БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА

ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Сборник статей
5-й Международной
научно-практической конференции

12 октября 2018 г.

Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2019

УДК 351.74:002
ББК 67
П 78

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России
имени И.Д. Путилина

Выпускается с 2015 года.

П 78 Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 5-й Международной научно-практической конференции. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2019. – 176 с.
ISBN 978-5-91776-269-2

В сборнике представлены научные статьи, в которых исследуются проблемы противодействия компьютерным преступлениям и обеспечения информационной безопасности.
Предназначен для курсантов, слушателей, адъюнктов, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников органов внутренних дел.

УДК 351.74:002
ББК 67

ISBN 978-5-91776-269-2

ПРОБЛЕМЫ ОРГАНИЗАЦИИ УЧЕБНОЙ И МЕТОДИЧЕСКОЙ РАБОТЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ МВД РОССИИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

УДК 37.013:519.81

Прокопенко А.Н.,
кандидат технических наук, доцент;
Тримасов Е.А.,
Колтунов Н.Л.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Ключевые слова: отечественное программное обеспечение, офисное программное обеспечение, импортозамещение, операционные системы, офисный пакет.

Аннотация: в статье рассматриваются задачи, поставленные Правительством Российской Федерации и МВД России, по замене используемого офисного программного обеспечения на отечественное ПО в рамках программы импортозамещения. Предлагаются пути решения данных задач, конкретные варианты отечественного программного обеспечения. Анализируются сложности и проблемы технического, программного и методического характера, которые возникнут в процессе импортозамещения.

PROBLEMS OF THE ORGANIZATION OF EDUCATIONAL AND METHODICAL WORK OF THE EDUCATIONAL ORGANIZATION MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION IN THE CONDITIONS OF IMPORT SUBSTITUTION OF THE SOFTWARE

Prokopenko A.N.,
Candidate of Technical Sciences, Associate Professor;
Trimasov E.A.,
Koltunov N.L.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in article the tasks set by the Government of the Russian Federation and the Ministry of Internal Affairs of the Russian Federation of replacement of the used office software on domestic ON within the import substitution program are considered. Solutions of these tasks, concrete versions of the domestic software are

offered. Difficulties and problems of technical, program and methodical character which will arise in the course of import substitution are analyzed.

Key words: domestic software, office software, import substitution, operating systems, office package.

В последние годы в мире сложилась сложная политическая обстановка, связанная с противоправными действиями так называемых «западных государств» против нашего государства. Постоянно выдумываются новые поводы для объявления санкций, ввода все новых экономических и политических ограничений. Россию обвиняют как в реальных преступлениях, совершенных другими лицами, например, сбитом украинской армией малазийском боинге, так и в совершенно нереальных и даже фантастических преступлениях: вмешательство в американские выборы или отравление в Солсбери. Ограничения накладываются как на отдельных физических лиц, так и на юридических лиц, государственных деятелей, банки и целые отрасли экономики. Причем логика этих ограничений одна – нанести как можно больший урон российской экономике. Таким образом, новые ограничения могут быть введены по любому поводу, в любой момент и затронуть любое направление человеческой жизнедеятельности.

В этой связи наблюдается постоянная угроза применения санкций к использованию нашей страной глобальных инструментов для жизни людей. К таким инструментам относятся, например, Общество всемирных межбанковских финансовых каналов связи (SWIFT), предназначенное для осуществления банковских переводов. Важнейшим глобальным инструментом является всемирная компьютерная сеть Интернет. Отключение России от мирового Интернета, блокирование программного обеспечения, используемого для работы на компьютерной технике, является одной из угроз, которые могут быть применены в любой момент.

