными устройствами. Одним из наиболее широко используемых протоколов, применяемых для подключения разнообразных технических устройств как вычислительной техники, так и устройств связи является протокол универсального асинхронного приемника-передатчика UART (последовательного асинхронного стартстопного устройства). Протокол используется при создании таких распространенных интерфейсов, как RS-232, RS-485, Bluetooth (в режиме использования протокола RFCOMM), и многих других. В рассматриваемых микроконтроллерах используется от одного до четырех специализированных портов UART. Их имплементация осуществляется стандартным образом: путем совмещения функций выводов универсального порта со специализированным функционалом при использовании в качестве функционального устройства или интерфейса.

Современные инструментальные средства программирования используют их стандартным образом путем применения программных платформ (фрэймворков), определяющих структуру программной системы или программного обеспечения, облегчающего разработку и объединение разных компонентов большого программного проекта в единое целое для решения стандартизированной задачи.

Такой подход позволяет достаточно просто реализовать взаимодействие посредством выбранного интерфейса с предлагаемым набором стандартных функций, но не позволяет управлять им, так как это не предусмотрено производителем микроконтроллера. Для более ясного представления иллюстрируемого метода определимся с количественными параметрами. В качестве базовых параметров используем технические характеристики микроконтроллера ATmega128. Исходя из базовой частоты работы UART, равной 115 200 Гц (для получения требуемой скорости передачи данных эта частота подвергается аппаратному деления на целочисленный коэффициент), и максимальной частоты работы процессора этого типа, равной 16 МГц, определим частоту работы процессора как 115 200 × 138 = 15 897 600 Гц. По схеме передачи данных 115200-8-N-1 для передачи одного бита требуется 138 тактов работы микроконтроллера (за это время можно выполнить до 138 команд при использовании RISC-архитектуры), а при использовании схемы 9600-8-N-1 для передачи одного бита потребуется 1 656 тактов работы микроконтроллера соответственно. Наличие таких ресурсов производительности микроконтроллера позволяет выполнить формирование требуемой последовательности протокола без

использования специализированного устройства. Номера тактов микроконтроллера, в которые осуществляются те или иные действия передатчика UART, представлены в табл. 1 для двух скоростей – 9 600 Бод и 115 200 Бод соответственно, согласно схеме передачи восьми битов данных, начиная с младшего бита, без контроля на четность и одного стопового бита.

Таблица 1

Номер такта работы микроконтроллера (относительная величина)

Событие	Схема 9600-8-N-1	Схема 115200-8-N-1
Бит «Старт передачи»	0	0
Бит D_0	1656	138
Бит D_1	3312	276
Бит D_2	4968	414
Бит D_3	6624	552
Бит D_4	8280	690
Бит D_5	9936	828
Бит D_6	11592	966
Бит D_7	13248	1104
Бит «Старт передачи»	14904	1242
Конец передачи	16560	1380

Приемник UART, в свою очередь, по приему стартового бита, что служит для него началом синхронизации приема передаваемой последовательности, выделяет передаваемые биты в строго определенных временных интервалах. Наличие интервалов для приема последовательности определяется фактором невозможности использования абсолютно одинаковых генераторов тактовых частот в приемнике и передатчике одновременно без использования внешней синхронизации процессов. Рассогласование частот тактовых генераторов в ряде случаев требует формирования второго стопового бита. В табл. 2 представлены допустимые диапазоны формирования фронтов принимаемой последовательности в тактах работы микроконтроллера при отклонении частоты приемника и передатчика в диапазонах -3...0 % и 0...3 % для скоростей 9 600 Бод и 115 200 Бод.

При работе устройств в относительно короткий интервал времени частоты работы генераторов изменяются очень незначительно. Их величины можно считать постоянными. А это означает, что при точном анализе времени формирования начала принимаемой битовой последовательности для реальных физических объектов будет наблюдаться смещение начала формирования бита только в одном из поддиапазонов, соответствующих соотношению частот генераторов передатчика и приемника UART, если, конечно, на данном интервале происходит изменение его значения на противоположное значение.

Таблица 2

Диапазон номеров тактов работы микроконтроллера (относительная величина)

Событие	Схема 9600-8-N-1		Схема 115200-8-N-1	
	$f_{пер} \geq f_{пр}$	$f_{пер} \leq f_{пр}$	$f_{пер} \geq f_{пр}$	$f_{пер} \leq f_{пр}$
Бит «Старт передачи»	0	0	0	0
Бит D_0	1606...1656	1656...1706	134...138	138...142
Бит D_1	3213...3312	3312...3411	268...276	276...284
Бит D_2	4819...4968	4968...5117	402...414	414...426
Бит D_3	6425...6624	6624...6823	535...552	552...569
Бит D_4	8032...8280	8280...8528	669...690	690...711
Бит D_5	9638...9936	9936...10234	803...828	828...853
Бит D_6	11244...11592	11592...11940	937...966	966...995
Бит D_7	12851...13248	13248...13645	1071...1104	1104...1137
Бит «Старт передачи»	14457...14904	14904...15351	1205...1242	1242...1279
Конец передачи	16063...16560	16560...17057	1339...1380	1380...1421

Используя этот факт, можно создать систему передачи последовательности данных по протоколу UART, которая будет нарушать стационарные вероятностные характеристики функционирования реального цифрового интерфейса, путем формирования последовательности с помощью встроенных в процессор многофункциональных счетчиков-таймеров. В режиме сравнения заданного значения регистра сравнения с текущим состоянием счетчика-таймера можно автоматически переключать соответствующий выход микроконтроллера в противоположное состояние. Совпадение состояний регистров вызывает соответствующее прерывание работы микроконтроллера. В ходе обработки прерывания задается новое значение регистра сравнения. Чередуя значения из различных диапазонов, можно сформировать требуемую последовательность, несущую полезную информацию или обладающую требуемыми вероятностными характеристиками. Аналогично используя режим захвата значения счетчика, организуется анализ принимаемой последовательности с целью определения нарушения стационарных вероятностных характеристик и извлечения скрытой передаваемой информации. К сожалению, объем статьи не позволяет привести код программы.

Необходимо отметить, что интерфейс, использующий протокол UART, выбран в иллюстративных целях для пояснения предлагаемого метода. Такое решение является не самым оптимальным. Поэтому для практического применения можно использовать более совершенные методы, не столь очевидные. Выбор того или иного метода зависит от цели, достигаемой в результате его применения.

РАЗДЕЛ 3

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

УДК 343.5

П.Л. Боровик

ВЫЯВЛЕНИЕ ПОРНОГРАФИИ С ИЗОБРАЖЕНИЕМ НЕСОВЕРШЕННОЛЕТНЕГО В ПИРИНГОВЫХ ФАЙЛООБМЕННЫХ СЕТЯХ: ОБЗОР ИНСТРУМЕНТАРИЯ

Успешное выявление и раскрытие преступлений, предусмотренных в ст. 343[1] УК Республики Беларусь (изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего), зависит от его своевременного обнаружения, выявления всех преступников, а также от установления фактических данных, полностью обосновывающих доказывание и привлечение виновных к уголовной ответственности. Залогом успеха в реализации вышеобозначенных задач в борьбе с преступностью данного вида является проведение еще до возбуждения уголовного дела оперативно-розыскных мероприятий.

Анализ оперативно-следственной практики с материалами дел о преступлениях обозначенного вида, а также исследованный нами международный опыт противодействия подобным деяниям свидетельствуют о том, что в настоящее время большинство таких преступлений совершается с использованием пиринговых файлообменных сетей (далее – P2P-сети), например eMule, MediaGet, Kazza, Gnutella, Overnet, Shareaza, Edonkey, uTorrent, BitTorrent и др. Выявление информационной продукции с признаками детской порнографии в этих сетях существенно осложняется тем, что принцип работы последних основывается на свободном и неконтролируемом обмене файлами между территориально удаленными компьютерами, как правило, без участия какого-либо центрального сервера либо интернет-провайдера (оператора связи). Каждый из участников P2P-сети открывает доступ к определенным файлам на своем жестком диске, после чего они заносятся в базу данных и становятся доступными для загрузки пользователями сети. В некоторых сетях могут создаваться группы открытого и закрытого типа (круг лиц ограничивается модераторами). Порнографическая продукция в таких сетях обычно распространяется лишь среди определенной категории лиц, а также по рекомендациям знакомых. При этом сама размещаемая информация в P2P-сетях не индексируется поисковыми системами, поэтому контролировать содержание хранилищ файлов, доходящих иногда до сотен тысяч или даже больше, а также идентифицировать пользователей сети особенно сложно. Все это способствует практически беспрепятственному распространению в P2P-сетях различного противоправного контента, включая порнографические изображения с участием несовершеннолетних.

Для выявления детской порнографии в сети Интернет оперативными подразделениями обычно используются возможности поисковых систем (например, Google, Yandex, Yahoo! и т. п.), при применении которых выявляются ресурсы, содержащие материалы с детской порнографией, отслеживаются источники их поступления, принимаются меры к их блокированию и установлению личности их организаторов. Практика показывает, что органом уголовного преследования используются также общедоступные интернет-сервисы (Соцпоиск, Twinitor.com, Topsy.com, Images от Google, Tineye.com, Yasiv.com/vk, web.archive.org и др.), позволяющие осуществлять: мониторинг ресурсов социальных сетей; поиск изображений по заданному образцу; выявление и визуализацию скрытых связей и зависимостей определенных лиц, объектов и событий в глобальной информационной сети; поиск противоправной информации в «архиве» интернета.

Наряду с вышеуказанными средствами, реализующими задачи поисковой деятельности в сети Интернет, органом уголовного преследования может также использоваться специализированное программное обеспечение по автоматизированному обнаружению и снятию информации уголовно наказуемого содержания, ее предварительной обработке и уничтожению. В качестве примера следует привести программный продукт PERKEO, который уже более 20 лет используется правоохранительными органами многих зарубежных стран для выявления детской порнографии в сети Интернет. Данная программа работает по принципу распознавания известной информации и ее копий путем сложения проверенных данных в банках данных, используемых для сравнения. Механизм ее действия состоит в том, что она с любой информации, независимо от названия, образует идентификационный

признак в виде цифрового «отпечатка пальцев», который сравнивается с информацией, поступающей в сравнительную базу данных. При совпадении указанных признаков местонахождение и название информации заносятся в текстовую картотеку. На основе «листа попаданий» можно сделать вывод о наличии или отсутствии на данном компьютере порнографических материалов с участием несовершеннолетних.

Похожее специализированное программное обеспечение под названием Child Exploitation Tracking System (CETS) разработано совместными усилиями канадского представительства корпорации Microsoft, Канадской полиции, полиции Торонто при участии Скотланд-Ярда, Интерпола и Министерства внутренней безопасности США. Данная программа с помощью встроенного биометрического сканера с большой точностью может распознавать лица детей, подростков и взрослых, фиксировать элементы интерьера, изображения лиц или их фрагментов, которые встречаются в интернете и, таким образом, может сравнивать один материал с другим. Кроме того, CETS имеет встроенную систему отслеживания путей, по которым в сеть поступает детская порнография, что обеспечивает возможность поиска как пострадавших от участия в порносъемках, так и непосредственно преступников. Анализируя с помощью CETS транзакции по номерам кредитных карт, а также переписку в чатах, сотрудники правоохранительных органов могут отслеживать как поставщиков детской порнографии в сети Интернет, так и покупателей.

Однако, несмотря на неоспоримые достоинства вышеприведенных программных средств, главным их недостатком является отсутствие возможности функционирования в P2P-сетях.

В настоящее время эксперты различных поисковых систем продолжают исследования технических возможностей для индексации содержимого баз данных криминальной информации, хранящейся в P2P-сетях, а также для доступа к закрытым ресурсам и идентификации пользователей. В результате использования нестандартного подхода к поиску оперативно значимой информации специалистами компании TLO и Министерства внутренней безопасности США было разработано принципиально новое программное обеспечение Child Protection System (система защиты детей), предназначенное для мониторинга P2P-сетей на предмет обнаружения компьютеров, предлагающих в режиме раздачи порнографические материалы с изображением несовершеннолетних.

Этот программный комплекс представляет собой набор специализированных компьютерных программ – утилит для мониторинга P2P-сетей. Общий принцип их работы основывается на сравнении контрольных

сумм изображений на компьютерах в файлообменных сетях с информацией, содержащейся в специализированной полицейской базе данных порнографических изображений детей, в которой имеется более 9 млрд записей, и размещенной на серверах департамента уголовных расследований штата Вайоминг, США и компании TLO. Выявленные таким образом IP-адреса и списки изображений с элементами детской порнографии вносятся в базу данных, доступ к которой предоставляется оперативным сотрудникам. База данных Child Protection System, обновляясь в режиме реального времени, содержит данные о компьютерах во всем мире, предлагающих к распространению материалы порнографического характера с изображением несовершеннолетних.

Child Protection System обеспечивает: быстрый доступ к информации о сетевой активности определенного IP-адреса; поиск по имени пользователя P2P-сети; доступ к базе данных контрольных сумм порнографических материалов с изображением несовершеннолетних; поиск посредством глобального идентификатора (GUID), который позволяет отследить конкретное лицо в интернете вне зависимости от смены им IP-адресов. Полученная информация позволяет сотрудникам правоохранительных органов проанализировать и изучить контент, связанный с IP-адресом лица, заподозренного в распространении детской порнографии.

Утилита PeerSpectre2, входящая в состав Child Protection System, загружает список ключевых слов с серверов системы защиты детей, которые дают результаты, содержащие порнографические изображения несовершеннолетних, и направляет запросы в компьютеры, подключенные к файлообменным сетям. В ответ на эти ключевые слова компьютерами направляется информация о размере, имени файла и его контрольной сумме, которые сравниваются с базой данных порнографических материалов с изображением несовершеннолетних. При обнаружении совпадений IP-адрес компьютера, порт и контрольная сумма соответствующего изображения вносится программой PeerSpectre2 в базу данных Child Protection System.

Утилита ShareazaLE позволяет сотрудникам правоохранительных органов исследовать содержимое компьютера подозреваемого и напрямую загрузить контент с определенного IP-адреса. Поисковые запросы для данного программного обеспечения формируются в веб-интерфейсе Child Protection System.

Утилита Media Library предоставляет пользователям возможность получать информацию, классифицировать, управлять и определять местоположение файлов, выявленных при использовании Child Protection System, которое, в свою очередь, позволяет сравнивать файлы с

базой данных контрольных сумм порнографических материалов с изображением несовершеннолетних, получить их классификацию, сделанную другими сотрудниками и при необходимости добавить свою собственную. Предусмотрена также возможность сохранения файлов и их организации по контрольным суммам, что дает быстрый доступ к ним в процессе проведения оперативных мероприятий.

Факт обнаружения в P2P-сети информации, представляющей оперативный интерес, может послужить основанием для возбуждения уголовного дела и производства расследования. В процессуальной же форме программное обеспечение может найти применение при проведении таких следственных действий, как осмотр (все его виды), выемка предметов, документов, а также следственный эксперимент, выполняемый с целью опытной проверки показаний.

Следует отметить, что доступ к Child Protection System разрешен исключительно пользователям, имеющим персональную лицензию, которую могут получить только действующие сотрудники правоохранительных органов, активно занимающиеся борьбой с распространением детской порнографии. Лицензии предоставляются бесплатно и действуют исключительно на территории государства национальной принадлежности сотрудника. Однако обязательным условием получения лицензии является прохождение сотрудниками правоохранительных органов соответствующего обучения. Такое обучение с 2013 г. проводится в Международном учебном центре подготовки, повышения квалификации и переподготовки кадров в сфере миграции и противодействия торговле людьми Академии МВД Республики Беларусь.

Вышеизложенное позволяет сформулировать следующие выводы.

1. Актуальным направлением деятельности оперативных подразделений по изучению материалов и расследованию дел об обороте детской порнографии является получение информации из P2P-сетей, используемых в преступных целях, а также перехват имеющих уголовно-релевантное значение изображений и сообщений, циркулирующих в них. Факт обнаружения объектов или информации в сети, представляющей оперативный интерес, может послужить основанием для возбуждения уголовного дела и производства расследования.

2. Использование специальных поисковых программных средств значительно упрощает процедуру блокирования ресурсов с запрещенным контентом и привлечения их владельцев к предусмотренной законодательством ответственности. Испытанная на практике методика использования Child Protection System в совокупности с уже имеющимися приемами поисковой деятельности в сети Интернет предоставляет широкие возможности для выявления фактов распространения запрещенного контента в P2P-сетях.

Учитывая, что в настоящее время информационный поиск в P2P-сетях выступает для субъектов оперативно-розыскной деятельности в качестве относительно нового направления деятельности, специфика применения поисковых мероприятий данного вида в сетевом информационном пространстве является актуальной темой отдельного исследования.

УДК 343.985.7:343.542.1

К.Ю. Гутер

DOS-АТАКИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ: СУЩНОСТЬ И КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ КЛАССИФИКАЦИЯ

В современном мире все большее значение приобретают автоматизированные системы, которые управляют различными критически важными процессами. Отказ в обслуживании в таких системах может привести к непредсказуемым последствиям. Именно поэтому возрастает актуальность вопросов защиты от DoS-атак (от англ. Denial of Service – отказ в обслуживании), обычно определяемых как умышленные атаки на вычислительную систему с целью доведения ее до отказа в обслуживании, т. е. создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам) либо этот доступ будет затруднен.

Для установления истинной картины содеянного и уяснения, в чем конкретно выразилось общественно опасное деяние рассматриваемого вида, имеет смысл подвергнуть криминалистически значимой классификации способы совершения DoS-атак в отношении автоматизированных систем управления (АСУ). Это позволит, с одной стороны, установить в первоначальных следственных ситуациях характерный способ совершения расследуемого преступления (даже по отдельным признакам) и выдвинуть типовую версию о расследуемом событии, а с другой – создать необходимую основу для разработки, внедрения и эффективного применения средств и методов противодействия преступлениям против информационной безопасности.

Анализ практики раскрытия и расследования преступлений, предусмотренных ст. 349–355 Уголовного кодекса Республики Беларусь (преступления против информационной безопасности), показывает, что способы совершения DoS-атак не всегда исследуются в полном объеме. Это вызвано прежде всего неразработанностью научно обоснован-

ной криминалистически значимой классификации способов совершения DoS-атак, что подтверждает преобладающее большинство опрошенных нами респондентов из числа оперативных работников и следователей, специализирующихся на раскрытии и расследовании рассматриваемых преступлений.

Обобщение теории и практики совершения преступлений против информационной безопасности позволяет выделить следующие типы и виды DoS-атак в зависимости от причин, из-за которых может возникнуть DoS-условие.

I. Насыщение полосы пропускания. Этот тип основан на «классической» атаке flood (англ. flood – наводнение, переполнение), которая предполагает критически большое количество бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию АСУ, приводящих к отказу в работе из-за исчерпания системных ресурсов – процессора, памяти или каналов связи.

1. HTTP-флуд (ping-флуд). Механизм этой DoS-атаки состоит в следующем: атакующий посылает незначительный по объему HTTP-пакет, в результате чего сервер АСУ отвечает на него пакетом, размер которого в сотни раз больше. Для предотвращения отказа в обслуживании из-за получения ответных HTTP-пакетов злоумышленник каждый раз подменяет свой IP-адрес IP-адресами узлов в сети. Указанный вид атак можно осуществить только в том случае, если канал атакующего намного шире канала атакуемой АСУ.

2. Smurf-атака (ICMP-флуд). Для реализации этой вида DoS-атаки злоумышленник использует широковещательную рассылку для проверки работающих в системе узлов, отправляя ping-запросы. Затем по широковещательному адресу злоумышленник отправляет поддельный ICMP-пакет, после чего адрес атакующего меняется на адрес АСУ, на который все узлы начинают отправлять ответы на ping-запросы. Соответственно, чем больше объем сети, тем быстрее наступает отказ в обслуживании.

3. Атака Fraggle (UDP-флуд). Атака Fraggle является аналогом Smurf-атаки, однако вместо ICMP-пакетов используются пакеты UDP. Принцип действия заключается в отправке на седьмой порт сервера АСУ echo-команд по широковещательному запросу, а затем – в подмене IP-адреса злоумышленника на IP-адрес сервера АСУ, который начинает получать множество ответных сообщений. Данная атака приводит к насыщению полосы пропускания и полному отказу в обслуживании.

4. Атака переполнения пакетами SYN (SYN-флуд). Принцип атаки заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок с целью переполнять на сервере очередь на подключения. При этом злоумышленник игнорирует SYN+ACK-пакеты цели, не высылая ответных пакетов, либо подделывает заголовок пакета, чтобы ответный SYN+ACK отправлялся на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения, ожидающие подтверждения от клиента. По истечении определенного таймаута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь либо устанавливают ее с существенными задержками.

II. Недостаток ресурсов. Злоумышленники прибегают к данному типу DoS-атак для захвата системных ресурсов АСУ, таких как оперативная и физическая память, процессорное время и др. Обычно такие атаки проводятся с учетом того, что хакер уже обладает некоторым количеством ресурсов системы. Целью атаки является захват дополнительных ресурсов. Для этого не обязательно насыщать полосу пропускания, а достаточно просто перегрузить процессор сервера атакуемой АСУ, то есть занять все допустимое процессорное время.

1. Отправка «тяжелых» пакетов. Атакующий посылает серверу пакеты, которые не насыщают полосу пропускания (канал обычно довольно широкий), но тратят все его процессорное время. Процессор сервера, когда будет их обрабатывать, может не справиться со сложными вычислениями. Из-за этого произойдет сбой, и пользователи не смогут получить доступ к необходимым ресурсам.

2. Переполнение сервера лог-файлами. Лог-файлы сервера – это файлы, в которых записываются действия пользователей сети или программы. Неквалифицированный администратор может неправильно настроить систему на своем сервере, не установив определенный лимит. Хакер воспользуется этой ошибкой и будет отправлять большие по объему пакеты, которые вскоре займут все свободное место на жестком диске сервера. Эта атака сработает только в случае с неопытным администратором, который не хранит лог-файлы на отдельном системном диске.

3. Плохая система квотирования. На некоторых серверах АСУ имеется так называемая CGI-программа, которая связывает внешнюю программу с Web-сервером. Если хакер получит доступ к CGI, он сможет создать скрипт, который задействует значительное количество ресурсов сервера, таких как оперативная память и процессорное время. Так, например, скрипт CGI может содержать в себе циклическое создание больших массивов или вычисление сложных математических формул.