Для минимизации угроз экономике Российской Федерации в мае 2014 года Президент России Владимир Путин подписал перечень поручений о дополнительных мерах по стимулированию экономического роста, в том числе по импортозамещению в промышленности и сельском хозяйстве. Одним из направлений был переход на отечественное программное обеспечение (далее – ПО). Необходимо отметить, что доля закупок отечественного ПО возросла с 36,7% в 2014 году до 64,8% в 2016 году и продолжает увеличиваться [3]. Одновременно возросла доля закупок работ/услуг в сфере IT с 21,7% до 52,9%.

В продолжение начатого курса на импортозамещение программного обеспечения Правительством Российской Федерации в 2016 году был утвержден План перехода в 2016-2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения [1]. В соответствии с Планом федеральные органы исполнительной власти должны осуществлять переход только на то отечественное офисное ПО, которое включено в единый реестр российских программ для электронных вычислительных машин и баз данных. А в случае предоставления отечественного офисного ПО с использованием

«облачных» технологий должна применяться защищенная система межведомственного электронного взаимодействия, которая используется для оказания государственных услуг населению.

План определил, что в период с мая по декабрь 2018 года федеральные органы исполнительной власти должны реализовать механизм перехода на использование отечественного офисного ПО. Кроме того, в мае 2018 года должны были быть разработаны предложения по реализации указанных механизмов, предусматривающих переход до конца 2020 года органов власти и организаций на использование отечественного офисного ПО.

Во исполнение Распоряжения Правительства Российской Федерации от 26.07.2016 № 1588-р МВД России был принят План-график перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года, утвержденный приказом МВД России от 10.05.2018 № 284 [2].

Приказ утвердил целевые показатели перехода на использование отечественного офисного ПО. Для организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России (к которым относятся образовательные организации), указанные показатели объединены в таблице 1.

Таблица 1.

Целевые показатели перехода на использование отечественного офисного программного обеспечения для организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России

№ п/п	**Наименование категории (типа) офисного программного обеспечения**	**Доля отечественного ПО или доля пользователей, использующих отечественное ПО, не менее**		
		2018 г.	**2019 г.**	**2020 г.**
1.	Офисный пакет или его составные части (текстовый редактор, табличный редактор, редактор презентаций, файл-менеджер, органайзер)	35%	60%	80%
2.	Операционные системы	30%	50%	80%
3.	Почтовые приложения (могут входить в состав офисного пакета)	35%	60%	80%
4.	Справочно-правовая система	100%	100%	100%
5.	Программное обеспечение системы электронного документооборота	50%	75%	100%
6.	Средства антивирусной защиты	100%	100%	100%
7.	Средства мультимедиа (при наличии в едином реестре программного обеспечения эквивалентов иностранному программному обеспечению)	15%	35%	70%
8.	Интернет-браузеры	35%	48%	75%

В соответствии с приведенными целевыми показателями наименьшие проблемы у всех подразделений МВД России, в целом, и у образовательных организаций, в частности, возникнут со справочно-правовыми системами и средствами антивирусной защиты (4 и 6 пункты плана). Это связано с тем, что для обеспечения информационной безопасности в системе МВД России используется антивирус «Касперского», который является отечественной разработкой. Кроме того, практически все справочно-правовые системы, используемые в нашей стране, являются отечественными разработками. К ним относятся и две лучшие СПС – «КонсультантПлюс» и ГАРАНТ. Кроме того, программное обеспечение компании «КонсультантПлюс» используется для функционирования СТРАС «Юрист», которая является справочно-правовой системой, обеспечивающей доступ к нормативным правовым актам МВД России.

Кроме того, представляется, что не возникнет проблем с переходом на отечественное программное обеспечение системы электронного документооборота (5 пункт плана). Это обусловлено тем, что большая часть СЭД на российском рынке разработана российскими компаниями. Например, в Бел ЮИ МВД России имени И.Д. Путилина в качестве внутренней СЭД используется система «Дело» компании «Электронные офисные системы». Кроме того, используемая в ИСОД МВД России СЭД также является отечественной разработкой.