При этом центральный процессор может обращаться к такому скрипту несколько тысяч раз. Следовательно, если система квотирования настроена неправильно, то такой скрипт за малое время отнимет все системные ресурсы у сервера. Конечно, выход из этой ситуации очевиден – установить определенный лимит на доступ к памяти, но и в этом случае процесс скрипта, достигнув этого лимита, будет находиться в ожидании до тех пор, пока не выгрузит из памяти все старые данные. Поэтому пользователи АСУ будут испытывать существенный недостаток в системных ресурсах.

4. Недостаточная проверка данных пользователя. Этот вид атак также приводит к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов АСУ (вплоть до исчерпания процессорных ресурсов) либо выделению большого объема оперативной памяти (вплоть до исчерпания доступной памяти).

5. Провокация. Это атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

III. Ошибки программирования. Данный тип атак основан на использовании специальных программ (эксплойтов), которые помогают атаковать сложные вычислительные ресурсы АСУ чаще всего из-за ошибок в программном коде, приводящих к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой необрабатываемой исключительной ситуации, когда происходит аварийное завершение программы-сервера – серверной программы.

1. Недостатки в программном коде. Суть атаки данного вида заключается в том, что злоумышленники ищут ошибки в программном коде какой-либо программы либо операционной системы АСУ, заставляя ее обрабатывать такие исключительные ситуации, которые она обрабатывать не умеет, в результате чего возникают ошибки. Простым примером такой атаки может служить частая передача пакетов, в которой не учитываются спецификации и стандарты RFC-документов. Злоумышленники наблюдают, справляется ли сетевой стек с обработкой исключительных ситуаций. Если не справляется, то передача таких пакетов приводит к панике ядра (kernel panic) или даже к краху всей системы в целом.

К этому виду относится ошибка Ping of death, распространенная еще в 1990-е гг. Длина пакета IPv4 по стандарту RFC 791 IPv4 не может превышать 65 535 байт. При этом на атакуемый сервер АСУ посылается ICMP-пакет большей длины, предварительно разбитый на части, в результате чего на сервере от такого пакета переполняется буфер.

2. Переполнение буфера. Переполнение буфера возникает и в том случае, если программа из-за ошибки программиста записывает данные за пределами буфера. Например, программист написал приложение для обмена данными по сети, которое работает по какому-либо протоколу. В этом протоколе строго указано, что определенное поле пакета максимум может содержать 65 536 байт данных. Однако после тестирования приложения оказалось, что в ее клиентской части сети в это поле нет необходимости помещать данные, размер которых больше 255 байт. Поэтому и серверная часть примет не более 255 байт. Далее злоумышленник изменяет код приложения так, что клиентская часть отправляет все допустимые по протоколу 65 536 байт, но сервер к их приему не готов. Из-за этого возникает переполнение буфера, и пользователи АСУ не могут получить доступ к приложению.

3. DoS-атака на уязвимости в программном обеспечении на DNS-серверах. В процессе этой атаки злоумышленник осуществляет подмену IP-адреса DNS-сервера домена АСУ. После чего атакуемый при запросе HTML-страницы попадает либо в «черную дыру» (если IP-адрес был заменен на несуществующий), либо прямиком на сервер злоумышленника. Второй случай чреват более серьезными последствиями, поскольку злоумышленник легко может получить доступ к информационным ресурсам АСУ.

Из вышеизложенного можно определить существование различных видов DoS-атак. К основным их разновидностям относятся насыщение полосы пропускания, недостаток ресурсов, ошибки программирования. Каждый тип угроз характеризуется специфическим способом осуществления и причинами возникновения DoS-условий.

УДК 004 + 351.74/76 + 623.71

А.В. Железняков

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ РАЗРАБОТКЕ ПЛАНА КОМПЛЕКСНОГО ИСПОЛЬЗОВАНИЯ СИЛ И СРЕДСТВ

В процессе управления подразделениями внутренних войск МВД Республики Беларусь возникает необходимость в выполнении ряда расчетных задач, обеспечивающих подготовку и планирование действий приданных сил. Принимаемые решения определяются опытом ответственного лица и реальным знанием местности района ответственности. В то же время при организации управления подчиненными си-

лами, особенно при осложнении обстановки, необходимо владеть информацией о географических объектах (здания, сооружения, транспортные магистрали и инженерные коммуникации, общественные места, лесные массивы и т. д.). Необходимость обрабатывать большой объем информации о местности, труднообозримой и плохо представляемой по карте, приводит к недопустимым временным затратам. В результате принимаемые решения могут быть недостаточно обоснованными, а следовательно, не обеспечивать эффективное выполнение поставленной задачи.

Исследования показывают, что внедрение средств автоматизации и современных информационных технологий в процесс управления дает реальную возможность повысить эффективность принимаемых решений, оперативность и качество управления. Интеграция геоинформационных систем в автоматизированные системы управления войсками обеспечит поддержку принятия более эффективных решений и их реализацию.

Одной из задач обработки цифровой картографической информации (цифровая карта или цифровой план местности) в целях повышения эффективности действий войсковых нарядов по охране общественного порядка (ООП) и обеспечению общественной безопасности (ООБ) является построение маршрутов патрулирования. Это предусмотрено разработкой плана комплексного использования сил и средств ООП, в котором определяются все маршруты войсковых нарядов, закрепленных за территориальным органом внутренних дел (ОВД).

Так, при патрулировании в населенном пункте имеет место выбор маршрута с максимальной площадью просматриваемой территории и минимальным временем нахождения на маршруте при средней скорости движения патруля (войскового наряда). При этом могут быть определены пункты, обязательные для посещения (места скопления граждан, места нахождения источников повышенной опасности, площади, вокзалы, аэропорты, рынки, станции метрополитена, объекты военного назначения, а также прилегающие к ним территории и т. д.). Следует учесть, что в одном районе службу несут несколько патрулей, следовательно, есть следующие ограничения: траектории маршрутов патрулирования не должны совпадать, однако пересечение допускается; интегрированные зоны видимости должны иметь как можно меньшую площадь перекрытия либо разнесены по времени.

Корректировка маршрутов осуществляется: в случае изменения криминогенной обстановки на территории, перераспределения сил и средств, при введении различных планов специальных мероприятий, строительства новых жилых массивов, торговых и развлекательных заведений и т. д.

Под маршрутом понимается передвижение войскового наряда от начальной точки $S_0(x,y)$ к конечной $S_K(x,y)$. А при построении маршрута возврата из точки $S_K(x,y)$ в точку $S_0(x,y)$ необходимо максимизировать площадь просматриваемой территории с минимизацией времени нахождения на маршруте и при этом избежать наложения или пересечения интегрированных зон видимости либо свести их к минимуму. Если принять среднюю скорость V_{cp} движения войскового наряда на всех участках одинаковой, то минимизация времени нахождения сводится к построению кратчайшего маршрута от начальной точки $S_0(x,y)$ к конечной $S_K(x,y)$.

Используя теорию графов, задачу поиска кратчайшего маршрута можно сформулировать следующим образом: на местности задан граф $G=(V,E)$ с двумя выделенными вершинами $p_0, q_0 \in V$, длины $l(e) \in N^+$ и веса $a(e) \in N^+$ для всех ребер $e \in E$. Необходимо найти в G простой путь из p_0 в q_0 с минимальным значением длины L и веса A. При этом под простым следует понимать такой путь, в котором ни одна вершина графа не встречается дважды.

В аналитическом виде задача записывается следующим образом:

$$\Theta = \sum_{i=1}^{k} A(v_i) + \sum_{i=1}^{k-1} L(v_i, v_{i+1}), \qquad (1)$$

где Θ – показатель эффективности найденного маршрута, который требуется оптимизировать; $\{v_i\}$ – вершины графа, через которые проходит маршрут, $i=\overline{1,k}$; k – число вершин, через которые проходит маршрут; $A(v_i)$ – функционал, в соответствии с которым вычисляется вес в вершине графа v_i; $L(v_i, v_{i+1})$ – функционал, определяющий длину ребра из вершины v_i в вершину v_{i+1}.

Вес вершин графа вычисляется в соответствии с функционалом $A(\bullet)$ в результате оценки местности и определяет соответствие дискрет местности предъявленной системе требований к маршруту.

В общем случае вес вершины будет определяться шагом дискретизации Δd и наличием тех или иных географических объектов и элементов обстановки в соответствующей дискрете местности, а также в некоторой окрестности рассматриваемой дискреты.

Для вычисления веса вершины графа необходимо сопоставить объекты, присутствующие в дискрете, с критичными для решаемой задачи объектами, которые определяются системой требований (критериев), предъявляемых к маршруту:

$$A(v_i) = A(\Delta d, P_i, \Omega'), \qquad (2)$$

где Δd – размер шага дискретизации; P_i – множество объектов местности и обстановки, присутствующих в дискрете, соответствующей вершине графа v_i, $i=\overline{1,k}$; Ω' – множество критичных для решаемой задачи объектов местности и обстановки.

С учетом применения матричной модели местности длина маршрута между вершинами графа v_i и v_{i+1} вычисляется в соответствии с выражением:

$$L(v_i, v_{i+1}) = \sqrt{(\Delta d \cdot \eta)^2 + h^2(v_i, v_{i+1})}, \qquad (3)$$

где

$$\eta = \begin{cases} \sqrt{2}, \text{если перемещение между дискретами осуществляется по диагонали,} \\ 1, \text{ во всех остальных случаях.} \end{cases}$$

– коэффициент, учитывающий направление перемещения между дискретами; $h(v_i, v_{i+1})$ – перепад высот в дискретах местности, соответствующих вершинам графа v_i и v_{i+1}.

Оптимизация первого слагаемого выражения (1) достигается благодаря прохождению маршрута по местности, соответствующей требованиям, предъявленным к маршруту. Оптимизация второго слагаемого достигается путем выбора из равных по значению первого слагаемого маршрутов самого короткого по протяженности. Отметим, что в данной постановке задачи не ставится акцент на минимизацию или максимизацию слагаемых, а все ограничивается лишь понятием «оптимизация», что позволяет более гибко использовать разрабатываемую модель как для нахождения наилучших маршрутов, так и для оценки наихудших вариантов.

Таким образом, если обозначить через вектор $\overline{V}$ множество вершин графа v_i, через которые проходит маршрут, то задача поиска оптимального маршрута сводится к поиску вектора $\overline{V}^*$, при котором достигается оптимальное значение показателя эффективности маршрута:

$$\overline{V}^* = \arg \underset{\overline{V} \in V}{\text{opt}} \{A(\overline{V}) + L(\overline{V})\}, \qquad (4)$$

где V – множество вершин, через которые может проходить маршрут.

Исходя из вышеизложенного, решение задачи поиска оптимального маршрута состоит из двух этапов:

на первом (подготовительном) этапе осуществляется оценка обстановки и выделение участков местности, соответствующих выражению (1), по которым может проходить искомый маршрут;

на втором (оптимизационном) этапе осуществляется нахождение оптимального маршрута в соответствии с выражением (4) и с учетом системы ограничений.

Эта задача решается построением интегрированной зоны видимости на основе суммирования зон видимости на каждом условном шаге перемещения войскового наряда от начальной к конечной точке.

УДК 343

В.Ф. Кетурко

ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Современный период развития органов внутренних дел характеризуется расширением использования современных информационных технологий в целях достижения более высокого качества, изменения содержания и характера труда сотрудников. Благодаря автоматизации целого ряда информационных процессов сотрудники ОВД освобождаются от рутинных, трудоемких операций.

В то же время, несмотря на положительные примеры использования современных информационных технологий в ОВД, практика показывает, что многие теоретические, методологические, организационные, правовые и технические вопросы еще требуют своего разрешения.

Наиболее актуальными являются проблемы правового регулирования процессов информатизации в правоохранительной сфере. Необходимо признать, что информатизация ОВД и насыщение ее современными информационными технологиями в настоящее время не обеспечены законодательной базой в достаточной степени. Несмотря на принятие ряда ведомственных нормативных правовых актов, затрагивающих отдельные аспекты данной проблемы, детально проработанной нормативной правовой базы информатизации, которая отвечала бы современным условиям, до сих пор не создано.

Хотелось бы подчеркнуть, что комплексное исследование правовых аспектов информатизации правоохранительной сферы будет способствовать выработке конструктивных предложений по существенному повышению эффективности управления всеми правоохранительными органами и ОВД в частности.

В Республике Беларусь политика информатизации начала формироваться с начала 90-х гг. XX в. В 1991 г. Совет Министров Республики Беларусь принял Программу информатизации на 1991–1995 гг. и на период до 2000 г. Впервые о проблеме информатизации в правоохра-

нительной системе было обозначено в Концепции судебно-правовой реформы в 1992 г. Однако действенных мер по информатизации ОВД она не внесла, требовалось принятие более кардинальных мер.

Основное внимание в программе информатизации в Республике Беларусь и в ОВД уделялось обеспечению научно-технических и организационно-экономических условий создания и развития информационных технологий, информационной структуры, системы формирования информационных ресурсов.

В 1995 г. вступает в силу Закон «Об информатизации», который становится законодательной базой информатизации в Республике Беларусь и в ОВД, сформулировав основные положения:

общедоступность документированной информации, не отнесенной в установленном порядке к категории с ограниченным доступом;

оперативность, полнота и точность предоставляемой пользователю документированной информации;

участие государства в формировании информационных ресурсов и обеспечении соответствия этих ресурсов задачам информатизации;

предоставление пользователю документированной информации на государственном языке Республике Беларусь или на языке, обусловленном договором субъектов правоотношений в сфере информатизации;

защита прав собственности на объекты в сфере информатизации.

В данный период достигнуты значительные успехи по выполнению Программы информатизации и Закона «Об информатизации»: применены информационные базы данных, а также наработан большой опыт работы с информационными системами в области правоохранительной деятельности.

Тем не менее по ряду причин, среди которых экономические, политические и организационные, информационное обеспечение государственных органов находится на недостаточном уровне. Поэтому проблемам информатизации в Республике Беларусь уделяется большое внимание с целью создания единого информационного пространства.

Основной задачей правовой информатизации является создание правовой информационной системы, способной предоставлять различным категориям пользователей полную и достоверную правовую информацию. На решение этой задачи направлены следующие решения Главы государства: Указ Президента Республики Беларусь от 30 июня 1997 г. № 338 «О создании Национального центра правовой информации Республики Беларусь», Указ Президента Республики Беларусь № 524 от 30 октября 1998 г. «О мерах по совершенствованию государственной правовой информации», Указ Президента Республики Беларусь № 585 от 1 декабря 1998 г. «О порядке распространения правовой информации в Республики Беларусь», Указ Президента Республики

Беларусь № 195 от 6 апреля 1999 г. «О некоторых вопросах информатизации в Республике Беларусь». В указанный период времени принимается Закон Республики Беларусь «Об электронном документе».

Содержанием государственной политики в сфере информатизации является создание органами государственной власти Республики Беларусь необходимых правовых, экономических, организационных и других условий, содействующих развитию информатизации, защищающих права и интересы граждан и государства при ее осуществлении.

Среди выполняемых задач – необходимость информационно-правового обеспечения деятельности ОВД, субъектов хозяйствования, юридических и физических лиц. Решение этих задач видится в создании информационно-правовой продукции на основе новейших информационных технологий с использованием единой телекоммуникационной среды для обеспечения процессов внутри- и межгосударственного обмена правовой информацией. Основными инструментами процесса телекоммуникационного обмена правовой информацией являются информационные и телекоммуникационные технологии, совокупность программных, технических и организационно-экономических средств решения задач передачи и обработки информации. Кроме того, для обеспечения процессов информатизации в правовой сфере необходима разработка тематических и проблемно ориентированных баз и банков данных.

Формирование баз и банков данных, используемых в процессе информатизации правовой деятельности, всего технического комплекса при их создании и распространении, определение правового статуса информационных ресурсов требуют законодательного закрепления и государственного регулирования. В настоящее время в Беларуси пока еще почти полностью отсутствуют нормативные акты, регулирующие эти процессы.

Применение новейших информационных технологий на основе современных программно-технических комплексов для правовой информатизации должно охватывать такие главные направления права, как правотворческая, правоохранительная и правоприменительная деятельность.

Информатизация в правотворческой деятельности направлена на обеспечение выявления объективной необходимости правового регулирования общественных отношений и деятельности государства по созданию новых правовых норм, изменению или отмене действующих.

Огромное внимание в республике к процессу правотворческой деятельности со стороны общественности, возросшие требования к качеству законотворчества определили необходимость совершенствовать законотворческой процесс на основе использования новейших информационных технологий.

В соответствии с Указом Президента Республики Беларусь от 24 июля 1998 г. № 376 «О создании компьютерного банка данных проектов законов Республики Беларусь» было решено разработать и вести компьютерный банк данных законопроектов Беларуси. Эта задача выполнена Национальным центром правовой информации. Компьютерный банк данных проектов законов Республики Беларусь представляет собой автоматизированную систему централизованного учета, накопления и доведения до сведения субъектов права информации о законодательной деятельности в Республике Беларусь.

Информационную основу компьютерного банка данных проектов законов Республики Беларусь составляют аутентичные копии проектов законов и сопроводительные документы к ним, подготовленные на различных стадиях законотворческою процесса, начиная с предоставления в Палату представителей Национального Собрания и заканчивая подписанием закона Президентом Республики Беларусь.

Кроме того, компьютерный банк данных законопроектов Республика Беларусь позволяет информировать мировую общественность о законотворческой деятельности нашей страны через сеть Интернет. В будущем планируется создавать экспертные системы для автоматизации процесса правотворчества.

В настоящее время действует Закон Республики Беларусь от 10 ноября 2008 г. «Об информации, информатизации защите информации».

Информатизация в правоохранительной деятельности осуществляется для реализации комплекса задач в области сбора, учета, обработки и анализа статистической и оперативно-розыскной информации.

Автоматизация правоохранительной деятельности служит целям взаимодействия правоохранительных органов при расследовании преступлений и борьбе с преступностью. С этой целью сформированы специальные базы данных по направлениям деятельности служб правоохранительных органов, сотрудничающих министерств и организаций. В решениях Координационного научно-технического совета по информатизации правоохранительных органов Республики Беларусь от 31 августа 1995 г. «О необходимости разработки Государственной программы правовой информатизации» поставлена задача создания интегрированных банков данных оперативно-розыскной информации с последующим включением их в единую телекоммуникационную систему информационно-правового пространства государств – участников СНГ.

При современном уровне информированности преступных элементов, возможности их быстрого перемещения и оснащенности современным вооружением становится совершенно необходимым и жизненно важным резкое повышение эффективности работы всех служб ОВД за счет использования современной техники и технологий.

Следует учитывать, что основным методом работы сотрудника ОВД является анализ имеющейся информации и поэтому узловой момент ведения дел – постоянный сбор и учет информации о подозреваемых в совершении преступления, возможности получения аналитических данных по любым срезам информации. Сделать это можно единственным способом – путем достижения высокого уровня компьютеризации всех служб ОВД и создания современных средств передачи информации на расстояния в целях оперативного взаимодействия заинтересованных служб.

Эффективность борьбы с различными видами преступности, предупреждение правонарушений, ускорение раскрытия преступлений во многом зависят от организации работы оперативно-розыскных учетов. Использование перспективных средств вычислительной техники, в том числе глобальных и локальных вычислительных сетей для информационного взаимодействия подразделений и служб, программных продуктов, а также специальных технических средств, обеспечивающих решение специфических задач различных служб ОВД, значительно повышает уровень борьбы с различными видами преступной деятельности.

Вместе с тем мероприятия по компьютеризации органов внутренних дел еще не в полной мере соотносятся со складывающейся криминальной ситуацией и задачам и борьбы с преступностью.

Недостаточно интенсивно идет обновление компьютерной техники подразделений ОВД, имеет место несогласованность в выборе программного и технического обеспечения созданных систем, отсутствует комплексная система эксплуатации технических средств и программной поддержки внедренных автоматизированных информационных систем (АИС). А также недостаточно развита система нормативно-правового регулирования информатизации ОВД, которая необходима для рассмотрения перспективных направлений совершенствования информатизации ОВД.

Раскрытие и расследование преступлений не может обойтись без использования современных информационных технологий, потребность сотрудников ОВД в информации определяется характером правоохранительной деятельности. Уровень информатизации напрямую связан с эффективностью выполнения поставленных задач перед подразделениями ОВД. Мировые тенденции направлены на постоянное увеличение информационных потребностей, в связи с этим возрастают объемы обработки, передачи и хранения информации, появляются новые методы ее получения и анализа, увеличивается производительность технических средств.

С 2010 г. информатизация в ОВД является одним из основных факторов, обеспечивающих полноценное противостояние имеющимся уг-

розам, инновационное развитие в правоохранительной системе, повышение правовой грамотности сотрудников ОВД и информированности населения.

Данный приоритет закреплен Национальной стратегией устойчивого социально-экономического развития Республики Беларусь на период до 2030 года, одобренной Президиумом Совета Министров Республики Беларусь 10 февраля 2015 г. Стратегия определяет принципы государственной политики Республики Беларусь в сфере информатизации и основные направления развития информационного общества с учетом совокупности факторов, влияющих на его прогресс.

Исходя из Стратегии развития информатизации в Республике Беларусь на 2016–2022 гг. можно выделить основные факторы, способствующие развитию информатизации ОВД Республики Беларусь:

устойчивость и эффективность правоохранительной системы;

признание информатизации одним из приоритетов устойчивого развития и совершенствования правового регулирования;

высокий образовательный уровень сотрудников ОВД.

Развитие информатизации ОВД в Республике Беларусь в течение 2011–2015 гг. осуществлялось в соответствии со Стратегией развития информационного общества на период до 2015 года, утвержденной постановлением Совета Министров Республики Беларусь от 9 августа 2010 г. № 1074, и разработанными для ее выполнения Национальной программой ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы, отраслевыми и региональными программами информатизации.

В целом информатизация ОВД в Беларуси находится на достаточно высоком уровне. Созданный в 2007 г. единый государственный банк данных правонарушений значительно ускорил и облегчил работу правоохранительных органов. Также в данный период были созданы и приняты в пользование ОВД автоматизированные информационные системы, такие как: АИС «Паспорт», АИС «ГАИ-Центр», АИС «ФР-оповещение», АИС «Пасажиропоток» и иные.