Таким образом, три из восьми позиций не вызовут существенных затруднений в процессе импортозамещения программного обеспечения.

Еще одна позиция плана может вызвать только некоторые сложности при замене на отечественного производителя. Речь идет об интернет-браузерах (8 пункт плана). Отечественный интернет-браузер – Яндекс-браузер является одним из лидеров нашего рынка и переход на него не должен вызвать существенных затруднений. Однако не все приложения, используемые в МВД России, в том числе, входящие в ИСОД МВД России, хорошо взаимодействуют с Яндекс-браузером. В частности, возникали определенные проблемы с работой электронной подписи. Представляется, что администраторы ИСОД МВД России в состоянии решить данные проблемы, что позволит выполнить восьмой пункт плана значительно раньше срока.

Выполнение оставшихся четырех пунктов плана (1, 2, 3 и 7) может сопровождаться существенными техническими, организационными и финансовыми сложностями.

Наиболее часто используемое программное обеспечение – это операционная система и офисный пакет (1 и 2 пункты плана). Операционная система является абсолютно обязательным элементом программного обеспечения. Замена операционных систем потребует не только переучивания сотрудников и работников органов и организаций МВД России, но и существенных финансовых вложений. Например, средняя цена лицензии на право использования операционной системы общего назначения Astra Linux Common Edition для рабочей станции на конец августа 2018 года составляет 4 225 рублей. Таким образом, за 1 млн рублей можно будет закупить только 235 лицензий для операци-

онных систем. Между тем, в Бел ЮИ МВД России имени И.Д. Путилина более 700 компьютеров, которые требуют закупки и установки отечественного ПО. При обращении к акционерному обществу «НПО РусБИТех», разработчик операционной системы согласился безвозмездно предоставить не более 50 лицензий на использование операционных систем «Astra Linux Special Edition» для обеспечения учебного процесса, несмотря на то, что для учебного процесса используется более 150 компьютеров.

При замене офисного пакета Microsoft Office на любой отечественный офисный пакет (преимущественно МойОфис) могут возникнуть проблемы с переводом части файлов в другой формат или неподдержкой отдельных функций. Например, в любой вариант МойОфис не входит система управления базами данных. В то время, как в MS Office имеется MS Access, которая является достаточно неплохой СУБД, позволяющей реализовывать как учебные, так и профессиональные задачи.

Кроме того, в состав пакета «МойОфис Образование», который для образовательных организаций распространяется бесплатно, не входит почтовое приложение. В результате возникнет необходимость или отдельной закупки почтового приложения, или закупки «МойОфис Стандартный», который включает такое приложение. Рекомендованная компанией стоимость одной лицензии на «МойОфис Стандартный» для образовательной организации составляет 761 рубль. Лицензия бессрочная, однако ежегодное обновление будет стоить образовательной организации 343 рубля. Таким образом, внедрение почтового приложения (пункт 3 плана) будет осуществлено вместе с офисным пакетом.

Особые проблемы возникнут с импортозамещением средств мультимедиа (пункт 7 плана). В настоящее время имеется несколько программных продуктов для работы с мультимедиа, внесенных в Единый реестр Российского программного обеспечения. Версии программных продуктов, которые распространяются бесплатно, обладают минимальными возможностями, например, только просмотр или воспроизведение. Понятно, что данные программы не смогут удовлетворить потребностям образовательного процесса по обеспечению мультимедийным контентом.

Версии программного обеспечения, которые позволяют осуществлять редактирование мультимедиа файлов (видеоредакторы, фоторедакторы, редакторы векторной графики), необходимо закупать. С одной стороны, количество необходимых экземпляров данного программного обеспечения расширенного функционала не столь многочисленно, поскольку пользователей, которым необходимы средства обработки мультимедиа, в институте не так уж и много. Однако, с другой стороны, возможности отечественных средств обработки мультимедиа существенно в настоящий момент уступают западным аналогам.