На государственном уровне практически создан базовый комплекс электронного правительства, в который входят такие компоненты, как: общегосударственная автоматизированная информационная система (ОАИС), система межведомственного электронного документооборота.

Министерство внутренних дел в целом организовало работу в соответствии с мировыми тенденциями развития системы массовых коммуникаций. Практически все ОВД представлены в сети Интернет.

Сегодня уже у граждан есть возможность не только направлять в ОВД обращения через сеть Интернет, но и получать сведения о рассмотрении направленных обращений.

В настоящее время ОВД в электронном виде оказывают следующие государственные услуги: прием, регистрацию и рассмотрение сообщений о преступлениях и иной информации о правонарушениях; регистрацию автотранспортных средств и прицепов к ним; предоставление сведений об административных правонарушениях в области дорожного движения. Скоро добавятся услуги по лицензированию и получению справок.

Сведения о возможности получения указанных государственных услуг, информация о порядке приема заявлений, сообщений и о порядке личного приема граждан в ОВД, шаблоны необходимых документов, нормативные правовые акты, местонахождения ОВД размещены в сети Интернет.

Основными факторами, замедляющими развитие информатизации ОВД, являются:

инертность при решении вопросов информатизации;

отсутствие мотиваций, необходимых для внедрения информационно-коммуникационных технологий;

недостаточный уровень инвестиций в информационно-коммуникационные технологии со стороны государства;

слабое использование возможностей государственно-частного партнерства, в том числе в области обучения и исследований.

Для развития информатизации ОВД в 2016–2022 гг. можно определить следующие задачи:

эффективное внедрение передовых информационно-коммуникационных технологий во все структуры правоохранительной деятельности;

совершенствование системы управления и правового регулирования процессами информатизации;

дальнейшее совершенствование информационно-коммуникационной инфраструктуры ОВД;

обеспечение прозрачности и удобства коммуникаций между гражданами и ОВД путем повсеместного перевода данных коммуникаций в электронную форму;

дальнейшее формирование единого информационного пространства для оказания электронных услуг на основе интеграции информационных систем;

создание условий для использования электронных услуг, стимулирующих их востребованность;

обеспечение непрерывности, безотказности, безопасности информационных потоков.

При решении данных задач следует руководствоваться принципами:

определение ведущей роли государства в формировании политики информатизации и стимулировании применения информационно-коммуникационных технологий в правоохранительной деятельности;

открытость управления, свобода доступа к информации за исключением информации, распространение которой является ограниченной;

развитие партнерства в сфере информатизации ОВД;

вовлечение в процесс информатизации ОВД всех слоев и социальных групп населения, ликвидация цифрового неравенства;

обеспечение нового уровня цифровой грамотности сотрудников ОВД.

Критерием успешности реализации данных направлений может явиться готовность ОВД к переходу на электронный документооборот к 2022 г.

Стремительное развитие информационной сферы ОВД, основанной на использовании современных информационных технологий, порождает большое количество проблем правового, управленческого, организационного, технического и финансового характера.

В заключение хотелось бы отметить, что одним из путей решения указанных вопросов является качественное совершенствование нормативного правового и организационного регулирования информатизации в ОВД. В связи с этим основное внимание в работе должно уделяться исследованию особенностей правого обеспечения, разработке и использованию современных информационных технологий в деятельности ОВД.

УДК 004.056.5

Е.Б. Кузин

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ УЧРЕЖДЕНИЙ ФСИН РОССИИ

Одной из задач развития систем информационного обеспечения учреждений уголовно-исполнительной системы (УИС) является совершенствование систем информационной безопасности и защиты информации. Применение криптографических средств защиты информации – важная составляющая часть создания комплексной системы защиты информации. К средствам криптографической защиты информации относят: средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования.

Современная криптография является областью знаний, связанной с решением таких проблем безопасности информации, как конфиденциальность, целостность, аутентификация. Достижение этих требований безопасности информационного взаимодействия и составляет основные цели криптографии.

Обеспечение конфиденциальности – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В зависимости от контекста вместо термина «конфиденциальная» могут выступать термины «секретная», «частная», «ограниченного доступа» информация.

Обеспечение целостности – гарантирование невозможности несанкционированного изменения информации. Для гарантии целостности необходим простой и надежный критерий обнаружения любых манипуляций с данными (вставка, удаление и замена).

Обеспечение аутентификации – разработка методов подтверждения подлинности сторон (идентификация) и самой информации в процессе информационного взаимодействия. Информация, передаваемая по каналу связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т. д.

Современная криптография включает в себя четыре раздела: симметричные ключи, открытые ключи, электронно-цифровая подпись, системы управления ключами.

Существуют две методологии криптографической обработки информации с использованием ключей – симметричная и асимметричная. Симметричная (секретная) методология предусматривает, что и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия. Если ключ не был скомпрометирован, то при расшифрке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию.

При асимметричной (открытой) методологии шифрования документ шифруется одним ключом, а расшифровывается другим. Каждый из участников передачи информации самостоятельно генерирует два случайных числа секретный (закрытый) и открытый ключи. Открытый ключ передается по открытым каналам связи другому участнику процесса криптозащиты, а секретный ключ хранится в секрете. Отправитель шифрует сообщение открытым ключом получателя, а расшифровать его может только владелец секретного ключа.

Огромным преимуществом публичной криптографии также является возможность использования электронной цифровой подписи (ЭЦП), которая позволяют получателю сообщения удостовериться в личности отправителя сообщения, а также в целостности (верности) полученного сообщения.

Еще одно важное преимущество использования криптографии состоит в том, что применяется так называемая хэш-функция, которая дейст-

вует таким образом, что в случае какого-либо изменения информации, пусть даже на один бит, результат хэш-функции будет совершенно иным. С помощью хэш-функции и закрытого ключа создается подпись, передаваемая программой вместе с текстом. При условии использования надежной формулы хэш-функции невозможно вытащить подпись из одного документа и вложить в другой либо каким-то образом изменить содержание сообщения. Любое изменение подписанного документа сразу же будет обнаружено при проверке подлинности подписи.

Цифровые сертификаты ключей упрощают задачу определения принадлежности открытых ключей предполагаемым владельцам. Цифровой сертификат ключа – это информация, прикрепленная к открытому ключу пользователя, помогающая другим установить, является ли ключ подлинным и верным. Цифровые сертификаты нужны для того, чтобы сделать невозможной попытку выдать ключ одного человека за ключ другого. Сертификат – это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется электронной цифровой подписью удостоверяющего центра сертификации.

Сертификаты выдаются конкретному субъекту и содержат его открытый ключ. Подлинность самого сертификата гарантируется его эмитентом, то есть выпустившей организацией, которой изначально доверяют все участники переписки.

Задачами развития систем информационного обеспечения учреждений УИС являются:

внедрение перспективных информационных технологий, средств вычислительной техники и телекоммуникаций, локальных вычислительных сетей, типовых программных средств и автоматизированных рабочих мест для обобщения и анализа информации, информационной поддержки оперативно-служебной деятельности;

совершенствование инфраструктуры информационно-телекоммуникационного и других видов обеспечения функционирования и развития системы передачи и обработки данных, систем информационной безопасности и защиты информации.

К средствам криптографической защиты информации (СКЗИ) относят средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования, средства изготовления ключевых документов и сами ключевые документы.

Служебная деятельность территориальных органов и учреждений УИС связана с хранением и обработкой персональных данных различных категорий, к защите которых законодательством РФ выдвигается ряд требований. Для их выполнения необходимо формирование модели

угроз персональным данным и разработки на ее основе системы защиты персональных данных, в состав которой должно входить средство криптографической защиты информации. К СКЗИ, внедренному в систему защиты персональных данных, выдвигаются следующие требования:

штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к нему требований;

сертифицировано в системе сертификации ФСБ России криптосредства для обеспечения безопасности персональных данных при их обработке.

Криптографическое средство, в зависимости от обеспечиваемого им уровня защиты, относится к одному из шести классов (КС1, КС2, КС3, КВ1, КВ2, КА1). Внедрение криптосредства того или иного класса в систему защиты обусловливается категорией нарушителя, которая определяется оператором в модели угроз.

Комплексный подход к защите информации подразумевает использование межсетевых экранов, антивирусов и фаерволов, а также включает разработку модели угроз информационной безопасности (ИБ), выработку необходимых политик ИБ, назначение ответственных за информационную безопасность, контроль электронного документооборота, контроль и мониторинг деятельности сотрудников и др.

Главное назначение системы электронного документооборота (СЭД) – это организация хранения электронных документов, а также работы с ними. Использование системы электронного документооборота позволяет значительно повысить производительность труда делопроизводственного персонала учреждений УИС, сокращает время, затрачиваемое на процессы документооборота. В СЭД реализованы надежные средства разграничения полномочий и контроля за доступом к документам. ЭЦП выступает как основной способ защиты и придания юридической силы информации. В СЭД используется простая электронная подпись (сочетание имени пользователя и пароля) и усиленная квалифицированная электронная подпись (электронный ключ с сертификатом электронной подписи) в соответствии с Федеральным законом Российской Федерации «Об электронной подписи».

Электронные торги и аукционы госзаказа проводятся на специализированных площадках (сайтах в глобальной сети Интернет). Для регистрации на площадках необходима электронная цифровая подпись, выпущенная специально для госзаказа. Получить ее можно в удостоверяющих центрах. ЭЦП необходима, чтобы поставщики были уверены, что работают и контактируют с реальными предложениями и участвуют в активных торгах. Контракты, содержащие электронную подпись, имеют юридическую значимость и содержат в себе полную юридиче-

скую силу только после соглашения и подписания контракта обеими сторонами – поставщиком и клиентом.

«КриптоПро CSP» представляет собой криптопровайдер – программный модуль, позволяющий осуществлять криптографические операции в операционных системах, управление которым происходит с помощью функций CryptoAPI. «КриптоПро CSP» поддерживает российские криптографические алгоритмы (ГОСТ) и имеет сертификаты ФСБ России.

КриптоПро CSP предназначен:

для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной цифровой подписи в соответствии с отечественными стандартами ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;

обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты в соответствии с ГОСТ 28147-89;

обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;

контроля целостности системного и прикладного программного обеспечения в целях защиты от несанкционированных изменений и нарушений правильности функционирования;

управления ключевыми элементами системы в соответствии с регламентом средств защиты.

«КриптоПро CSP» поддерживает следующие типы ключевых носителей:

электронный USB-ключ или смарт-карту eToken;

процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК) с использованием считывателя смарткарт-GemPlus GCR-410;

таблетки Touch-Memory DS1993-DS1996 с использованием устройств «Аккорд 4+», электронный замок «Соболь» или устройство чтения таблеток Touch-Memory DALLAS;

реестр Windows.

Основные функции, реализуемые «КриптоПро CSP»:

генерация секретных (256 бит) и открытых (1024 бита) ключей ЭЦП и шифрования;

формирование секретных ключей на различных типах носителей;

криптографическая защита информации (система электронной цифровой подписи на базе асимметричного криптографического алгоритма);

хеширование данных;

шифрование данных;

имитозащита данных;

формирование электронной цифровой подписи;

опциональное использование пароля (PIN-кода) для дополнительной защиты ключевой информации;

реализация мер защиты информации пользователя от несанкционированного доступа.

Аппаратно-программный комплекс обеспечивает криптографическую защиту информации (в соответствии с ГОСТ 28147–89), передаваемой по открытым каналам связи, между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры. Комплекс предназначен для организации удаленного доступа к корпоративным ресурсам, а также защиты компьютера пользователя от несанкционированного доступа извне.

Комплекс имеет два компонента: абонентский пункт и межсетевой экран.

Абонентский пункт подключается к корпоративным ресурсам и обеспечивает обмен информации в зашифрованном виде. Поддерживается работа с криптопровайдерами «Код Безопасности CSP» (входит в состав программного обеспечения абонентского пункта) и «КриптоПро CSP» (устанавливается отдельно).

Для защиты от проникновения со стороны сетей общего пользования комплекс «Континент 3.7» обеспечивает фильтрацию принимаемых и передаваемых пакетов по различным критериям (адреса отправителя и получателя, протоколы, номера портов, дополнительные поля пакетов и т. д.). Осуществляет поддержку VoIP, видеоконференций, ADSL, Dial-Up и спутниковых каналов связи, технологии NAT/PAT для сокрытия структуры сети.

Для подключения к корпоративным ресурсам абонентский пункт устанавливает соединение с сервером доступа, расположенным в корпоративной сети. Сервер доступа определяет права пользователя на доступ к корпоративным ресурсам. Аутентификация пользователя выполняется с помощью метода асимметричного шифрования.

Для взаимодействия абонентского пункта и сервера доступа используют следующие сертификаты открытых ключей:

сертификат пользователя – для аутентификации пользователя на сервере доступа;

сертификат сервера доступа – для аутентификации сервера доступа;

сертификат корневого центра сертификации – для подтверждения подлинности сертификата пользователя и сертификата сервера доступа.

Межсетевой экран обеспечивает фильтрацию IP-пакетов сетевого трафика компьютера, на котором установлен абонентский пункт.

Материалы статьи могут использоваться в учебном процессе при изучении дисциплины «Информационная безопасность» по специализации «Правоохранительная деятельность».

УДК 004.94

В.В. Лавренов

ПОСТРОЕНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ДЛЯ ОЦЕНКИ ОПЕРАТИВНОЙ ОБСТАНОВКИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

В настоящее время информационно-коммуникационные технологии используются практически во всех сферах жизни, в том числе и в правоохранительной деятельности. Развитие практики борьбы с преступностью, обеспечение безопасности и общественного порядка показывает, что успешное решение задач, стоящих перед органами внутренних дел, во многом определяется уровнем информационного и аналитического обеспечения их деятельности.

Аналитическая работа предусматривает выяснение причин и условий, обстоятельств, обусловивших конкретное состояние преступности в республике, области, районе, городе и результаты работы органов внутренних дел. Состояние оперативной обстановки является одним из объективных показателей деятельности структурных подразделений МВД Республики Беларусь. Традиционно изменения состояния оперативной обстановки связываются главным образом с состоянием, динамикой и структурой преступности. Представляется, что такой подход не совсем точен, поскольку преступность является основным, но не единственным объектом правового воздействия органов внутренних дел. В числе основных задач МВД Республики Беларусь определены организация и осуществление мер по предупреждению и пресечению преступлений и административных правонарушений, выявлению, раскрытию и расследованию преступлений.

Современные теоретические и прикладные аспекты организации деятельности органов внутренних дел по осуществлению ими возложенных на них задач и функций нуждаются в корректировке и уточнении. В органах внутренних дел имеет место практика изучения и оценки оперативной обстановки исключительно на основе статистических данных о фактическом состоянии преступности, удельном весе различных видов преступлений, уровне их раскрываемости и роли подразделений и служб в предупреждении и раскрытии преступлений. Это весьма ограниченный подход, который мешает принятию эффективных управленческих решений и не способствует выработке адекватных мер борьбы с преступностью. Надо знать, что оперативная обстановка – это совокупность взаимосвязанных условий, складывающихся из географического положения территории, находящейся в зоне ответственности ОВД, ее социально-

экономических особенностей, состояния общественно-политической активности населения, демографических особенностей, состояния преступности и уровня нарушений общественного порядка, сил и средств ОВД, задействованных в борьбе с преступностью и в обеспечении охраны общественного порядка, и результативности их деятельности.

Таким образом, оперативная обстановка должна рассматриваться как сложная система, состоящая из двух основных блоков – внешней среды (внешние условия функционирования ОВД) и самого органа внутренних дел, включая средства, методы и результаты правоохранительной деятельности. Компонентами оперативной обстановки являются: географическое положение; социально-экономические особенности; состояние общественно-политической активности населения; демографические особенности; состояние преступности и общественного порядка; силы и средства ОВД, задействованные в борьбе с преступностью и в обеспечении охраны общественного порядка.

Для оценки оперативной обстановки предлагается использовать системы поддержки принятия решений (СППР). Роль СППР заключается не в замене человека, а в повышении эффективности его работы. Цель СППР заключается не в автоматизации процесса принятия решения, а в осуществлении взаимодействия между системой и человеком в процессе принятия решений.

Системы поддержки принятия решений должны иметь возможность адаптироваться к изменению вычислительных моделей, общаться с пользователем на специфическом для управляемой области языке, представлять результаты в такой форме, которая способствовала бы пониманию результатов.

Основными компонентами СППР являются: база знаний (БЗ), база данных (БД), механизм логического вывода, блок обучения, блок понимания ограниченного естественного языка, блок введения и управления БД и БЗ, управляющий блок.

База знаний подсистемы, имитирующей решения задач экспертом, в этом случае представляется совокупностью пар «ситуация – пример», «решение – пример». При этом вывод решения в конкретной ситуации будет основан на сравнении описания текущей ситуации с описаниями ситуации из ситуационной базы знаний, поиске наиболее близкой ситуации-примера и применении ее способа решения к данной текущей ситуации.

Пусть задано:

группа экспертов $E_1, E_2, \ldots, E_m$;

система критериев $C_1, C_2, \ldots, C_k$, влияющих на оперативную обстановку;

ситуация-пример S_1, S_2, …, S_n,

решение ситуации-примера U_1, U_2, …, U_n.

Требуется разработать метод, который бы на основе субъективной экспертной информации вычислял веса критериев, проводил ранжирование и принимал решение о предпочтительном выборе ситуации для изменения наилучшим образом оперативной обстановки.

Сложность в реализации заключается в том, что:

в БЗ невозможно предусмотреть все возможные ситуации, складывающиеся в предметной области;

текущая ситуация может отличаться от имеющейся в базе знаний, следовательно, решение для нее также должно быть отличным от известного «решение – пример».

Необходимо разработать способ формализации представления ситуаций и решений, который позволит получать решения для текущих ситуаций на основе формальных преобразований «пример – решение».

Учитывая основные свойства задачи (трудность формализации, субъективность исходной информации, неопределенность цели и т. п.) для определения приоритетов критериев, наиболее подходящим для ее решения является подход, основанный на анализе иерархий. Гибкая методология данного подхода учитывает материальные и нематериальные факторы, позволяет работать как с количественными параметрами, так и с качественными характеристиками, с объективными данными и экспертными оценками.

Метод анализа иерархий использует в качестве языка формализации нечеткую логику.

В соответствии с описанной выше методологией необходимо построить модель задачи в виде некоторой иерархической структуры, разработать алгоритмы вычисления весов (для критериев), разработать алгоритм выбора принятия решений (выбор наиболее предпочтительного решения ситуации-примера). Возможность влиять на характеристики, которые определяют степень достижения цели, формализуется как выбор значения управляющего параметра. При этом управляющий параметр может быть числом, вектором, может быть элементом конечного множества или иметь более сложную математическую природу.

Для оценки возможных решений используются различные критерии. Под критериями понимаются, во-первых, показатели, характеризующие степень приближения к цели каждого из вариантов ее достижения, во-вторых, показатели, служащие для объективного сопоставления различных вариантов решения и выбора из них наиболее эффективного. Критерии могут выражаться в каких-либо показателях использования ресурсов или времени. При выборе и использовании критериев существуют следующие сложности. Во-первых, критерии не всегда могут быть выражены определенными количественными показателями, а во-вторых, чаще всего используется не один критерий выбора альтернатив. Как правило, альтернативы оцениваются по целому комплексу критериев. Для оценки управленческих решений необходимо применять систему критериев.

Необходимость использования совокупности количественных и качественных критериев ставит вопрос о приведении их к «общему знаменателю». Тем самым ставится задача агрегирования частных критериев или выбора одного критерия в качестве основного.

Динамика реальных сложных систем такова, что большинство формальных моделей дают только качественную картину. Например, не существует математических моделей, позволяющих достаточно точно спрогнозировать состояние преступности одноразовым решением. Разнообразные формальные методы управления сложными системами во многих случаях не могут дать однозначных ответов. Хотя процесс построения СППР является очень сложным, тем не менее СППР является инструментом повышения эффективности использования информационных ресурсов в деятельности органов внутренних дел в борьбе с преступностью и по профилактике правонарушений.

УДК 351/354

В.Н. Лебедев

РАЗВИТИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

В современном мире право физического лица на личную тайну закреплено конституциями всех развитых государств. Суть этого права заключается в том, что только сам человек, владеющий некими сведениями о себе, может решать, подлежат они разглашению или нет.

В случае неправомерного разглашения таких сведений их владелец имеет право на защиту своих нарушенных интересов. В ряде стран, в том числе в России, неправомерное разглашение персональных данных определенного характера является уголовным преступлением. Однако в судах все чаще рассматриваются споры о разглашении персональных данных (ПДн) физических лиц. Данная проблема, в том числе, связана с широким использованием информационных систем для обработки персональных данных (ИСПДн).

В соответствии с нормами федерального законодательства сведения о гражданах после обработки в органах внутренних дел вносятся в банки данных. Министерство внутренних дел Российской Федерации является оператором, организующим и осуществляющим обработку ПДн, а следовательно, обязано принимать установленные законом ме-

ры для их защиты. С этой целью МВД России создана система защиты ПДн, которая представляет собой совокупность следующих элементов: 1) персональные данные и носители таких данных; 2) должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн; 3) способы, техника и средства защиты ПДн; 4) мероприятия, проводимые в целях защиты ПДн. Кратко рассмотрим эти элементы.

Персональные данные, которые обрабатывают органы внутренних дел, определены прежде всего ч. 3 ст. 17 Федерального закона РФ «О полиции», а также нормами других законодательных актов. Кроме того, в различных подразделениях и службах органов внутренних дел (медицинские учреждения, кадровые, финансово-экономические, тыловые подразделения) обрабатываются ПДн сотрудников (работников), а также данные членов их семей.

В соответствии с требованиями приказа МВД России руководители (начальники) территориальных органов МВД России, руководители структурных подразделений территориальных органов МВД России, эксплуатирующие ИСПДн, обеспечивают выполнение правовых, организационных и технических мер, направленных на обеспечение безопасности ПДн, и являются ответственными за соблюдение требований по защите ПДн при их автоматизированной обработке в подчиненном органе внутренних дел.

Кроме указанных выше должностных лиц, ответственными за соблюдение требований по защите ПДн являются администраторы информационных систем персональных данных, пользователи, непосредственно обрабатывающие ПДн, инженерно-технический персонал, имеющий доступ к элементам ИСПДн.

Координацию и контроль деятельности по защите ПДн осуществляет Департамент информационных технологий связи и защиты информации МВД России (ДИТСиЗИ МВД России), в территориальных органах МВД России – подразделения информационных технологий, связи и защиты информации или должностные лица, назначенные ответственными за проведение мероприятий по технической защите ПДн, а также ответственными за организацию обработки ПДн в подразделении.

К способам и методам защиты персональных данных в ИСПДн органов внутренних дел относятся:

способы и методы защиты ПДн от несанкционированного доступа к ПДн (методы и способы защиты информации от несанкционированного доступа);

способы и методы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к ПДн (методы и способы защиты информации от утечки по техническим каналам).

В целях защиты ПДн, обрабатываемых в ИСПДн, применяются средства:

от несанкционированного доступа при передаче по каналам связи сетей общего и (или) международного обмена (средства управления и разграничения доступа пользователей к ПДн; обеспечения регистрации и учета действий с информацией; обеспечения целостности данных; антивирусной защиты; межсетевого экранирования; анализа защищенности; обнаружения вторжений; криптографической защиты ПДн);

от утечки по техническим каналам (генераторы активного акустического, виброакустического и электромагнитного маскирующего зашумления, сетевые помехоподавляющие и телефонные фильтры, а также средства экранирования и заземления и др.).

Выбор средств защиты информации осуществляется в соответствии с требованиями Федеральной службы по техническому и экспертному контролю и ФСБ России: применяемые средства защиты информации должны пройти оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

Законодатель определяет некоторые меры, направленные на обеспечение безопасности ПДн. Например, к основным из них относятся: определение угроз безопасности ПДн, применение организационных и технических мер по обеспечению безопасности ПДн, оценка эффективности принимаемых мер по обеспечению безопасности ПДн и др. Содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн устанавливаются ФСБ России и ФСТЭК России в соответствии с их полномочиями.

Мероприятия, проводимы в органах внутренних дел в целях обеспечения безопасности ПДн, можно разделить на две группы:

1. Управленческие (или организационно-управленческие). Направлены на создание системы технической защиты ПДн и управления ею. Ответственными за организацию проведения данных мероприятий являются руководитель территориального органа МВД России и руководители структурных подразделений, обрабатывающих ПДн.

2. Организационно-технические (по обеспечению безопасности ПДн и аттестации ИСПДн по требованиям защиты информации). Обработка ПДн в ИСПДн органов внутренних дел должна осуществляться после завершения работ по созданию системы технической защиты ПДн, аттестации и вводу в эксплуатацию ИСПДн.

Таким образом, мы рассмотрели систему защиты ПДн, существующую в органах внутренних дел Российской Федерации. Однако, как любая организационная система, система защиты ПДн органов внутренних дел требует своего развития и совершенствования. Попробуем предложить основные направления развития данной системы.

1. Совершенствование системы подготовки руководителей в области обработки и защиты ПДн. Как показывает практика, руководители территориальных органов и структурных подразделений далеко не в полной мере обладают необходимыми знаниями и организационными навыками и умениями в области защиты ПДн.

Академия управления МВД России имеет многолетний опыт, есть необходимая материально-техническая база для подготовки руководителей органов внутренних дел разного уровня в области информационной безопасности, в том числе и защиты ПДн.

2. Дальнейшее развитие органов аттестации объектов информатизации на соответствие требованиям безопасности информации, получение территориальными органами МВД России на региональном уровне лицензий на деятельность по технической защите конфиденциальной информации.

3. Максимальная унификация (типизация) информационных систем обработки персональных данных в органах внутренних дел с целью упрощения аттестации на соответствии требованиям защиты информации.

4. Применение в масштабах ведомства унифицированных технических средств и систем защиты ПДн, обрабатываемых в ИСПДн, в целях сокращения расходов на построение систем защиты ИСПДн.

5. Сокращение перечня документов, необходимых для аттестации ИСПДн на соответствие требованиям защиты информации, упрощение самой процедуры аттестации.

В заключение хочется отметить, что эффективная деятельность органов внутренних дел предполагает обеспечение прав и свобод человека и гражданина, что неразрывно связано с обеспечением конфиденциальности личных данных граждан и сведений об их частной жизни, а для этого необходимо совершенствование системы защиты персональных данных в ОВД РФ.

УДК 343

А.Н. Лепёхин

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Анализ характера совершаемых преступлений свидетельствует, что современный этап развития общественных отношений характеризуется, несмотря на предпринимаемые правоохранительными органами меры, эволюцией противоправной активности в части появления новых способов криминальной деятельности, коммуникаций между преступ-

никами и смещения акцентов в пользу высокотехнологичных решений достижения преступного результата. Указанные факторы являются серьезным препятствием динамичному социально-экономическому развитию государства.

В этой связи становится актуальным вопрос о формировавании единых и совершенствании имеющихся правовых основ, актуализации, с учетом современных требований, содержания и методики проведения информационно-аналитической работы (ИАР), а также разработки новых подходов ее проведения в правоохранительных органах. При реализации указанных направлений необходимо смещение векторов проведения правоохранительными органами ИАР с информацинной составляющей в пользу совершенствования аналитического обеспечения данной деятельности. Современный этап развития общества характеризуется резким ростом генерируемой информации по различным направлениям, в том числе и имеющей значение для оперативно-служебной деятельности правоохранительных органов. Сегодня в условиях так называемой информационной избыточности вопрос о получении информации (при обеспечении ее свойств – оперативности, достоверности и достаточности) остро не стоит. Более актуальным является ее своевременная аналитическая обработка и принятие на ее основе соотвествующих управленческих решений.

Разработка рекомендаций по правовому регулированию информационно-аналитической работы направлены на формирование и закрепление единых подходов к системе и содержанию нормативных правовых актов, регулирующих отношения в сфере информационно-аналитического обеспечения правоохранительной деятельности, а также на создание необходимых условий для действенной охраны и защиты прав, свобод и законных интересов личности, интересов общества и государства.

Перечисленные обстоятельства позволяют сформировать следующие концептуальные положения рассматриваемой предметной области.

Объектом правового регулирования являются урегулированные законодательством общественные отношения, складывающиеся в сфере правового обеспечения информационно-аналитической деятельности правоохранительных органов в государстве.

Целью подготовки рекомендаций является разработка единых организационно-правовых подходов к информационной и аналитической составляющей правоохранительной деятельности.

Задачами совершенствования и гармонизации законодательства государства, регулирующего отношения в сфере информационно-аналитического обеспечения правоохранительной деятельности, являются:

раскрытие особенностей правового регулирования отношений в рассматриваемой сфере (предмет, метод, способ и тип регулирования);

определение содержания и характеристик информационно-аналитического обеспечения правоохранительной деятельности;

формирование перечня правоохранительных органов (адресатов рекомендаций по правовому регулированию);

разработка системы нормативных правовых актов, регламентирующих как отдельные вопросы, так и информационно-аналитическую работу в целом.

Решение указанных задач позволит внедрить общие подходы к правовому регулированию информационно-аналитического обеспечения правоохранительной деятельности, унифицировать национальное законодательство государства, регулирующее правоотношения в указанной сфере, повысить эффективность правоприменительной деятельности субъектов обеспечения национальной безопасности.

Методологической основой разработки является диалектико-материалистический метод, а также комплекс методов:

общетеоретического уровня – системно-структурный, восхождение от абстрактного к конкретному;

эмпирического уровня – наблюдение, описание, сравнения (в том числе изучение и анализ нормативных правовых актов государства, регламентирующих деятельность уполномоченных субъектов в сфере обеспечения национальной безопасности, а также модельного законодательства Организации Договора о коллективной безопасности и Содружества Независимых Государств);

общелогических – анализ, синтез, обобщение;

конкретно-социологического уровня – интервьюирование специалистов в области правового регулирования отдельных сфер обеспечения национальной безопасности, проведение экспертных оценок;

специальных – формально-юридический, сравнительно-правовой, толкования правовых норм.

Таким образом, постановка указанных проблем предопределяет актуальность проводимого юридического анализа и разработки на основе полученных результатов рекомендаций и предложений по совершенствованию правового регулирования рассматриваемой сферы с учетом научно обоснованных положений юридической науки и с учетом базирующейся на обобщении и анализе практики правоохранительных органов.

УДК 343

С.А. Медведев

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННО-ПОИСКОВОЙ ДЕЯТЕЛЬНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Развитие информационных технологий в современном мире привело к тому, что объемы информации, циркулируемой в сети, постоянно растут. Сведения о гражданах, событиях и обстоятельствах, представляющих интерес для выполнения оперативно-розыскной деятельности (ОРД), концентрируются в многочисленных ресурсах сети. В этих условиях знания особенностей проведения оперативно-розыскных мероприятий (ОРМ) открывают перед оперативными подразделениями новые возможности в противодействии преступности.

В настоящее время обширно распространяются среди пользователей сети Интернет сервисы IP-телефонии, которые обеспечивают голосовую связь абонентов с дополнительными возможностями (визуальный контакт, конференц-связь). Очевидно, что оперативно-розыскной контроль подобных переговоров удовлетворяет признакам не только контроля в сетях электросвязи, но и такого оперативно-розыскного мероприятия, как слуховой контроль.

С развитием форм сетевого общения появляются новые методы проведения опроса. В киберпространстве имеются условия для получения сведений о криминальной активности лица при изучении сообщений в местах сетевого общения. В указанных местах может проводиться опрос лиц, которым известны сведения, представляющие оперативный интерес.

Особое содержание в сетевом пространстве приобретает ОРМ «оперативное отождествление». Как правило, такое мероприятие базируется на сравнении полученных из оперативных источников данных о личности фигуранта, который причастен к преступной деятельности, со сведениями о субъекте, сетевая активность которого изучается. К формам отождествления личности можно отнести опознание по фотографиям, которые размещают на персональных страницах социальных сетей, по указанным там же автобиографическим данным, по используемым псевдонимам, адресам электронной почты, номерам ICQ, IP-адресам.

Функционирование в сети Интернет мощных справочно-информационных систем создает условия для наведения справок путем прямого изучения размещенных в них документов, а также направления по электронной почте запросов в организации, у которых есть интересующие сведения.

Одним из наиболее сложных ОРМ при реализации в киберпространстве является оперативный эксперимент. Международной практике известны примеры осуществления оперативного эксперимента, которые связаны с созданием в сетевом пространстве негласно контролируемых объектов, представляющих интерес для преступников.

Ограниченное применение возможно и для контроля почтовых отправлений. Такие действия в конкретных ситуациях позволяют не только получать важные фактические данные, но и создавать препятствия обмену информацией между изучаемыми лицами.

Рост количества торговых операций, которые реализуются через сеть Интернет, заставляет расширять практику использования и ОРМ «проверочная закупка» и «контролируемая поставка» в целях выявления преступлений в сфере торговли и в сфере распространения запрещенных к обороту объектов. К примеру, в практике известно успешное применение проверочной закупки в ходе реализации контролируемых поставок наркотических средств.

Решение задач по поиску, отбору и систематизации оперативной информации предполагает применение информационных систем, позволяющих существенно расширить круг информации, необходимой для аналитической работы, и распространяется в нескольких направлениях.

Важной стороной информационного обеспечения деятельности оперативного сотрудника является организация содействия в анализировании имеющейся информации для формирования решений. Экспертные системы, применяющиеся в оперативной работе, занимают особое место среди информационного обеспечения.

Существует несколько видов экспертных систем раскрытия и расследования преступлений: выявления скрытых преступлений, прогнозирования преступлений, поиска и установления личности преступника.

В деятельности подразделений ОВД используется специализированное программное обеспечение, которое ориентировано на непосредственное применение при осуществлении ОРМ в направлении борьбы с информационной преступностью.

Следовательно, в информационном пространстве (при учете его социальной составляющей) на сегодняшний день может осуществляться практически любое из предусмотренных законом оперативно-розыскное мероприятие. В то же время при подготовке и проведении таких мероприятий оперативный сотрудник обязан учитывать специфику сетевого информационного пространства и сформировавшейся в нем криминогенной среды.

УДК 004.056

М.К. Новиков, Т.Ф. Старовойтова

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ЕДИНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТАМОЖЕННЫХ ОРГАНОВ РЕСПУБЛИКИ БЕЛАРУСЬ

В середине 2016 г. Государственным таможенным комитетом Республики Беларусь была введена единая автоматизированная информационная система таможенных органов (ЕАИС ТО) Республики Беларусь. Данная система включает в себя 40 информационных систем. Основные из них:

автоматизированная подсистема «Транзит Таможенного союза»;

Национальная автоматизированная система электронного декларирования;

автоматизированная информационная система автоматизации операций таможенного оформления и контроля, ведения базы данных таможенной информации на уровне пунктов таможенного оформления и таможни;

автоматизированная система управления рисками;

автоматизированная подсистема «Модуль автоматической рассылки сообщений».

Система защиты информации (СЗИ) ЕАИС ТО Республики Беларусь предназначена для обеспечения конфиденциальности, целостности и доступности информации ограниченного распространения и другой критичной информации, обрабатывающейся в ЕАИС ТО, а также для обеспечения защиты информации при взаимодействии ЕАИС ТО с внешними информационными системами.

СЗИ ЕАИС ТО включает в себя следующие подсистемы: управления пользователями и разграничения доступа, аудита событий, защиты каналов связи, криптографической защиты информации, антивирусной защиты, резервного копирования и восстановления работоспособности.

В конце 2016 г. система защиты информации ЕАИС ТО Республики Беларусь была аттестована. Это означает, что система защиты информации ЕАИС ТО Республики Беларусь класса Б2 (по СТБ 34.101.30-2007) соответствует всем требованиям законодательства Республики Беларусь в области защиты информации, а именно: Закону Республики Беларусь «Об информации, информатизации и защите информации», приказу Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации».

Но, несмотря на все принимаемые меры по защите информации, найти в огромном массиве данных конфиденциальную информацию и выявить факт записи ее на внешнее запоминающее устройство или передачи по сети, электронной почте очень сложно. DLP-система (систе-

ма предотвращения утечки информации) поможет автоматизировать этот процесс.

DLP-система создает защищенный цифровой контур вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию. Контролируемым является информационный поток, состоящий из документов, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываются на принтере, отправляются по сети и по почте и т. д.

Все DLP-системы по способности блокирования конфиденциальной информации можно разделить на активные и пассивные. Первые умеют блокировать передаваемую информацию, вторые, соответственно, такой способностью не обладают. Первые системы гораздо лучше борются со случайными утечками данных, но при этом способны допустить нечаянную остановку передачи важного документа в организации, вторые же безопасны, но подходят только для борьбы с систематическими утечками.

Как правило, по сетевой архитектуре DLP-системы используют совместно шлюзовые и хостовые компоненты (серверная часть и агенты, работающие на рабочих станциях сотрудников). Агенты только передают всю информацию серверной части. Поступившая от агентов информация анализируется ресурсами сервера.

Таким образом, внедрение DLP-системы в таможенные органы Республики Беларусь позволит отследить и проанализировать основные каналы передачи конфиденциальной информации и выявить факты нарушения информационной безопасности.

УДК 004.832+351.759.6

Ю.Б. Савва

МЕТОДИКА ВЫЯВЛЕНИЯ СРЕДСТВАМИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ УЧАСТНИКАМИ ВИРТУАЛЬНЫХ СОЦИАЛЬНЫХ СЕТЕЙ

В виртуальных социальных сетях (ВСС), завоевавших пользователей интернета в последнее десятилетие, нашли свое отражение как положительные, так и негативные черты современного общества. К числу последних относятся: пропаганда терроризма и экстремизма, привлечение к употреблению наркотических и психотропных веществ, вовлечение в секты, понуждение к суициду и другие противоправные действия, направленные на деструктивное воздействие на участников ВСС. В связи с этим перед органами правопорядка встала задача выявления и пресечения противоправного поведения и деструктивной деятельно-

сти в ВСС, эффективно решить которую возможно только посредством использования средств современных информационных технологий по соответствующим методикам.

Для решения данной задачи нами разработана автоматизированная система мониторинга и анализа сообщений участников ВСС, структура которой приведена на рис. 1. Методика выявления противоправных действий участников ВСС средствами информационных технологий основывается на лингвистическом анализе текстов сообщений, как размещаемых ими на «стенах», так и тех сообщений, которыми они обмениваются между собой в личной переписке.

При сканировании ВСС с использованием специально разработанной программы «Краулер» модель ВСС представляется в виде графа $G = (V, E)$, где V – это множество узлов, представляющих участников ВСС, а E – множество дуг, обозначающих отношения между этими участниками.

Сканирование графа ВСС начинается с одного или нескольких узлов (система позволяет вести сканирование параллельно как в одной ВСС, так и в нескольких сетях одновременно). При посещении одного узла осуществляется сбор отправленных с него текстовых сообщений на «стену». Эти сообщения собираются в пакеты, которые подвергаются компьютерному лингвистическому анализу. При этом формируется список соседей этого узла с целью выявления его контактов, что позволяет получать тексты сообщений между участниками ВСС при их прямом общении. Эти сообщения также собираются в пакеты для последующего компьютерного лингвистического анализа.

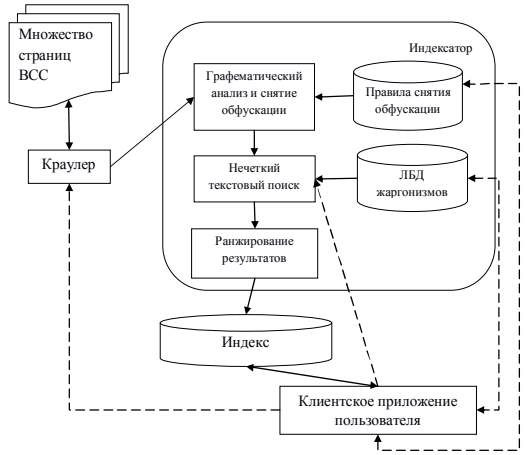

Рис. 1. Структура автоматизированной системы мониторинга и анализа сообщений участников виртуальных социальных сетей

Для сокрытия своих истинных намерений участники ВСС, ведущие противоправную деятельность в сетях, используют как специфическую терминологию – жаргонизмы, так и обфускацию текстов (рис. 2) – намеренное искажение написания слов с целью затруднения получения информации третьими лицами при проведении компьютерного лингвистического анализа. Поскольку обфусцированные тексты сообщений не поддаются простому лингвистическому анализу с помощью поиска ключевых слов, в рассматриваемой автоматизированной системе используются специально разработанные базы данных жаргонизмов и лингвистический процессор.

```
====================== RESTART: C:/Python34/deobf.py ======================
>>> D=Deobf(connection)
>>> D.deobfuscate(tree,"""schanc
так кт о ж мы, на конец? уа - chасть той силы, чтоо вehно hочет зла и вечно сов
ершает бллаг^о
Товарищ, друг, не скупись, купи немножко конопли
Ой m@ma mь|ла rra3y лала voda водафон
я-пришёл-к-тебе-с-приветом
это мыло давно и неправда н е п р а в д а
ч
у
ш
ь
весь коотрый соабка рпишёл дмой анольд коова кроова
жи3нь - б0/\ь и прочие радости страдание исчо""")
шанс так что мы наконец я часть той силы что вечно хочется и вечно совершает бл
аго товарищ друг не скупись купе немножко коноплиой м мыла разу вода вода он я
пришел тебе с приветом это мыло давно и неправда не правда чушь весь который со
бака решил домой анольдкоова крова жизнь больше и прочие радости страдание исче
>>>
```

Рис. 2. Пример вскрытого обфусцированного текста сообщения участника ВСС «ВКонтакте»

Базы данных жаргонизмов аккумулируют в себе соответствующую лексику, предоставляют возможность пополнения словарей жаргонизмами сфер незаконного оборота наркотических средств и психотропных веществ, пропаганды терроризма и экстремизма, вовлечения в секты, понуждения к суициду.

Лингвистический процессор производит:

графематический анализ текстов сообщений и снятие с них обфускации в соответствии с правилами, основанными на использовании скрытой марковской модели и методе N-грамм;

нечеткий текстовый поиск жаргонизмов в текстах сообщений и интерпретацию лингвистического анализа этих сообщений;

ранжирование результатов – распределение текстов сообщений и их авторов по тематике противоправных действий.

Также извлекаются профили авторов сообщений, отнесенных к категории противоправных действий, собирается информация об их активности: время нахождения в сети и совершаемые ими контакты вне зависимости от того, с какого устройства (персональный компьютер, планшет, мобильный телефон) они заходили в сеть (рис. 3).

Выявление устойчивых групп участников ВСС производится на основе построения графа их контактов и формировании истории активности выбранных членов этих групп: дата и время активности, статус и устройство (в том числе его тип), с которого было зафиксировано посещение персональной страницы.

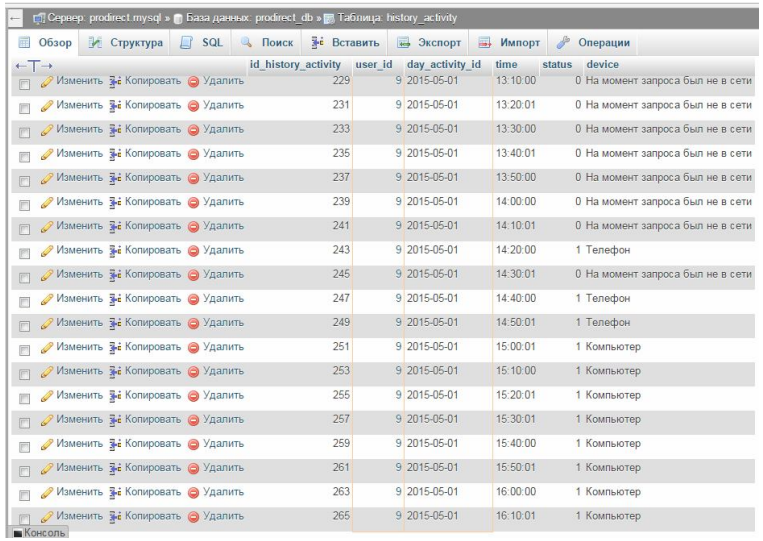

Рис. 3. Скриншот выборки из базы данных активности одного из участников ВСС

Разработанная автоматизированная система мониторинга и анализа сообщений участников ВСС позволяет решать проблему контроля за противоправной деятельностью лиц в этих сетях. Опытная эксплуатация данной системы в ряде уполномоченных органов показала ее эффективность. В настоящее время ведутся работы по следующим направлениям:

идентификация участников сетей, использующих браузер Tor, а также пиринговые сети;

чтение и определение содержания текстов, размещенных участниками сети на фотографиях (в том числе пропаганда ИГИЛ и т. п.).

УДК 004.891, 004.942

В.М. Шишкин

МОДЕЛИ КОМПЛЕКСНОЙ ОЦЕНКИ ФАКТОРОВ РИСКА И ДИНАМИКИ УГРОЗ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ

Технологии ведения террористической деятельности имеют комплексный характер и, следовательно, противодействие угрозам соответствующей направленности нельзя рассматривать исключительно как выявление и предотвращение инцидентов, т. е. в контексте оперативной работы, – результативность такого подхода будет заведомо ограниченной.

Отдельно следует остановиться на информационно-психологических воздействиях. Террористические цели предполагают то или иное влияние на психику, моральное состояние как масс, так и лица, принимающего решения, чтобы были получены материальные или политические результаты.

Понятно, что используются не только узкоспециальные методы и средства, но и широкий спектр разнообразных воздействий на психологическое состояние как на индивидуальном, так и групповом уровне. Наряду с собственно психологическими методами и средствами применяются трудно определяемые и неизмеряемые, но объективно существующие и крайне важные для безопасности, выражаемые на ментальном, интеллектуальном, культурном, аксиологическом, духовном уровнях. Нельзя в этот ряд не включить и так называемый человеческий фактор – комплекс угроз безопасности в человеко-машинных, социотехнических системах, которые связаны с разнообразными проявлениями поведенческих особенностей людей во взаимодействии с технологической средой. Если абстрагироваться от деталей, то все риски нарушения безопасности имеют системный техно-гуманитарный характер.

Таким образом, в первую очередь при рассмотрении процессов противодействия террористическим угрозам следует обратить внимание на сложность и неопределенность системы взаимодействий разнородных факторов с многочисленными обратными связями, что в результате может дать неожиданные эффекты в любой сфере, материальной и нематериальной, независимо от собственно террористических целей. Поэтому для исследования данной проблематики необходим адекватный ее сложности методический аппарат и инструментарий, способный учесть неопределенность и разнородность исходной информации при определении обоснованных метрически сравнимых оценок всему спек-

тру угроз. Только тогда, имея оценку значимости угроз, можно будет целенаправленно и эффективно противодействовать им, причем не исключено, что решение проблем противодействия террору придется искать в далеких от него сферах.

При этом следует также учитывать двойственный характер любых мер противодействия угрозам: их применение способно одновременно с желаемым результатом по отношению к одним факторам вызвать негативные последствия относительно других. Примером необходимости учета данного обстоятельства в антитеррористических мероприятиях может служить катастрофа самолета German wings в начале 2015 г., когда именно антитеррористическая защита создала условия для действий пилота, по сути, террористических. Другим примером, весьма актуальным сегодня, является широкое информирование о совершенных терактах, проведении публичных антитеррористических мероприятий. С одной стороны, оно мобилизует общество и создает некоторые препятствия повторению терактов, но с другой, опять-таки учитывая психологические особенности разных людей и групповое поведение, особенно в мегаполисах, во-первых, создает атмосферу страха, тревоги, что и является одной из целей теракта, а во-вторых, стимулирует людей с неустойчивой психикой на совершение аналогичных действий.

В общем случае включение новых элементов в защищаемый объект всегда приводит к его усложнению, создавая новые структуры факторов, внося дополнительную неопределенность, формируя новые уязвимости и риски, а средства защиты способны не только противодействовать одним угрозам, но и усиливать другие или даже создавать новые.

Еще одно направление, которому не уделяется пока достаточного внимания в теоретическом осмыслении и на практике, связано с преобладанием защитного подхода к обеспечению безопасности. Проблемы в сфере информационной безопасности, например, по-прежнему рассматриваются преимущественно с позиций безопасности информации, которая часто сводится к еще более узкой проблематике – практическим вопросам защиты информации. Ситуация меняется, но в целом подходы к обеспечению безопасности остаются пока преимущественно оборонительными.

Однако за последние годы складывается следующая тенденция: обеспечение безопасности на различных ее уровнях и в разных аспектах приобретает черты противоборства и становится непрерывным процессом. Ориентация лишь на защиту становится недостаточной для поддержания безопасности, технология ее обеспечения требует уже тех или иных атакующих или упреждающих воздействий на потенциального противника. Это обусловлено тотальной информатизацией социо-

и техносферы, всех систем обеспечения жизнедеятельности и управления, самого образа жизни подавляющей части населения, перевод конфликтов в информационное пространство. Даже ставший тривиальным сетевой криминал можно интерпретировать как социотехническое противоборство, а так называемые информационные войны глобального уровня вполне могут быть масштабированы до межкорпоративных конфликтов. Что касается борьбы с террором, то иначе как наступательной она быть не может. При этом информационная и материальная, гуманитарная и технологическая составляющие конфликтов стали неразрывно связанными. Такого рода процессы могут быть описаны и исследованы в терминах динамических моделей.

Первое из обозначенных направлений связано с выявлением профиля риска, т. е. с определением и оценкой значимости некоторого спектра разнородных угроз, не обязательно лежащих в сфере антитеррористической деятельности, с целью выработки наиболее эффективных мер противодействия. И соответствующие данной предметности модели будут сводиться к дискретному оцениванию.

Второе направление предполагает моделирование непрерывных процессов во времени с целью выявления некоторых качественных тенденций или закономерностей, проверку сценариев при вариации начальных условий, коэффициентов, пространства фазовых переменных, представляющих разнородные факторы.

Оба эти направления, внешне разные (в одном случае – оценка состояния, в другом – наблюдение процесса), объединяет то, что объектом исследования являются слабо структурированные, трудно формализуемые системы, с разнородными элементами и плохо измеряемыми показателями. Объединительным для указанных подходов может являться используемое в англоязычной литературе понятие Holistic security.

Разумеется, обозначенные вопросы активно изучаются, обсуждаются, но чаще их анализ сводится к вербальным рассуждениям, не допускающим объективной оценки, когда на всякое обоснованное мнение найдется другое, не худшее и не менее обоснованное. Таким образом, есть потребность в применении формального аппарата, позволяющего пусть не доказать то или иное утверждение или строго обосновать рекомендацию, но, по крайней мере, согласовав базовые положения модели, объективно проверить результаты экспериментов на ней для различных сценариев и начальных условий. Предлагаемые модели в какой-то мере удовлетворяют этим требованиям, показав в эксперименте правдоподобные результаты и потенциальную применимость в исследовании проблем безопасности в различных предметных областях.

В докладе будет представлены основные элементы методики и реализации автоматизированной системы стохастического риск-анализа и

динамической модели противоборства. Полученные на ней некоторые предварительные качественные результаты показали, в частности, что целью противоборства с террористическими организациями, в отличие от отношений с менее агрессивными противниками, может быть только подавление.

Для эффективного противодействия террористическим угрозам необходимо выявление наиболее значимых и актуальных из них, а также их источников, которые могут обнаруживаться далеко от конкретных и конечных проявлений террористической активности или ее организаторов. Видимое решение проблем борьбы с террором может оказать негативное влияние в других сферах жизнедеятельности мегаполисов.

Успешное противодействие угрозам должно непременно включать активную составляющую: защитные мероприятия невозможны без активного противодействия – оборонительная позиция ведут к поражению. При этом активное противодействие не всегда предполагает силовую составляющую, оно может включать организационные меры, экономические, юридические, педагогические и другие вполне мирные средства.

Предложенные формальные методы аналитики в исследовании проблем, порождаемых террористической деятельностью, являются лишь инструментом и не могут заменить традиционные для данной предметной области подходы и методы. Понятно, что модели, построенные для решения конкретных задач, отразят текущий уровень знания (незнания) экспертов, но оценки, получаемые на их основе, по этой же причине будут, по крайней мере, не хуже результатов многовариантного вербального обсуждения, имея при этом преимущество – отсутствие ангажированности и возможность согласования.

УДК 343

А.В. Штрапов

НЕКОТОРЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Начало XXI в. характеризуется отчетливо выраженными явлениями глобализации и перехода от индустриального общества к обществу информационному. В настоящее время идет процесс быстрого развития и внедрения компьютерной техники во все сферы человеческой деятельности. Под воздействием научно-технического прогресса повсеместно внедряются новые информационные технологии, которые

предоставляют уникальные возможности для быстрого и эффективного развития как государства в целом, так и отдельно взятого человека.

Повышение эффективности работы правоохранительных органов по раскрытию преступлений в настоящее время невозможно без интеграции в служебную деятельность новых информационных технологий, в первую очередь связанных с персональными компьютерами. Они обладают рядом несомненных преимуществ: относительно низкая стоимость и высокая степень надежности, компактность и малое потребление энергии, что позволяет внедрять их буквально на каждое рабочее место как автономно, так и с включением в локальные информационные сети или в качестве терминалов больших и средних ЭВМ.

Информация является результатом отражения и обработки в человеческом сознании многообразия окружающего мира. Информация, которая позволяет ее существующему (потенциальному) владельцу получать какой-либо выигрыш (моральный, материальный, политический и т. п.), приобретает некоторую цену.

С другой стороны, информация является основой для процессов управления, несанкционированное вмешательство в которые может привести к катастрофическим последствиям в объекте управления – в производстве, в транспорте, в военном деле, в деятельности органов внутренних дел.

Объем информации, окружающей нас, постоянно возрастает. Естественно, что в этих условиях невозможно обойтись без компьютера и программного обеспечения, предназначенного для операций обработки, создания, копирования, поиска и других действий с информацией.

Внедрение новых информационных технологий в большинство сфер современного общества оказывает влияние и на правоохранительные органы. Совершенствуется система управления и информационного обеспечения, возникают новые методы сбора и анализа информации, меняются облик и возможности специальных технических средств и т. п. Более того, информатизация органов внутренних дел связана не только с переводом системы криминалистической информации на электронные носители, но и с широким применением территориально распределенных баз данных для борьбы с преступностью.

Сбор, упорядочение, хранение, обработку и выдачу пользователям информационных ресурсов осуществляют автоматизированные информационные системы (АИС). Под информационным обеспечением АИС понимается система реализованных решений по объемам, размещению и формам организации информации, циркулирующей в АИС при ее функционировании. Специфическими формами организации информации в АИС является база данных (БД) – поименованная, целостная, единая система данных, организованная по определенным правилам, которые предусматривают общие принципы описания, хранения и обработки данных.

В соответствии со ст. 15, 17 Закона Республики Беларусь «Об оперативно-розыскной деятельности» органы, осуществляющие оперативно-розыскную деятельность, могут создавать и (или) использовать базы данных (учеты), информационные системы, а также заводить дела оперативного учета.

Дела оперативного учета заводятся при наличии оснований, предусмотренных ст. 16 закона, в целях систематизации, проверки и оценки сведений, полученных органом, осуществляющим оперативно-розыскную деятельность, при выполнении задач оперативно-розыскной деятельности, а также для принятия на их основе соответствующего решения должностным лицом органа, осуществляющего оперативно-розыскную деятельность.

Дела оперативного учета прекращаются в случае выполнения задач оперативно-розыскной деятельности или установления обстоятельств, свидетельствующих об объективной невозможности выполнения этих задач. Если по делу оперативного учета, которое прекращено, получены новые сведения, требующие проверки путем проведения оперативно-розыскных мероприятий, заводится новое дело оперативного учета.

Виды дел оперативного учета и порядок их ведения определяются нормативными правовыми актами органов, осуществляющих оперативно-розыскную деятельность. Факт заведения дела оперативного учета не является основанием для ограничения прав, свобод и законных интересов граждан, прав и законных интересов организаций.

Следует отметить, что в настоящее время в органах внутренних дел особое внимание уделяется интенсификации разработки и внедрения в практическую деятельность автоматизированных информационных систем, а также отдельных подсистем и задач управленческого, оперативно-розыскного и профилактического назначения. Большинство внедренных автоматизированных систем эксплуатируется на технической базе информационно-аналитических центров, обслуживающих аппараты и службы органов внутренних дел.

При использовании данной технологии обмена информацией обеспечивается комплексная компьютеризация служебной деятельности и информационной работы при выработке управленческих решений, раскрытии преступлений, расстановке сил и средств, обработке статистических данных, планировании и контроле.

В Информационном центре МВД Республики Беларусь сотрудникам внутренних дел доступны ряд автоматизированных информационных систем: Единый государственный банк данных о правонарушениях, АС «Похищенный автомототранспорт», АИС «Плательщики сбора», Реестр

Национальной системы подтверждения соответствия, АИПС «Оружие» Главного информационно-аналитического центра МВД России, банк данных криминальной информации (оперативно-розыскные и профилактические учеты), АС «Паспорт», АИС «ГАИ-Центр» и ряд других.

Скорость получения сведений во многом зависит от эффективного использования существующих АИС в сфере деятельности правоохранительных органов. Однако в настоящее время идет процесс переориентации на более совершенные программные продукты, способные поддерживать работоспособность огромных массивов данных, обеспечивать необходимые параметры времени и прав доступа к информации на различных уровнях.

Сегодня, как никогда, остро стоит вопрос разработки единого программного обеспечения, реализующего широкий спектр возможностей автоматизированных без данных, сопряжение имеющихся данных по различным направлениям работы для получения оперативными работниками интересующей их информации без многочисленного обращения к различным автономным базам и банкам данных. При этом требуется высокая степень адаптируемости системы к изменению нормативной и законодательной базы без вмешательства разработчика, простота и надежность в эксплуатации.

Таким образом, основным направлением использования вычислительной техники с целью решения задач ОРД является сбор, обработка, надежное хранение и оперативный доступ сотрудников служб и подразделений органов внутренних дел к этой информации. В настоящее время осуществление информационного процесса ведется с использованием вычислительной техники и программных средств – автоматизированных информационно-поисковых систем или автоматизированных банков данных.

РАЗДЕЛ 4

ИННОВАЦИОННЫЕ ПОДХОДЫ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

УДК 378:004.9

П.Л. Боровик, Е.В.Чистая

ИЗ ОПЫТА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ УЧЕБНЫХ ИЗДАНИЙ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ КАФЕДРЫ ПРАВОВОЙ ИНФОРМАТИКИ АКАДЕМИИ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

Анализ педагогической литературы, посвященной информатизации образования, показывает, что использование электронных учебных изданий (ЭУИ) в учебном процессе учреждения высшего образования (УВО) является одним из перспективных направлений. Реализация специфических возможностей ЭУИ, таких как компьютерная визуализация учебной информации, незамедлительная обратная связь между пользователем и компьютером, автоматизация процессов информационно-методического обеспечения и контроля за результатами усвоения учебного материала обучающимися, создает предпосылки для совершенствования и активизации образовательного процесса.

Признавая многообразие научных изысканий, касающихся обозначенной тематики, следует отметить, что проблемы создания и использования ЭУИ в ходе профессиональной подготовки специалистов для ОВД не перестают быть актуальными. С одной стороны, имеющиеся результаты исследований в целом позволяют разрабатывать содержание подготовки будущих сотрудников ОВД в образовательном процессе УВО на базе широкого использования ЭУИ, а с другой – качественное решение этой задачи может быть обеспечено на основе результатов комплексного сравнительного анализа уровня усвоения знаний при

использовании традиционных форм обучения и ЭУИ, удовлетворяющих общим дидактическим принципам и научно-обоснованным организационно-педагогическим требованиям.

Отмеченные обстоятельства предопределили необходимость проведения в 2016/17 учебном году на кафедре правовой информатики Академии Министерства внутренних дел Республики Беларусь педагогического эксперимента на тему «Сравнительный анализ уровня усвоения знаний при использовании традиционных форм обучения, компьютерных программных средств и мультимедийных обучающих комплексов» (для курсантов первого курса факультета милиции, следственно-экспертного и уголовно-исполнительного факультетов Академии МВД). Опытно-экспериментальное исследование проводилось в три основных этапа.

На первом (диагностико-прогностическом и организационно-подготовительном) этапе (январь – сентябрь 2016 г.) были определены исходные положения исследования: определена проблема, проведено изучение и анализ теоретических основ использования ЭУИ в процессе обучения, обобщен опыт других исследований по изучаемой тематике; сформулированы цель, задачи и гипотеза исследования; определен понятийный аппарат и разработан исследовательский инструментарий (методические рекомендации, анкеты и тестовые задания для входного и выходного контроля знаний курсантов и др.).

Для проведения исследования и обеспечения педагогического эксперимента коллективом кафедры правовой информатики Академии МВД разработано ЭУИ по учебной дисциплине «Практикум по информационным технологиям» (далее – ЭУИ), предназначенное для курсантов первого курса, обучающихся по специальности 1-24 01 02 «Правоведение». Данное программное обеспечение представляет собой обучающее средство, методическое назначение которого заключается в передаче обучающимся необходимых знаний и в формировании навыков учебно-практической деятельности, а также в обеспечении необходимого уровня усвоения знаний, устанавливаемого системой обратной связи и реализуемого средствами программы (структура разработанного на кафедре ЭУИ представлена на рис. 1).

При создании ЭУИ учитывались как общие дидактические принципы (научность, системность, последовательность, наглядность, доступность, активность, сознательность, прочность знаний, связь теории с практикой и др.), так и организационно-педагогические требования, основанные на психофизиологических особенностях восприятия, переработки и хранения информации.

Рис. 1. Структура электронного учебного издания по учебной дисциплине «Практикум по информационным технологиям»

На втором (практическом) этапе (сентябрь – декабрь 2016 г.) исследования осуществлялась опытно-экспериментальная работа, суть которой заключалась в проверке эффективности разработанного ЭУИ, в проведении сравнительного анализа уровня усвоения знаний при использовании традиционных форм обучения и ЭУИ в ходе проведения занятий по учебной дисциплине «Практикум по информационным технологиям».

На третьем (обобщающем) этапе (январь – февраль 2017 г.) была проведена систематизация и предварительное обобщение результатов исследования, осуществлена оценка всех статистических данных, полученных в ходе экспериментальной работы, выполнена их итоговая математическая обработка; проведен сравнительный анализ полученных данных, который позволил сформулировать выводы и рекомендации, направленные на дальнейшее совершенствование процесса использования ЭУИ в образовательном процессе УВО; подтверждена выдвинутая гипотеза исследования.

Практический этап исследования состоял в проведении трех видов педагогического эксперимента: констатирующего, формирующего и контролирующего.

Основной целью констатирующего эксперимента являлось определение первоначального уровня знаний, умений и навыков использования курсантами первого курса Академии МВД современных информационных технологий. В начале первого семестра обучения было проведено входное тестирование, результаты которого позволили сформировать выборочную совокупность исследования из числа учебных групп обучающихся, которые имеют схожий уровень знаний (общее количество респондентов составило 325 человек, из них: курсанты факультета милиции – 118 человек, следственно-экспертного факультета – 119, уголовно-исполнительного факультета – 88). На основании результатов входного тестирования было отобрано по одной учебной группе каждого факультета с примерно одинаковым средним баллом.

С учетом того, что при проведении практических и лабораторных занятий в компьютерных классах учебные группы обычно разделяются на две подгруппы, каждая из вышеуказанных групп была также разделена на две части, составившие, таким образом, контрольную и экспериментальную подгруппы по 15 человек. В итоге общее количество обучающихся, задействованных в педагогическом эксперименте в составе контрольной статистической выборки с учетом числа факультетов составило 45 человек, столько же в составе экспериментальной.

Формирующий эксперимент проводился в течение первого семестра 2016/17 учебного года и состоял в выполнении курсантами практических и лабораторных заданий при изучении учебной дисциплины. Учебные занятия в контрольных подгруппах проводились по традиционной методике, а в экспериментальных – с использованием ЭУИ (в соответствии с разработанными методическими рекомендациями по использованию ЭУИ в образовательном процессе).

Всего в ходе проведения формирующего эксперимента курсантами выполнено 10 практических и 5 лабораторных заданий (в соответствии с учебной программой). Результаты работы каждого курсанта оценивались в журналах текущей успеваемости.

В целях обеспечения надежности и достоверности полученных результатов, а также их теоретической обоснованности математические расчеты проводились по *t*-критерию Стьюдента, используемого для определения статистической значимости различий средних арифметических величин.

Так, статистика критерия для случая несвязанных, независимых выборок равна: $t_{эмп} = \dfrac{\bar{x} - \bar{y}}{\sigma_{x-y}}$,

где x, y – средние арифметические выставленных оценок в экспериментальной и контрольной группах, σ_{x-y} – стандартная ошибка разности средних арифметических, рассчитываемая по формуле:

$$\sigma_{x-y} = \sqrt{\frac{\sum (x_1 - x)^2 + \sum (y_1 - y)^2}{n_1 + n_2 - 2}\left(\frac{1}{n_1} + \frac{1}{n_2}\right)},$$

где n_1 и n_2 соответственно величины первой и второй выборки.

Если $n_1 = n_2$, то стандартная ошибка разности средних арифметических будет высчитываться по формуле:

$$\sigma_{x-y} = \sqrt{\frac{\sum (x_i - \bar{x})^2 + \sum (y_i - \bar{y})^2}{(n-1) \cdot n}},$$

где n – величина выборки.

Подсчет числа степеней свободы осуществляется по формуле $k = n_1 + n_2 - 2$. При численном равенстве выборок $k = 2n - 2$.

Следует отметить, что статистический подход справедлив и при относительно малом количестве измерений. Распределение Стьюдента при числе измерений $n \to \infty$ (число измерений стремится к бесконечности) переходит в распределение Гаусса, а при малом числе отличается от него.

Для расчета абсолютной ошибки при малом количестве измерений (в нашем случае число измерений равно количеству курсантов в подгруппе – 15 человек) используется специальный коэффициент Стьюдента t, зависящий от надежности вероятности P и числа измерений n.

Опуская теоретические обоснования его введения, заметим, что

$$\Delta x = S_x \times t,$$

где Δx – абсолютная ошибка для данной доверительной вероятности; S_x – среднеквадратичная ошибка среднего арифметического.

Приведенный анализ дает возможность утверждать, что величина среднеквадратичной ошибки позволяет вычислить вероятность попадания истинного значения измеряемой величины в любой интервал вблизи среднего арифметического.

При $n \to \infty$ $S_x \to 0$, т. е. интервал, в котором с заданной вероятностью находится истинное значение μ, стремится к нулю с увеличением числа измерений.

Однако точность расчетов существенно увеличивается лишь до тех пор, пока случайная ошибка не станет сравнимой с систематической. Дальнейшее увеличение числа измерений нецелесообразно, поскольку конечная точность результата будет зависеть только от систематической ошибки. Зная величину систематической ошибки, нетрудно задаться допустимой величиной случайной ошибки, взяв ее, например, равной 5 % от систематической. Задавая для выбранного таким образом

доверительного интервала определенное значение P (например, P = 0,95), нетрудно найти необходимое число измерений, гарантирующее малое влияние случайной ошибки на точность результата. Для этого следует воспользоваться таблицей, в которой интервалы заданы в долях величины σ, являющейся мерой точности данного опыта по отношению к случайным ошибкам.

Таблица

Необходимое число измерений для получения ошибки Δ с надежностью P

Δ = Δx/σ	Значения P					
	0,5	0,7	0,9	0,95	0,99	0,999
1,0	2	3	5	7	11	17
0,5	3	6	13	18	31	50
0,4	4	8	19	27	46	74
0,3	6	13	32	46	78	127
0,2	13	29	70	99	171	277
0,1	47	169	273	387	668	1089

Из приведенной таблицы следует, что выборка из 15 человек и ошибка Δ, равная 0,5, дают достаточно высокую вероятность P, находящуюся между 0,9 и 0,95. Это свидетельствует о том, что количественным результатам успеваемости, вычисленным с использованием среднего арифметического, можно доверять.

Так, результаты сравнительного анализа среднего балла текущей успеваемости курсантов – участников педагогического эксперимента за весь семестр представлены по факультетам на рис. 2.

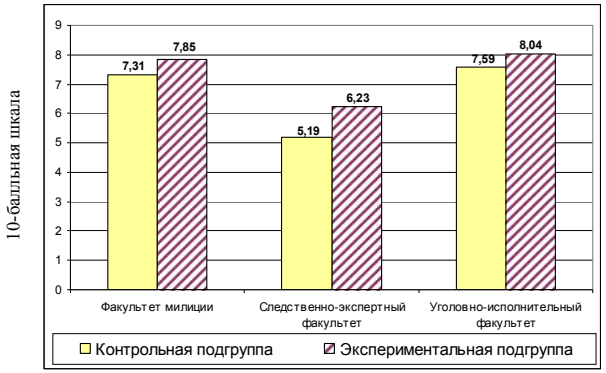

Рис. 2. Сравнительный анализ среднего балла текущей успеваемости курсантов – участников педагогического эксперимента

Как видно из представленных данных, курсанты экспериментальных подгрупп продемонстрировали лучшую (в среднем на 10,02 %) текущую успеваемость по сравнению с обучающимися в составе контрольных подгрупп в течение всего проводимого педагогического эксперимента.

При проведении контролирующего эксперимента (декабрь 2016 г.) осуществлялась фактическая констатация итогового уровня сформированности знаний, умений и навыков использования современных информационных технологий. Указанная работа осуществлялась путем проведением выходного тестирования с помощью единого комплексного теста, состоящего из 50 вопросов, охватывающих содержание учебной дисциплины и оцениваемых в баллах (за правильный вопрос выставлялся 1 балл, за ошибочный – 0 баллов). Максимальное количество баллов, которые мог получить обучающийся по итогам тестирования – 50 баллов. Правильность оценки тестов проверялась независимой комиссией из числа преподавателей кафедры, не участвующих в настоящем исследовании.

Согласно итоговым данным статистических расчетов лучшие результаты (в среднем на 18,44 %) закономерно показали курсанты экспериментальных подгрупп, обучение в которых проводились с использованием ЭУИ (рис. 3).

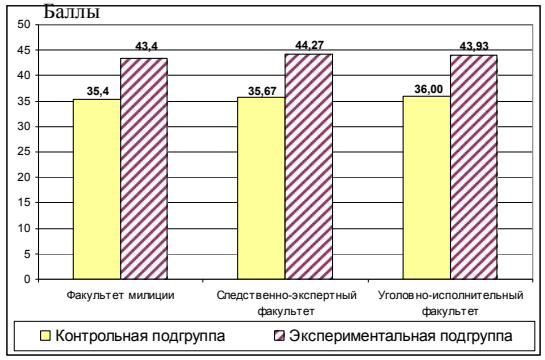

Рис. 3. Сравнительный анализ среднего балла итогового тестирования курсантов – участников педагогического эксперимента

В ходе наблюдения за процессом обучения в экспериментальных группах установлено, что использование ЭУИ при проведении учебных занятий, а также во время управляемой самостоятельной подготовки существенно повышает интерес курсантов к изучаемой учебной дисциплине за счет использования различных типов мышления и видов

познавательной деятельности, обеспечивает наглядность учебного материала и позволяет достичь большей глубины его понимания и усвоения.

Таким образом, результаты проведенного педагогического эксперимента позволили не только сделать вывод о явном преимуществе использования ЭУИ в образовательном процессе УВО, но и обосновать дидактические принципы и педагогические условия, при которых возможности электронных обучающих средств оказывают наиболее результативное влияние на формирование знаний, умений и навыков. Используя разработанное ЭУИ, большинство курсантов экспериментальных подгрупп в течение всего исследования демонстрировали более высокий уровень знаний, умений и навыков использования современных информационных технологий по сравнению с обучающимися в контрольных подгруппах, в которых обучение проводились по традиционной методике.

УДК 004

М.В. Левданский

НОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ КОМПАНИИ D-LINK ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО СЕТЕВЫМ ТЕХНОЛОГИЯМ

Начиная с мая 2017 г. мир потрясает очередная эпидемия компьютерного вируса WannaCry и связанных с ним последствий. В настоящее время по оценкам экспертов около 100–120 тыс. компьютеров поражены вирусом по всему миру. Заражению подверглись различные категории пользователей: и силовые структуры, и медицинские учреждения, и обычные пользователи. При этом вирус использовал малораспространенный вектор атаки на редко используемый устаревший протокол – уязвимость, закрытую компанией-разработчиком еще в марте 2017 г. (подробнее можно прочитать в статье «Пора плакать: как хакеры пустили в ход кибероружие АНБ и ЦРУ» на информационном ресурсе «РБК»). Масштаб эпидемии и ущерб еще только предстоит оценить. Однако уже сейчас можно заметить, что тех пользователей, которые грамотно подошли к вопросам сетевой безопасности, данный инцидент обошел стороной.

Таким образом, вопросы сетевой безопасности, сетевой грамотности пользователей, системных администраторов, профильных специалистов сегодня актуальны как никогда.

Компания D-Link позиционирует себя на рынке как поставщик решений для SOHO-сегмента, оборудования для доступа, агрегации и

младшего уровня ядра сетей передачи данных. Собственно, если рассмотреть типовую структуру сети, то ее решения находятся на первой линии взаимодействия с пользователем. Поэтому мы, представители компании, прекрасно понимаем и владеем информацией о том, что происходит в этой зоне, как нужно правильно строить свои решения, что нужно использовать (какие методы и функциональности устройств), чтобы максимально исключить возможности для сетевых атак.

При этом мы четко осознаем необходимость обладания как обычными пользователями, так и профильными специалистами соответствующей квалификацией для защиты себя и своих объектов от вирусов, хакерских атак и т. д. Поэтому наша компания совместно с ведущими вузами разрабатывает учебные программы, методические пособия, лабораторные курсы, которые можно использовать для проведения обучения на любом уровне.

В настоящее время мы уже выпустили следующие учебные пособия.

Лапонина О.Р. Основы сетевой безопасности. Часть 1: Межсетевые экраны. 2014. Целью учебного пособия является изучение принципов и получение практических навыков создания безопасной сетевой инфраструктуры с использованием межсетевых экранов D-Link (имеют сертификат Федеральной службы по техническому и экспертному контролю). По окончании курса слушатели будут знать принципы создания надежной и безопасной ИТ-инфраструктуры, классификацию межсетевых экранов, классификацию систем обнаружения и предотвращения проникновений; иметь практические навыки основ администрирования и создания политик межсетевого экрана, использования различных способов приоритизации трафика и создания альтернативных маршрутов, совместного использования межсетевых экранов и систем обнаружения и предотвращения проникновений.

Лапонина О.Р. Основы сетевой безопасности. Часть 2: Технологии туннелирования. 2014. Целью учебного пособия является изучение принципов и получение практических навыков создания безопасной сетевой инфраструктуры с использованием межсетевых экранов D-Link. По окончании курса слушатели должны знать основы криптографических механизмов безопасности, технологии туннелирования, способы хранения учетных записей, иметь практические навыки использования различных протоколов туннелирования.

Смирнова Е.В. и др. Построение коммутируемых компьютерных сетей. 2012. Целью учебного пособия является приобретение знаний об основах построения и поддержки компьютерных сетей, сетевых технологиях, телекоммуникационном оборудовании, а также навыков, которые можно применить в начале работы в качестве специалиста по сетям.

Смирнова Е.В. и др. Технологии коммутации и маршрутизации в локальных компьютерных сетях. 2013. Целью учебного пособия является описание базовых протоколов коммутации 2-го и 3-го уровня, а также принципов статической и динамической IPv4/IPv6-маршрутизации, технологий обеспечения качества обслуживания, функций управления многоадресной рассылкой и доступом к сети, мониторинга, которые требуются для функционирования современной сети масштаба среднего предприятия, равно и на уровне доступа сетей провайдеров услуг.

Данные учебные методические пособия разрабатываются сотрудниками D-Link совместно с преподавателями МГТУ им. Н.Э. Баумана, факультета вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, Рязанского государственного радиотехнического университета и других высших учебных заведений. Благодаря этому мы можем сказать, что они изначально адаптированы для широкой аудитории: как для тех, кто желает получить начальные знания, так и для более углубленного изучения конкретной задачи.

По итогам 2016 г. компания D-Link открыла для широкого доступа в Республике Беларусь сайт дистанционного обучения (https://learn.dlink.ru). Данный сайт представляет возможность прохождения обучения по всем нашим курсам и методическим пособиям из любой точки мира, где есть сеть Интернет. Обучение бесплатно и доступно всем желающим после обязательной регистрации. В рамках программы обучения любой желающий сможет пройти теоретический курс обучения, сдать промежуточный и общий экзамены, при желании возможно прохождение сертификационного испытания, включающее в себя и практическую часть.

В то же время данный сайт представляет возможность для образовательных заведений Республики Беларусь организовывать собственные учебные курсы для своих обучающихся. В рамках сотрудничества с вузами мы предлагаем возможность проведения обучения по смешанным учебным курсам, которые содержат не только наши материалы, но и авторские материалы преподавателей вуза и предусматривают развернутый контроль за успеваемостью, организацию вебинаров и др.

В настоящее время представительство D-Link International в Республике Беларусь уже осуществляет взаимодействие с ведущими техническими учреждениями образования Республики Беларусь:

Гомельским государственным университетом им. Ф. Скорины (кафедра общей физики физического факультета). В 2017 г. университет получил статус авторизованного учебного центра D-Link. Наличие учебной лаборатории и сертифицированных преподавателей позволяет проводить практические работы с использованием последних учебных материалов и на основе консультаций компании D-Link. Также все

студенты, прошедшие обучение по методикам ГГУ, могут сдавать квалификационный экзамен на промышленный сертификат D-Link;

Белорусским государственным университетом информатики и радиоэлектроники (кафедра сетей и устройств телекоммуникаций). Уже почти 5 лет университет использует наши материалы для чтения курсов лекций по направлению «Технологии коммутации и маршрутизации современных сетей Ethernet» – системы коммутации, системы коммутации каналов и пакетов, системы подвижной связи. В настоящее время преподаватели и аспиранты данной кафедры проходят квалификационные экзамены на получение статуса сертифицированных преподавателей;

Белорусским государственным университетом;

Лидским колледжем Гродненского государственного университета им. Я. Купалы.

Представительство ООО «D-Link International PTE Ltd» в Республике Беларусь открыто для любого сотрудничества с учреждениями высшего образования Республики Беларусь. Мы готовы рассмотреть любые предложения и помочь с внедрением в образовательные процессы современных материалов, с разработкой учебных программ и планов, готовы поделиться нашей компетенций и опытом с любой аудиторией как студентов, так и профессионалов, нуждающихся в повышении квалификации. На базе нашего представительства в Минске мы проводим бесплатные семинары и консультации по всем вопросам и аспектам, касающимся как сетевых технологий, так и технологий защиты информации.

УДК 343

А.Н. Лепёхин, И.В. Горошко

ИСПОЛЬЗОВАНИЕ МАТЕМАТИЧЕСКОГО ИНСТРУМЕНТАРИЯ В АНАЛИТИЧЕСКОЙ РАБОТЕ

Современные тенденции развития, а также объективные предпосылки современного социума детерминируют изменения в преступной среде общества, порождая новые способы и методы совершения криминальных деяний. Более того, информационные процессы, сопровождающие указанные явления, обусловливают фокусирование внимания правоохранительных органов не только на противоправной деятельности и соответствующей реакции государства в рамках действующего законодательства по раскрытию и расследованию преступлений, но и на профилактической, упреждающей деятельности органов правопо-

рядка, направленной на реализацию превентивной функции соответствующих государственных органов. Очевидно, для качественной реализации указанных направлений деятельности правоохранительных органов необходимо соответствующее не только информационное, но и аналитическое обеспечение правоохранительной деятельности.

Указанные обстоятельства свидетельствуют, что в рамках информационно-аналитической работы следует смещать акценты ее осуществления с информационной составляющей (что также является важным) в сторону аналитического обеспечения реализации своих функций правоохранительными органами, поскольку современные реалии таковы, что постоянно и многократно возрастают информационные потоки и объемы информации. К источникам такой информации можно отнести: сведения в различных информационных банках данных органов внутренних дел; сведения, имеющие отношение к решению служебных задач, из автоматизированных банков данных других государственных органов; информация, образующаяся в процессе служебной деятельности органов внутренних дел (рапорта, справки, служебные материалы и др.); информация от других государственных органов, юридических лиц и граждан; сведения из средств массовой информации, в том числе и размещенные в сети Интернет; а также другие источники.

Соответственно, современный этап развития общества характеризуется взрывным характером роста генерируемой информации по различным направлениям, включая оперативно-служебную деятельность. И в настоящее время, по сути, в условиях так называемой информационной избыточности вопрос о получении информации остро не стоит. Да, есть вопросы в части обеспечения свойств информации, необходимой для принятия управленческого решения, – оперативности, достоверности и достаточности, но более остро, как мы полагаем, ставится вопрос о ее своевременной обработке и принятии на ее основе соотвествующих решений.

Таким образом, реализация функций и задач, возложенных на правоохранительные органы и органы внутренних дел, в первую очередь зависит от способности быстро и эффективно обработать, проанализировать большие объемы информации и выдать конечный готовый продукт – оптимальное управленческое решение.

Решение данной задачи, по нашему мнению, невозможно без соответствующего научно-методического обеспечения, инструментария аналитического решения прикладных задач. И в первую очередь необходимо говорить о математических моделях и методах, позволяющих произвести операции отбора, ранжирования и верификации получаемой информации и продукта ее переработки – аналитических документов, и, соответственно, о принятии на их основе решений оперативно-тактического и стратегического характера.

Анализ действующих подходов к проведению информационно-аналитической работы в правоохранительных органах в целом и в органах внутренних дел в частности показывает, что она имеет поверхностный характер и заключается в основном в сравнении определенных показателей оперативно-служебной деятельности с предыдущим периодом, а также в проведении изредка факторного анализа и в разработке регрессионных моделей, используемых в прогнозной деятельности. Нисколько не умаляя такой подход, следует отметить, что такая методика имеет серьезные методологические ограничения как по срокам проведения прогнозной деятельности, так и по качеству ее реализации.

Очевидно, возникает необходимость в использовании иного инструментария в информационно-аналитической деятельности. По нашему мнению, существенную помощь в этом может оказать использование инструментария математической науки, и в первую очередь следует говорить о применении математических методов и моделей в информационно-аналитической работе правоохранительных органов.

Относительно применения математических моделей в информационно-аналитической работе необходимо сразу выделить некоторые методологические ограничения их использования, поскольку популярность данного метода научного познания привела к достаточно активному его внедрению в моделировании различных социально-экономических процессов (в том числе, как полагаем, уместно говорить и об управлении органами внутренних дел). Вместе с тем, считаем, очень важно при разработке математических моделей управления любым социальным процессом или явлением выделить управляющие параметры системы, т. е. те воздействия (изменения), которые оказывают существенное влияние на саму систему. С одной стороны, традиционные модели характеризуются некоторой избыточностью и усложненностью, что привело к тому, что, как полагаем, они перестали выражать истинные причинно-следственные закономерности развития социальных процессов. С другой – такие модели описывают, как правило, трендовые траектории и не учитывают точки бифуркации, не могут предложить достоверное развитие процесса явления даже в среднесрочной перспективе, т. е. имеют достаточно ограниченный горизонт прогнозирования.

Закономерно возникают вопросы о выделении таких управляющих параметров системы, о применении соответствующих математических методов.

Рассматривая второй вопрос, можно отметить, что инструментарий может быть применен различный, но важно учитывать, с одной стороны, ограниченный характер методов для различных прикладных задач, с другой – важно не перейти порог избыточности, чтобы не получилась модель ради модели, без ее аналитического компонента.

Как один из вариантов решения вопроса аналитического обеспечения правоохранительной деятельности является использование положений теории графов. И, соответственно, инструментом для проведения анализа информации является разработка в общем виде графовой модели $G = (V, E)$, определения вершин графа $(V1, V2, ..., Vn)$ – управляющих параметров, «параметров порядка», и его дуг $(E1, E2, ... Em)$ для ориентированных графов в части формирования весовых коэффициентов воздействия на управляющие параметры.

Представленный подход является одним из возможных вариантов решения вопроса совершенствования информационно-аналитической деятельности правоохранительных органов в целом и органов внутренних дел в частности. Соответственно, использование математических методов и моделей в этой деятельности, и в первую очередь при анализе информации, позволит существенно повысить достоверность аналитической и прогнозной деятельности в правоохранительной сфере.

УДК 378:147

А.В. Луговая, А.В. Душкин, С.С. Кочедыков

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ В ВОРОНЕЖСКОМ ИНСТИТУТЕ ФСИН РОССИИ

Важным этапом совершенствования профессиональной подготовки сотрудников уголовно-исполнительной системы (УИС) является непрерывное повышение образовательного уровня в условиях возрастающей роли информационно-телекоммуникационных технологий (ИТТ).

Внедрение современных ИТТ в деятельность УИС предполагает реализацию комплекса мероприятий, направленных на совершенствование инфраструктуры информационно-телекомуникационных систем (ИТКС), повышение функционирования и развития ведомственной системы передачи и обработки данных, эксплуатируемых автоматизированных информационных систем специального назначения (АИС СН), а также систем информационной безопасности (ИБ) и защиты информации (ЗИ).

С целью успешной реализации указанных направлений необходимо проведение комплекса организационно-правовых, организационно-технических, технологических и кадровых мероприятий, направленных на обеспечение ИБ и ЗИ эксплуатируемых и вновь создаваемых ИТКС и объектов УИС.

В настоящее время в УИС существует потребность в высококвалифицированных кадрах, обладающих специальными компетенциями в области ИБ и технической ЗИ при организации деятельности подразделений ФСИН России. Сотрудники УИС в своей профессиональной деятельности должны:

неукоснительно соблюдать режим секретности;

реализовывать комплекс мер по обеспечению безопасности информации, защиты государственной тайны и персональных данных;

обеспечивать соблюдение специальных требований безопасности информации в сфере защиты государственной и служебной тайны при организации ведомственного документооборота;

обеспечивать защиту персональных данных, обрабатываемых как на бумажных, так и на электронных носителях, в том числе с использованием системы электронного документооборота;

проводить мероприятия по контролю за обеспечением ЗИ, в том числе защиты государственной тайны;

осуществлять информационно-аналитическое обеспечение оперативно-розыскных мероприятий;

применять при выполнении профессиональных задач криминалистическую и специальную технику;

соблюдать и контролировать в профессиональной деятельности требования нормативно-правовых актов при обеспечении режима секретности и защиты государственной тайны с использованием современных технических средств и методов обеспечения ИБ и ЗИ;

применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ информации в ИТКС, а также АИС СН.

Решение обозначенной проблемы влечет за собой необходимость кадрового обеспечения структурных подразделений УИС специалистами инженерно-технического профиля.

Одной из приоритетных задач, обозначенной Программой развития системы ведомственного профессионального образования на период до 2020 года, является оптимизация структуры набора в учебные заведения с учетом кадровых потребностей служб и подразделений УИС.

Воронежский институт ФСИН России является единственной ведомственной образовательной организацией, осуществляющей подго-

товку инженерно-технических кадров для УИС по образовательным программам высшего и дополнительного профессионального образования, а также по программам подготовки научно-педагогических кадров в адъюнктуре.

В целях обеспечения кадрами, обладающими профессиональной компетентностью в области информационной безопасности при организации деятельности подразделений ФСИН России, в 2015 г. в Воронежском институте ФСИН России началась подготовка курсантов по образовательной программе высшего образования 10.05.02 «Информационная безопасность телекоммуникационных систем».

Профессиональная компетентность выпускников в области информационной безопасности образуется из системной интеграции в научно-исследовательской, проектной, контрольно-аналитической, организационно-управленческой и эксплуатационной деятельностях.

В результате освоения образовательной программы у выпускника должны быть сформированы общекультурные, общепрофессиональные, профессиональные и профессионально-специализированные компетенции.

Перечень необходимых для формирования общекультурных, общепрофессиональных и профессиональных компетенций применительно к каждому виду деятельности определяется федеральными государственными стандартами высшего образования. Профессионально-специализированные компетенции соответствуют специализации образовательной программы: в Воронежском институте ФСИН России – сети специальной связи. Среди профессиональных специализированных компетенций выделяются:

способность обеспечить защиту информации в информационных системах учреждений и органов УИС;

способность проводить в учреждениях и органах УИС монтаж и эксплуатацию технических средств защиты информации;

способность осуществлять техническую эксплуатацию в учреждениях и органах УИС современных инфокоммуникационных систем для организации и обеспечения связи, ее развития и совершенствования;

способность организовывать в учреждениях и органах УИС техническую эксплуатацию инженерно-технических средств охраны и надзора (ИТСОН), системы электронного мониторинга подконтрольных лиц и спецтранспорта.

Формирование профессиональной компетентности выпускников осуществляется в ходе изучения дисциплин как базовой части, в том числе дисциплин специализации, определяемые институтом самостоятельно, так и вариативной.

Профессионально-специализированные компетенции формируются в ходе изучения таких дисциплин, как «Информационная безопасность», «Организационно-правовое обеспечение информационной безопасности», «Технические средства и методы защиты информации», «Программно-аппаратные средства и методы защиты информации».

Большую роль играет практическая подготовка курсантов в рамках учебной, производственной и преддипломной практики, проходящей на базе структурных подразделений ФСИН России, особое место среди которых занимает Научно-исследовательский институт информационных технологий ФСИН России, на базе которого курсанты в период прохождения практики формируют профессиональные умения и навыки будущей профессиональной деятельности.

Образовательный процесс в институте обеспечивают высококвалифицированные специалисты, обладающие высоким уровнем научного потенциала, достаточным опытом педагогической работы и практической деятельности. 82 % профессорско-преподавательского состава кафедр имеют ученую степень и звание, 19 % из них – доктора наук, профессора.

Развитая учебно-материальная база института представлена лабораториями и специализированными кабинетами, такими как лаборатория технических каналов утечки информации, лаборатория технической защиты информации, аудитория специальной техники и оперативно-технических мероприятий, на базе которых проводятся учебные занятия по дисциплинам специализации, что позволяет отрабатывать у обучающихся практические профессиональные умения и навыки по избранной специальности в сфере ИБ и ЗИ.

Выпускники Воронежского института ФСИН России по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» и направлению подготовки 10.07.01 «Информационная безопасность» могут работать в подразделениях инженерно-технического обеспечения и связи учреждений и управлений ФСИН России, в уголовно-исполнительных инспекциях на должностях, связанных с организацией и эксплуатацией сетевого и коммутационного оборудования, инженерно-технических средств обеспечения надзора, информационной безопасности в системах связи и сетях передачи данных, систем электронного мониторинга, а также в научно-исследовательских подразделениях и учебных заведениях УИС.

Исходя из изложенного планируется дальнейшее совершенствование подготовки кадров по информационной безопасности для уголовно-исполнительной системы в Воронежском институте ФСИН России за счет выполнения необходимых мероприятий:

по разработке проекта концепции развития ИБ и ЗИ УИС до 2030 г.;

планированию кадровой обеспеченности подразделений ФСИН России, в которых требуются специалисты в области ИБ и ЗИ;

открытию в Воронежском институте ФСИН России новой специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», позволяющей готовить универсальных специалистов как юридического, так и технического профиля.

УДК 343

Н.В. Лукашов

СОВРЕМЕННЫЕ МЕТОДЫ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ И ПОДГОТОВКИ КАДРОВ ДЛЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОМПЬЮТЕРНЫХ И ИНЫХ ВЫСОКИХ ТЕХНОЛОГИЙ

Термин «высокие технологии» (ВТ) все чаще используется в юридической теории и практике. Однако при этом наблюдается тенденция усугубляющейся неоднозначности трактовки термина, особенно в связи с расследованием преступлений, когда ВТ понимается в узком смысле – синонимом компьютерным информационным технологиям. Так, инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола в разделе «Информационное обеспечение борьбы с преступлениями в области высоких технологий» предусмотрено, что взаимодействующие органы направляют запросы о преступлениях в области высоких технологий, связанных с «неправомерным доступом к компьютерной информации; созданием, использованием и распространением вредоносных программ для ЭВМ; нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети». Данная инструкция фактически ограничивает сферу ВТ сферой информационных технологий (ИТ).

Между тем вне сферы правоохранительной деятельности ВТ трактуются существенно шире и определяется, например, в Большой российской энциклопедии как «совокупность информации, знаний, опыта, материальных средств, используемых при разработке, создании и производстве как новых (ранее неизвестных) продукций и процессов, так и для улучшения качества и удешевления производства известных продуктов».

Исходя из этого понятно, что к ВТ относятся ядерные, космические, генетические, нано- и ряд других технологий, что и подтверждается практикой. Очевидно расхождение между юридической и общепринятой терминологией в определении одной предметной области, а именно сужение общего, родового понятия ВТ до видового ИТ. Это негативно ска-

зывается на эффективности раскрытия и расследования преступлений в данной сфере, имеющих ряд специфических особенностей.

Одной из них является расширенная практика привлечения специалистов и экспертов. Другая особенность – повышенная общественная опасность преступлений в сфере ВТ, что позволяет поставить вопрос о совершенствовании квалификации преступлений и рассматривать использование ВТ в качестве отягчающего обстоятельства. Третьей особенностью является «инновационность» преступности в сфере ВТ, использование не известных ранее схем совершения преступлений, что обусловлено естественной новизной самих технологий.

Таким образом, можно обозначить ряд проблем, требующих безотлагательного решения. Среди них мы выделяем:

1. Необходимость нормативного закрепления понятия «высокая технология». Основной признак ВТ – их сложность и оригинальность, недоступность для воспроизведения без специальных знаний, инструментов, материалов, а также, как правило, без глубокого разделения труда специалистов разного профиля.

2. Совершенствование, наработка методик расследования и квалификации преступлений в сфере ВТ.

3. Формирование системы упреждающего реагирования и профилактики на вероятные угрозы для общества при совершении преступлений в сфере ВТ.

Традиционные подходы к организации раскрытия и расследования преступлений нуждаются в пересмотре в связи со спецификой современных ВТ, которые появились в результате перехода общества в новую стадию развития – так называемую информационную цивилизацию.

Очевидно, что оперативная работа сегодня, как правило, не проводится без использования в той или иной степени технических средств, информационных систем и т. д. Арсенал современного оперативника несравненно богаче, чем у его коллеги, например, в XIX в., когда был сформирован классический образ сыщика.

В этой связи можно было бы предположить, что эффективность, показатели работы современного оперативного работника должны быть выше, чем 100, 50 или даже 20 лет назад. Однако этого не наблюдается. Более того, если исходить из соотношений общей численности оперативных работников (с учетом специалистов по отдельным видам ОРД) к количественным показателям эффективности, получатся обратные зависимости.

Дело в том, что применение современных высокотехнологичных средств предполагает наличие специальных навыков в технической, а не гуманитарной (юриспруденция, психология и т. д.) сфере, то есть человек должен сочетать в себе оба качества, традиционно считающие-

ся мало совместимыми. Поэтому в силу объективной необходимости, существуя в мире машин и компьютеров, сыщик даже самого гуманитарного склада вынужден в той или мере их осваивать. Но лишь очень немногие могут похвастаться хорошим знанием техники и умением владеть ею.

Эта особенность человеческого сознания не позволяет большинству оперативных работников органично сочетать гуманитарные и технические формы и методы работы, как и переключаться с одного вида деятельности на другой, что часто бывает психологически трудно. К тому же использование технических и иных средств специальными службами отвлекает от непосредственной работы с людьми, снижая психологизм, глубину познания сути происходящего. Между тем, несмотря на обилие техники, управляют ею по-прежнему люди, и именно люди совершают преступления, пусть даже и в самой высокотехнологичной сфере.

Наиболее рациональным решением проблемы представляется развитие коллективных (бригадных) методов работы. В этом случае, сводя к минимуму формализм во взаимодействии специалистов по двум-трем направлениям, можно существенно повысить эффективность раскрытия и расследования преступлений. Идея сама по себе не нова, в ведомственной литературе она неоднократно освещалась и прорабатывалась, однако на тот момент не получила достойного практического воплощения.

Такой способ систематически практиковался с участием автора в особых условиях на рубеже 1990-х гг. и неизменно показывал чрезвычайно высокую эффективность. Так, количество ОРМ, проводимых с использованием технических средств соответствующими специалистами в составе бригады при наличии нормативных правовых оснований, в 5–10 раз превышало соответствующий показатель при организации аналогичных мероприятий на основе межведомственного и внутриведомственного взаимодействия отдельных служб. При этом существенно возрастала результативность и оперативность, а снижалась трудоемкость подготовки и проведения.

К сожалению, на базе действующей системы организации деятельности субъектов ОРД и органов расследования, широкое внедрение такого проведения ОРМ представляется крайне трудно решаемой задачей. В первую очередь по причине внутриведомственного и межведомственного разграничения регламентов на проведение различных видов ОРМ и процессуальных регламентов, которыми руководствуется оперативный работник. Необходимо разработать единые регламенты, стандарты расследования, подготовки и проведения ОРМ, позволяющие снизить уровень внутриведомственной и межведомственной разобщенности.

Это позволило бы формировать оперативные группы с участием представителей разных специализированных служб под общим единым руководством, уполномоченным решать вопросы с привлечением их для выполнения соответствующих заданий напрямую, без трудоемкой процедуры согласования.

Одним из возможных путей организации такого взаимодействия может стать использование ситуационных центров или центров оперативного управления, развитие которых стало одним из трендов в ходе реформирования системы правоохранительных органов.

На базе таких ситуационных центров могли бы функционировать смешанные, в том числе межведомственные, оперативно-следственные группы, в составе которых сменами по 2–3 месяца, вахтовым методом, работали бы специалисты необходимых профилей. Срок привлечения специалистов может определяться средним временем раскрытия и расследования преступления (группы преступлений) до передачи дел в суд. Такой центр расследования преступлений (ЦРП) в сфере ВТ может иметь картотеку сотрудников и специалистов, обладающих необходимыми знаниями и навыками, и привлекать их к работе на плановой (посменной) или при крайней необходимости внеплановой основе.

В свою очередь, специалисты, перенимая передовой опыт работы в ЦРП, могут стать проводниками для его распространения в своих базовых подразделениях. Очевидно, что такой Центр помимо методических функций должен осуществлять прогнозирование, а также разработку мер по превентивному реагированию и профилактике преступности в сфере ВТ.

Таким образом, противодействие новому виду преступлений, характерному для современного этапа развития общественных отношений, может и должно осуществляться на основе новых принципов организации выявления, раскрытия и расследования преступлений.

УДК 002.6(476)

А.А. Мушта

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ПРОСТРАНСТВО БЕЛАРУСИ: КОМПЕТЕНТНОСТЬ АНАЛИТИКИ И КУЛЬТУРА АНАЛИТИКА

Установка Президента А.Г. Лукашенко о необходимости придать экспертно-аналитическую направленность управленческим решениям, принимаемым по важнейшим вопросам социально-экономического развития государства и обеспечения его безопасности, продолжает оставаться актуальной. В пользу этого свидетельствует ряд обстоятельств.

Во-первых, как показывает практика, некоторые из разрабатываемых проектов правовых актов, госпрограмм и масштабных управленческих решений, затрагивающих интересы граждан, общества и государства, не получают продуманного научно-экспертного обоснования, вследствие чего они нередко неадекватны сложившейся обстановке.

Во-вторых, несмотря на то, что, по данным Белстата, научными исследованиями и разработками в Беларуси в 2016 г. занимались 431 организации (25,9 тыс. человек), сложившаяся в стране разветвленная система государственных научно-исследовательских институтов, иных информационно-аналитических и экспертных органов, наряду с несомненными достоинствами, имеет фрагментированный и неоднородный характер, узкопрофессиональную специализацию, ведомственную раздробленность и подвержена бюрократизму. В итоге экспертное сообщество недостаточно задействовано в решении назревших и долгосрочных проблем страны.

В-третьих, имеющиеся в стране возможности для использования науки в качестве «интеллектуального усилителя» государственного управления реализованы не в полной мере. Так, например, несмотря на ряд прорывных социологических проектов (прогностическое исследование «Беларусь-2030», Республиканский научный кластер изучения социально-политической ситуации), директор Института социологии НАН Беларуси И. Котляров вынужден констатировать следующее: «Проблема огромной важности – безопасность, теоретических и прикладных социологических исследований ей явно не хватает. Они не приобрели важной самостоятельной научной траектории и находятся в тени...»

В-четвертых, остается мало востребованным аналитический потенциал негосударственного сектора экспертного сообщества Беларуси. При том, что в нем, согласно Международному индексу исследовательских центров («2016 GlobalGoTo ThinkTankIndex»), функционирует 21 «фабрика мысли».

В-пятых, резервы и точки роста имеются и у информационно-аналитических структур органов правопорядка и безопасности, от которых Глава государства требует «постоянно держать руку на пульсе жизни страны, представлять Президенту абсолютно объективный анализ и прогноз развития обстановки, оперативно выявлять проблемы, угрожающие национальной безопасности, экономической и социальной стабильности, и вносить конкретные предложения по их решению».

Представляется, что в основе вышеуказанных проблем лежит сложный комплекс причин, обусловленных как внешними факторами, так и ситуацией, сложившейся непосредственно в самом экспертном сообществе. Отметим некоторые из них.

1. Проблемы ресурсного обеспечения информационно-аналитической работы (техническое, технологическое, программное, финансовое, научно-методическое, нормативно-правовое и собственно кадровое обеспечение).

2. Острый дефицит аналитических кадров. В системе подготовки и переподготовки кадров для органов безопасности и правопорядка необходимо продолжить развивать образовательные и обучающие программы, направленные на дальнейшую профессионализацию и специализацию сотрудников аналитических подразделений. При этом образование и переподготовка аналитиков должны стать стандартной, цикличной чертой их служебной карьеры. Позитивным примером здесь является программа переподготовки кадров по новой специальности «информационно-аналитическая работа в системе органов государственного управления», реализуемая в рамках государственного заказа с 1 сентября 2015 г. на базе Института государственной службы Академии управления при Президенте Республики Беларусь.

3. Проблемы профессиональной компетентности и информационно-аналитической культуры практикующих аналитиков. Так, например, попытки привлечения для работы в органы госуправления внешних экспертов нередко наталкиваются на их политическую ангажированность, конъюнктурность и оторванность от реальных проблем. Многие из «примелькавшихся» в СМИ, на телеэкранах и в соцсетях экспертов имеют двусмысленные идеологические взгляды и неоднозначную репутацию.

4. Всеядность подвизающихся на аналитическом поприще отдельных персонажей размывает границы между научной экспертизой, политической аналитикой, пропагандой и пиаром. В итоге весьма затруднительно оценить подлинную квалификацию того или иного «эксперта», претендующего на объективность анализа.

Интернет и связанные с ним социальные сети ломают традиционную иерархию экспертных авторитетов и выстраивает новую. На базе интернет-форумов возник феномен диванной аналитики, характеризующейся высокой степенью самоорганизации, чрезвычайной активностью и крайне низким уровнем компетентности, деформированными представлениями об аналитической культуре.

В этих условиях отдельные специалисты заговорили даже о «смерти экспертизы». Вот что пишет Tom Nichols: «Я – эксперт. Когда я высказываюсь на какую-то тему, я ожидаю, что мое мнение будет иметь больший вес, чем таковое большинства других людей. Но сейчас, оказывается, это не так. Сегодня любое утверждение эксперта провоцирует взрыв гнева группы или отдельных граждан. Таковых особенно мно-

го в социальных медиа. Сейчас любой может ворваться в комментарии любой интернет-публикации. Иногда такой аттракцион способствует мышлению. Но в большинстве же случаев это значит, что любой может написать все, что захочет, скрывая свое под «ником», без какой-либо обязанности защищать свое мнение или быть призванным к ответу за ложные высказывания».

Речь идет о таких признаках отсутствия аналитической культуры, как попытки убеждения оппонента не логическими доводами и фактами, а через повторение бездоказательных утверждений; необоснованные обобщения и экстраполяции; стремление к опровержению статистических данных единичными примерами; избирательное применение данных и логических рассуждений; непонимание неравной ценности различных источников информации; неспособность к логическим рассуждениям как таковым.

5. Недостаточное внимание к позитивному зарубежному опыту. Речь идет об аналитических структурах таких стран, как Украина, Республика Казахстан, Российская Федерация, США. Так, например, в 1993 г. Национальная академия наук Украины создала Службу информационно-аналитического обеспечения органов государственной власти. В структуре Национальной академии государственного управления при Президенте Украины с 2000 г. действует кафедра национальной безопасности, которая готовит специалистов госуправления сферой нацбезопасности и стратегического планирования. На фоне длящегося уже три года вооруженного конфликта заметно выросла роль Национального института стратегических исследований (НИСИ) – базового научно-исследовательского учреждения, осуществляющего научно-аналитическое сопровождение деятельности Президента Украины и Совета национальной безопасности и обороны. В частности, НИСИ сыграл важнейшую роль в подготовке концептуально новых документов, в числе которых Стратегия национальной безопасности, Военная доктрина, Концепция развития сектора безопасности и обороны Украины, Концепция информационной безопасности, Стратегический оборонный бюллетень Украины. Отдельно следует отметить впервые принятую Стратегию кибербезопасности Украины. Но даже в условиях такой, казалось бы, весомой востребованности директор НИСИ академик В. Горбулин признает: «Сегодня мы оказались в ситуации неоднозначных отношений между государством и научно-экспертным сообществом. ... Государство не формулирует задач для украинской науки. Во многом потому, что оно само работает преимущественно в режиме спонтанного реагирования и простейших реакций, в нем часто отсутствует функция прогнозирования».

В сложившейся социально-экономической ситуации роль экспертно-аналитического обеспечения управленческих процессов значительно возросла. Следует согласиться с исследователями, утверждающими, что именно информационно-аналитическая функция является системообразующей в системе государственной службы. С учетом этого, видимо, пришло время на государственном уровне проанализировать состояние экспертной деятельности в стране, ее инфраструктуру, тематику научно-исследовательских работ, механизм их финансирования, порядок подготовки кадров и повышения их квалификации, чтобы внести предложения по ее системному совершенствованию. В целях институционализации научно-экспертного сопровождения госуправления можно было бы рассмотреть вопрос о целесообразности разработки законопроекта «О научно-экспертном сопровождении государственного управления». Наконец, в связи с созданием и предстоящим вводом в Беларуси единого портала государственной службы следует подумать над тем, чтобы его важной частью стал модуль «Информационно-аналитическое обеспечение и экспертиза».

Игнорирование или недооценка информационно-аналитической работы ведет к социальной агнозии, т. е. либо к неспособности полного и качественного отбора и глубокого анализа информации о социальных процессах, либо к фрагментарному, избирательному, социально-непродуктивному ее использованию. Любой из вариантов чреват возникновением негативных социальных последствий.

УДК 613.8

С.В. Петровский

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ АНАЛИТИКА СПЕЦСЛУЖБЫ

Процесс развития информационного общества, помимо многочисленных позитивных моментов, связанных с увеличением количества легкодоступных информационных ресурсов, породил и ряд серьезных проблем, обусловленных уходом в виртуальное пространство открытых телекоммуникационных сетей политических, экономических, религиозных и других конфликтов. Обыденными (как для политиков, так и для бизнесменов) стали следующие понятия: «информационная война», «сетевая война», «информационный вброс», «аналитическая разведка», OSINT (разведка по открытым источникам), «конкурентная разведка», «бархатная революция» и т. п.

Значительное увеличение интенсивности информационных потоков потребовало совершенствования методов поиска, сбора и обработки

информации, необходимой для ведения разведывательной, контрразведывательной, оперативно-розыскной деятельности, информационно-аналитического обеспечения при принятии управленческих решений.

Информационно-аналитическая работа из вспомогательного вида контрразведывательной/оперативно-розыскной деятельности институализировалась в самостоятельный вид оперативно-служебной деятельности спецслужб и правоохранительных органов.

Класификация «аналитик» стала массовой, что породило ряд проблем, связанных с подбором, подготовкой и обеспечением эффективной работы профессионалов в сфере информационного обеспечения управления.

Практика аналитической работы в спецслужбе, а также исследования, проводившиеся российскими и американскими психологами, показывают, что аналитик, осуществляющий информационно-аналитическую поддержку управления оперативным подразделением/органом должен иметь развитый интеллект, обладать способностью (и навыками) к самосовершенствованию, знать специфику деятельности подразделения/органа, иметь представление об оперативной работе, владеть навыками практического психолога, владеть писательским мастерством, уметь эффективно работать в стрессовых условиях, обладать хорошим здоровьем (психофизиологической выносливостью).

По мнению профессора Московского государственного института культуры Н.А. Слядневой, информационная аналитика как интеллектуальный вид деятельности предполагает синтез трех компонентов: владение аналитическими методами (функциональный компонент), знание предметной области (отраслевой компонент) и определенный тип одаренности, структуры личности (личностный компонент).

Функциональный и отраслевой компоненты достаточно легко нарабатываются в ходе обучения и профессиональной деятельности аналитика, методики их развития достаточно хорошо описаны в литературе и вопросов не вызывают. Что касается личностного компонента, то он в первую очередь включает навыки творческого мышления, повышенную обучаемость, устойчивость к информационным перегрузкам и стрессоустойчивость.

На сегодняшний день формированию личностного компонента в ходе подготовки и переподготовки специалистов-аналитиков должного внимания не уделяется. И если применительно к развитию творческих способностей имеются устоявшиеся методики подготовки профессионалов для научно-исследовательской, творческой, преподавательской, управленческой и других видов деятельности, то в том, что касается обеспечения их информационно-психологической безопасности (ИПБ), отсутствует не только понимание необходимости работы в этом направлении, но и однозначное определение такого явления, как ИПБ.

Под информационно-психологической безопасностью аналитика, как правило, понимается не защита его сознания, не обеспечение высокой степени упорядочения работы головного мозга, не устойчивость режима сознательного распределения внимания на совершаемых операциях, а защита от внешнего информационного (идеологического) воздействия.

Работа аналитика связана с постоянным, длительным и интенсивным воздействием (или ожиданием воздействия) экстремальных значений профессиональных, социальных, экологических факторов, которое сопровождается негативными эмоциями, перенапряжением физических и психических функций организма.

При этом отсутствует понимание того, что, как указывали в своих работах российские аналитики Ю.В. Курносов и П.Ю. Конотопов, информационно-аналитическая работа (ИАР) – это специфический вид мыслительной деятельности человека, связанный с извлечением из некоторого массива входных данных информации (нового знания об объекте исследования) на основе использования некоторой относительно устойчивой субъективной модели мира. Специфика этого вида мыслительной деятельности, по мнению авторов, заключается в недопущении субъектом ИАР (аналитиком) неконтролируемой, спонтанной модификации собственной модели мира в результате воздействия потока входных данных – в противном случае мы наблюдаем полную потерю не только творческой, но и физической работоспособности.

Наиболее характерным психическим состоянием, развивающимся на фоне длительной работы в форс-мажорных обстоятельствах, является информационный стресс – состояние информационной перегрузки, возникающее в результате увеличения интенсивности потока данных, приводящего к состоянию, при котором объемы поступающей полезной информации превосходят возможности ее восприятия человеком. Аналитик в условиях сильного информационного зашумления не успевает обрабатывать входящую информацию и, соответственно, решать поставленные задачи, принимать правильные решения в требуемом темпе, неся при этом ответственность за последствия принимаемых руководителем управленческих решений.

Психологи, работающие в сфере обеспечения безопасности (национальной, экономической и т. п.), неоднократно обращали внимание на то, что высокая напряженность и специфика труда специалистов в области информационно-аналитической работы требует специальных мер и приемов, нацеленных на обеспечение их личной информационно-психологической безопасности. Н.А. Сляднева еще несколько лет назад весьма критично высказывалась в отношении данной проблемы. «…Поскольку в большинстве случаев эти люди, обладающие высочай-

шей квалификацией в своей предметной области, не проходили специальной подготовки, а приемы интеллектуальной деятельности изучали самостоятельно и бессистемно, постольку в вопросах защиты от разнообразных угроз, проявленных в информационно-психологической сфере, они оказываются фактически безграмотными», – считает она.

К критериям ИПБ личности аналитика можно отнести: степень удовлетворенности личности состоянием ИПБ; степень адекватности отражения личностью окружающего мира; степень устойчивости личности к информационно-психологическим воздействиям.

В свою очередь, показателями информационно-психологической устойчивости являются: развитость мышления, внимания; навыки и умения информационно-аналитической работы; знание об угрозах информационной среды, а также о методах обеспечения личной информационно-психологической безопасности; стрессоустойчивость.

Часть этих показателей можно существенно повысить посредством тренировок. На сегодняшний день можно выделить несколько основных направлений повышения интеллектуальной активности и стрессоустойчивости аналитика:

методы классической и восточной психологии, в основе которых лежат либо различные подходы к аутогенной тренировке, либо медитативные практики, например различные варианты психической саморегуляции, тренинги увеличения скорости чтения и запоминания информации, развития внимания, разрабатываемые школой академика Андреева, центром интеллектуальных технологий И. Полонейчика, Хасаем Алиевым (метод «ключ») и т. п.;

методы аудиовизуальной стимуляции работы мозга, в том числе программно-аппаратные методы бинауральной стимуляции и синхронизации работы мозга, например аудио-CD-диски Института Монро (США), Gateway Sound Studio (Москва), майнд-машины разработки ООО НПП «МедПАСС» (Санкт-Петербург), «Навигатор» (Москва) и Photosonix (США), а также их программные реализации («Радуга – дуга» Андрея Патрушева);

использование природных и искусственных нутриентов для улучшения деятельности мозга (антиоксиданты, ноотропы, активаторы мозговых метаболизмов, церебральные вазодиляторы и др.).

Апробация отдельных комбинаций вышеуказанных методов на базе центра подготовки космонавтов РФ, Военно-медицинской академии РФ им. С.М. Кирова, Санкт-Петербургского научно-исследовательского института физической культуры, Уральского юридического института МВД России показала их высокую эффективность и возможность использования для снижения психоэмоциональных нагрузок и повышения стрессоустойчивости сотрудников информационно-аналитических подразделений спецслужб и правоохранительных органов.

УДК 343

В.В .Чикунов

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями. Происходит эволюция информационного противоборства как новой самостоятельной стратегической формы глобальной конкуренции. Распространяется практика целенаправленного информационного давления, наносящего существенный ущерб национальным интересам. В связи с этим одним из приоритетных направлений является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится активизации деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством, комплексному совершенствованию процессов предупреждения и борьбы с преступностью, в первую очередь с коррупцией, терроризмом и экстремизмом во всех их проявлениях, расовой и религиозной нетерпимостью.

Как известно, оперативно-розыскная деятельность направлена на предупреждение, выявление, пресечение и раскрытие преступлений, т. е. является первоначальным звеном в борьбе с преступностью. Иными словами, оперативно-розыскные органы, осуществляющие указанную деятельность, практически встречают преступников и других правонарушителей на пороге действия уголовного законодательства, препровождая их для дальнейшего осуществления расследования и судебного рассмотрения в сферу уголовного процесса (досудебного и судебного производства) и воздействия уголовного права, решения вопроса о применении наказания к виновным лицам.

На сегодняшний день широта сферы действия оперативной деятельности основана на теоретических исследованиях, включающих в себя вопросы права, специального технического оснащения, методов и тактики оперативной работы, особенностей получения информации, ее анализа и т. д.

Оперативные подразделения правоохранительных органов в последнее время претерпели незначительные организационно-штатные изменения, которые не повлияли на эффективность управленческой деятельности в сфере ОРД, но имеется необходимость во внедрении новых подходов и методов к организации борьбы с преступностью. Они, прежде всего, должны основываться на системном анализе разнородной информации, имеющей отношение к решению задач ОРД, чтобы определить тенденции развития основных криминогенных процессов, происходящих в обществе. Важнейшую роль в этом плане призвана играть аналитическая работа в сфере ОРД (далее – аналитическая работа, аналитическая деятельность или криминальный анализ), характеризующаяся совокупностью особых признаков, которые выделяют ее среди прочих видов анализа в деятельности органов внутренних дел, и являющаяся одним из основных элементов процесса познания, осуществляемого в ходе решения задач ОРД.

Состояние правопорядка в Республике Беларусь свидетельствует о том, что правоохранительным органам, в первую очередь органам внутренних дел, в настоящее времени удалось найти адекватные средства противодействия преступности, обеспечить надежную защиту личности, общества, государства от противоправных посягательств.

Система МВД, располагая наибольшими среди иных правоохранительных органов возможностями по противодействию преступности, использует их достаточно эффективно. Однако имеются случаи, когда принимаемые на уровне МВД, УВД, РОВД меры по реагированию на изменения оперативной обстановки отстают от объективных реалий и поэтому теряют свою остроту и действенность. Это свидетельствует об имеющихся резервах в аналитической работе и принятии управленческих решений в органах внутренних дел различного иерархического уровня.

Возможное снижение качества, надежности и оперативности управления органами внутренних дел может быть обусловлено рядом причин, в том числе недооценкой значимости информационно-аналитической работы, недостатком высококвалифицированных специалистов аналитиков-управленцев, ухудшением уровня материально-технического оснащения подразделений, особенно районного звена.

В этой связи с целью совершенствования практики организации информационно-аналитического обеспечения ОРД по борьбе с преступностью предлагается осуществить ряд организационных мер по следующим основным направлениям:

1. Совершенствование организационно-структурного построения подразделений оперативно-информационной работы криминального блока РОВД. Создание подразделений ИАР КМ (на уровнях центрального аппарата, УВД и РОВД), основной задачей которых должен являться анализ оперативной обстановки на обслуживаемой территории и выработка предложений по ее улучшению.

Результаты проведенного исследования показали, что в МВД Республики Беларусь созданы отделы оперативно-информационной работы согласно Приказу МВД Республики Беларусь № 345 от 29 июля 2013 г. На уровне территориального ОВД за данной линией работы, как правило, закрепляется один из сотрудников, в функциональные обязанности которого вменяется регистрация материалов оперативно-розыскного характера, проверка правильности заполнения карточек, ведение статистических учетов, внесение оперативных сведений.

В ОВД первой и второй категории ввиду малочисленности подразделений криминальной милиции подобные обязанности возложены, как правило, на начальника подразделения или старшего группы. Поэтому можно констатировать, что реальный анализ полученной оперативно-розыскной информации не проводится, что в итоге сказывается на состоянии всей организации оперативно-розыскной деятельности по борьбе с преступностью по всем направлениям служебной деятельности.

На первоначальном этапе решения данной проблемы нами видится необходимо закрепления руководителем РОВД за наиболее квалифицированным сотрудником служб КМ линии по информационно-аналитическому обеспечению ОРД в полном объеме. Причем, как нам представляется, важно создать сотруднику такие условия, при которых он будет заниматься исключительно данным направлением деятельности.

2. Активное внедрение в практику возможностей сети Интернет. В последние годы из-за развития информационных технологий сотрудники оперативных аппаратов РОВД могут получать сведения благодаря механизму инициативного поиска с использованием открытых источников (OSINT), в том числе в сети Интернет.

3. Создание принципиально новых и синхронизация уже имеющихся автоматизированных информационных систем оперативно-розыскного назначения с возможностью сквозного поиска, т. е. создание единой поисковой информационной системы МВД.

4. Разработка и внедрение специального программного обеспечения по сбору, обработке и анализу данных и подготовка и переподготовка кадров на различных ступенях образования.

СВЕДЕНИЯ ОБ АВТОРАХ

АЛЕФИРЕНКО Виктор Михайлович, доцент кафедры проектирования информационно-компьютерных средств Белорусского государственного университета информатики и радиоэлектроники, кандидат технических наук, доцент.

АРЧАКОВ Владимир Юрьевич, заместитель Государственного секретаря Совета Безопасности Республики Беларусь.

БАБИЧ Максим Александрович, аспирант Белорусского государственного университета информатики и радиоэлектроники.

БЕЛЫЙ Денис Владимирович, инженер-программист Объединенного института проблем информатики Национальной академии наук Беларуси.

БОБОВИЧ Николай Михайлович, доцент кафедры правовой информатики Академии МВД Республики Беларусь, кандидат технических наук, доцент.

БОНДУРОВСКИЙ Владимир Владимирович, заместитель Ответственного секретаря Парламентской Ассамблеи ОДКБ, член Координационного совета Международного союза юристов, кандидат юридических наук, доцент.

БОРОВИК Владан, магистр наук в области информационных технологий, технический специалист в области информационных технологий, Министерство внутренних дел Сербии.

БОРОВИК Петр Леонидович, доцент кафедры правовой информатики Академии МВД Республики Беларусь, кандидат юридических наук.

БУЛАЙ Родика Ивановна, преподаватель кафедры специальной разыскной деятельности и информационной безопасности Академии «Штефан чел Маре» МВД Республики Молдова, магистр информационной безопасности.

БУЛАЙ Юрий Георгиевич, доцент кафедры уголовного процесса и криминалистики Академии «Штефан чел Маре» МВД Республики Молдова, доктор права.

ВУС Михаил Александрович, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН России, кандидат технических наук.

ВЯТКИН Денис Николаевич, начальник сектора Оперативно-аналитического центра при Президенте Республики Беларусь.

ГОРОШКО Игорь Владимирович, начальник кафедры математики и информационных технологий управления Академии управления МВД России, доктор технических наук, профессор.

ГУБИЧ Михаил Валерьевич, старший преподаватель кафедры правовой информатики, кандидат юридических наук.

ГУТЕР Кристина Юрьевна, курсант уголовно-исполнительного факультета Академии МВД Республики Беларусь.

ДРЫБИН Евгений Александрович, аспирант Белорусского государственного университета.

ДУШКИН Александр Викторович, начальник кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, доктор технических наук, доцент.

ЖЕЛЕЗНЯК Владимир Кириллович, заведующий кафедрой радиоэлектроники Полоцкого государственного университета, доктор технических наук, профессор.

ЖЕЛЕЗНЯКОВ Александр Владимирович, начальник кафедры специальных и инженерно-технических дисциплин факультета внутренних войск Военной академии Республики Беларусь.

ИЗОТОВ Петр Павлович, начальник сектора разработок цифровых систем Гомельского филиала Научно-исследовательского института технической защиты информации, кандидат технических наук, доцент.

КАЛИБЕРОВ Андрей Васильевич, доцент кафедры специальных дисциплин Государственного института повышения квалификации и переподготовки кадров таможенных органов Республики Беларусь.

КАСАНИН Сергей Николаевич, заместитель директора по науке Научно-исследовательского института технической защиты информации, кандидат технических наук, доцент.

КЕТУРКО Виктор Федорович, преподаватель правовой информатики Академии МВД Республики Беларусь.

КИСЛИНСКИЙ Роман Валентинович, старший преподаватель кафедры специальных и инженерно-технических дисциплин – начальник службы (автоматизации) Военной академии Республики Беларусь.

КЛАЧКЕВИЧ Евгений Михайлович, курсант факультета внутренних войск Военной академии Республики Беларусь.

КОВАЛЕНКО Александр Николаевич, заместитель начальника кафедры специальных и инженерно-технических дисциплин факультета внутренних войск Военной академии Республики Беларусь.

КОВАЛЬЧУК Александр Александрович, адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

КОЧЕДЫКОВ Сергей Сергеевич, профессор кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, кандидат технических, доцент.

КУЗИН Евгений Борисович, преподаватель кафедры математики и информационных технологий управления Академии права и управления ФСИН России.

КУК Кристиян, доцент кафедры информатики и вычислительной техники Академии криминалистических и полицейских исследований (Сербия), кандидат технических наук.

ЛАВРЕНОВ Виктор Вячеславович, старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

ЛЕБЕДЕВ Вадим Николаевич, заместитель начальника кафедры информационных технологий Академии управления МВД России, кандидат технических наук, доцент.

ЛЕВДАНСКИЙ Максим Владимирович, глава представительства ООО «D-Link International Pte Ltd» (Сингапур) в Республике Беларусь.

ЛЕМЕШЕВСКИЙ Олег Олегович, магистрант факультета внутренних войск Военной академии Республики Беларусь.

ЛЕПЁХИН Александр Николаевич, начальник кафедры правовой информатики Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

ЛУГОВАЯ Алла Владимировна, заместитель начальника Воронежского института ФСИН России по учебной работе, кандидат философских наук, доцент.

ЛУКАШОВ Николай Васильевич, ведущий научный сотрудник отдела исследований и стратегических проблем управления научно-исследовательского центра Академии управления МВД России, кандидат физико-математических наук, доцент.

МАКАРОВ Олег Сергеевич, начальник информационно-аналитического управления Государственного секретариата Совета Безопасности Республики Беларусь, доктор юридических наук, доцент.

МАЛИКОВ Владимир Викторович, начальник цикла технических и специальных дисциплин Центра повышения квалификации руководящих работников и специалистов Департамента охраны МВД Республики Беларусь, кандидат технических наук, доцент.

МАСКИНА Мария Сергеевна, доцент кафедры математики и информационных технологий управления Академии права и управления ФСИН России, кандидат педагогических наук, доцент.

МАЦЫЛЕВИЧ Александр Ромуальдович, начальник научно-исследовательского отдела (защиты информации и информационных технологий) Научно-исследовательского института Вооруженных Сил Республики Беларусь.

МЕДВЕДЕВ Станислав Андреевич слушатель факультета заочного обучения Академии МВД Республики Беларусь.

МИШУК Сергей Сергеевич, доцент кафедры философии, экономики и истории Международного государственного института имени А.Д. Сахарова БГУ, кандидат философских наук, доцент.

МЛАДЕНОВИЧ Драгун, технический специалист в области информационных технологий, Министерство внутренних дел Сербии.

МУРИНОВ Игорь Викторович, заместитель директора Гомельского филиала Научно-исследовательского института технической защиты информации.

МУШТА Александр Александрович, главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь, кандидат философских наук, доцент.

НОВИКОВ Михаил Константинович, магистрант кафедры управления информационными ресурсами Академии управления при Президенте Республики Беларусь.

ПАНОВИЦЫН Алексей Михайлович, старший инспектор по особым поручениям группы мобилизационной подготовки и территориальной обороны Академии МВД Республики Беларусь

ПАТРАШКО Александр Валерьевич, начальник отдела непрерывного образования Департамента профессионального и менеджменского развития Академии «Штефан чел Маре» МВД Республики Молдова.

ПАЦКЕВИЧ Илья Денисович, курсант факультета внутренних войск Военной академии Республики Беларусь.

ПАШКОВСКИЙ Сергей Владимирович, сотрудник Оперативно-аналитического центра при Президенте Республики Беларусь.

ПЕРЕВАЛОВ Дмитрий Васильевич, заместитель начальника учреждения образования «Центр повышения квалификации руководящих работников и специалистов «Центр специальной подготовки» по научной работе, кандидат юридических наук, доцент.

ПЕРХАЛЬСКИЙ Егор Олегович, магистрант Белорусского государственного университета информатики и радиоэлектроники.

ПЕТРОВСКИЙ Сергей Валерьевич, старший преподаватель специальной кафедры Института национальной безопасности Республики Беларусь.

ПОЛЕЩУК Дмитрий Григорьевич, аспирант Института правовых исследований Национального центра законодательства и правовых исследований Республики Беларусь, магистр юридических наук.

ПОЛКОВНИЧЕНКО Юрий Владимирович, курсант следственно-экспертного факультета Академии МВД Республики Беларусь.

ПОЛЯКОВ Александр Сергеевич, ведущий научный сотрудник Объединенного института проблем информатики Национальной академии наук Беларуси, кандидат технических наук, доцент;

РАНДЕЛОВИЧ Драган, заведующий кафедрой информатики и вычислительной техники Академии криминалистических и полицейских исследований (Сербия), кандидат технических наук, профессор.

САВВА Юрий Болеславович, доцент кафедры информационной безопасности Орловского государственного университета имени И.С. Тургенева, кандидат технических наук, доцент.

САДОВ Василий Сергеевич, аспирант Белорусского государственного университета.

СВИРСКИЙ Евгений Анатольевич, декан факультета инновационного развития и информационных технологий, заместитель директора по учебной и научной работе Института повышения квалификации и переподготовки в области технологий информатизации и управления Белорусского государственного университета, кандидат физико-математических наук.

СИДОРОВИЧ Владислав Олегович, инженер научно-производственного Научно-исследовательского института технической защиты информации.

СТАРОВОЙТОВА Татьяна Феликсовна, доцент кафедры управления информационными ресурсами Академии управления при Президенте Республики Беларусь, кандидат экономических наук, доцент.

СТЕПАНОВА Оксана Вячеславовна, студентка Института подготовки государственных и муниципальных служащих Академии ФСИН России.

СУШКО Александр Евгеньевич, начальник управления по расследованию преступлений против информационной безопасности и интеллектуальной собственности Главного следственного управления Следственного комитета Республики Беларусь.

ТАРАСЕНКО Вячеслав Александрович, курсант 2-го курса факультета внутренних войск Военной академии Республики Беларусь.

ТОПОРИКОВА Ольга Олеговна, начальник отдела криминологической экспертизы проектов законов Научно-практического центра проблем укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь.

УВАРОВ Николай Сергеевич, инженер-программист Научно-исследовательского института технической защиты информации.

ФЕДОРЦОВ Анатолий Викторович, научный сотрудник Научно-исследовательского института Вооруженных Сил Республики Беларусь.

ФУРМАНОВ Алексей Владимирович, курсант 2-го курса следственно-экспертного факультета Академии МВД Республики Беларусь.

ХАНАНОВ Андрей Мавлитович, начальник сектора разработок радиотехнических систем Гомельского филиала Научно-исследовательского института технической защиты информации.

ЧЕРНЫШЕВА Светлана Андреевна, профессор кафедры логистики и информационно-математических дисциплин частного учреждения образования «БИП – Институт правоведения», кандидат технических наук, доцент.

ЧЕРТКОВ Валерий Михайлович, старший преподаватель кафедры радиоэлектроники Полоцкого государственного университета, магистр технических наук.

ЧИКУНОВ Виктор Васильевич, слушатель магистратуры Академии МВД Республики Беларусь.

ЧИСТАЯ Елена Викторовна, преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

ЧУДИЛОВСКАЯ Татьяна Геннадьевна, старший преподаватель кафедры правовой информатики Академии МВД Республики Беларусь.

ШАРАПОВ Сергей Анатольевич, заместитель начальника отдела Оперативно-аналитического центра при Президенте Республики Беларусь.

ШВЕД Надежда Александровна, главный специалист отдела криминологического прогнозирования и разработки предложений по предупреждению преступности, укреплению законности и правопорядка Научно-практического центра проблем укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь, кандидат юридических наук.

ШЕДЬКО Александр Николаевич, заместитель начальника кафедры оперативно-тактической подготовки внутренних войск факультета внутренних войск Военной академии Республики Беларусь.

ШЕМАРОВ Александр Иванович, доцент кафедры электронных вычислительных средств Белорусского государственного университета информатики и радиоэлектроники, кандидат технических наук, доцент.

ШИШКИН Владимир Михайлович, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации РАН России, кандидат технических наук, доцент.

ШТРАПОВ Александр Валентинович, слушатель магистратуры Академии МВД Республики Беларусь.

ЭРЛЕВАЙН Драган, магистр наук, технический специалист в области информационных технологий, Агентство безопасности Республики Сербия.

ЮСУПОВ Рафаэль Мидхатович, директор Санкт-Петербургского института информатики и автоматизации РАН России, доктор технических наук, профессор, заслуженный деятель науки и техники РСФСР, член-корреспондент РАН.

ЯБЛОЧНИКОВ Сергей Леонтьевич, заведующий кафедрой экологии, безопасности жизнедеятельности и электропитания Московского технического университета связи и информатики, доктор педагогических наук, кандидат технических наук, профессор.

ЯБЛОЧНИКОВА Ирина Остаповна, докторант Института высшего образования Национальной академии педагогических наук Украины, кандидат педагогических наук, доцент.

ЯБЛОЧНИКОВА Мария Сергеевна, студентка Московского физико-технического института.

СОДЕРЖАНИЕ

РАЗДЕЛ 2

СОВРЕМЕННЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

РАЗДЕЛ 3

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

РАЗДЕЛ 4
ИННОВАЦИОННЫЕ ПОДХОДЫ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Научное издание

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы Международной научно-практической конференции
(Минск, 18 мая 2017 г.)

Подписано в печать 01.03.2018. Формат 60×84 1/16.
Бумага офсетная. Ризография. Усл. печ. л. 13,48. Уч.-изд. л. 12,79.
Тираж 70 экз. Заказ 66.

Издатель и полиграфическое исполнение:
учреждение образования
«Академия Министерства внутренних дел Республики Беларусь».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий № 1/102 от 02.12.2013.
Пр-т Машерова, 6, 220005, Минск