Отдельно необходимо остановиться на некоторых организационных проблемах перехода на отечественное офисное ПО.

МВД России в настоящий момент централизованно не определило, на какое отечественное офисное программное обеспечение необходимо осуществлять переход. Предложенные нами в статье варианты решения проблемы –

это видение сотрудников Бел ЮИ МВД России имени И.Д. Путилина. У сотрудников других образовательных организаций или территориальных органов могут возникнуть другие варианты решения проблемы, особенно в части выбора операционной системы и офисного пакета. В результате файлы, созданные в одной организации, могут не читаться программным обеспечением другой организации. Программное обеспечение может конфликтовать. Если же централизованное решение о конкретном офисном программном обеспечении, которое должно использоваться в подразделениях МВД России, будет принято позже, то это повлечет дополнительные затраты на закупку программного обеспечения и переобучение сотрудников и работников.

Вторым вопросом является дальнейшее использование программного обеспечения, применяемого для функционирования электронной информационно-образовательной среды (ЭИОС) и библиотечных систем, а также издательских пакетов программ. Указанное программное обеспечение не упомянуто в Распоряжении Правительства Российской Федерации от 26.07.2016 № 1588-р и Приказе МВД России. Кроме того, для создания ЭИОС и библиотечных систем использовалось программное обеспечение с открытым кодом, и его можно считать в нашей переработке отечественным ПО. Использование специальных программ, типа издательских систем, возможно будет осуществлять без замены операционной системы или офисного пакета, поскольку Приказ МВД России от 10.05.2018 № 284 предусматривает перевод не 100%, а 80% данных типов программ на отечественное ПО. По средствам мультимедиа данный процент составляет 70%, что также даст возможность лицам, создающим мультимедийный контент, продолжить использовать имеющееся программное обеспечение, которое невозможно или сложно заменить на современном этапе.

В целом можно констатировать, что переход на отечественное офисное программное обеспечение существенно повысит информационную безопасность деятельности российских государственных органов и даст значительный толчок к разработке отечественного ПО. При этом, некоторые трудности на данном пути представляются временными и преодолимыми.

Библиографический список

1. Распоряжение Правительства Российской Федерации от 26.07.2016 № 1588-р «Об утверждении плана перехода в 2016-2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения» // Собрание законодательства Российской Федерации. 2016. № 31. Ст. 5068.

2. Приказ МВД России от 10.05.2018 № 284 «Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года» // СПС «КонсультантПлюс».

3. Импортозамещение в ИТ. Электронный ресурс: Сайт газеты «Независимая правда» (дата публикации: 01.07.2018). – URL: http://www.ng.ru-/society/2018-07-01/100_import010718.html.

4. *Жукова П.Н., Прокопенко А.Н., Гуржий А.А.* Использование информационных технологий в системе ведомственного образования на современном этапе (на примере Бел ЮИ МВД России имени И.Д. Путилина) / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 4-й Международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2018. С. 3-11.

ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ, ПОСЯГАЮЩИЕ НА ЖИЗНЬ И ЗДОРОВЬЕ НЕСОВЕРШЕННОЛЕТНИХ

УДК 343.62

Нудель С.Л.,
доктор юридических наук, доцент
(Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации)

Аннотация: в научной статье автором проанализированы отдельные проблемы уголовной ответственности за преступления в информационной сфере, посягающие на жизнь и здоровье несовершеннолетних. В частности, рассмотрены вопросы криминализации склонения к совершению самоубийства или содействие совершению самоубийства (ст. 110.1 УК РФ), организации деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2 УК РФ) и вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2 УК РФ). Также в работе проанализирован ряд актуальных проблем квалификации указанных преступлений.

Ключевые слова: преступление, несовершеннолетние, самоубийство, информационная безопасность.

PROBLEMS OF CRIMINAL RESPONSIBILITY FOR CRIMES IN THE INFORMATION SPHERE, CHALLENGING TO LIFE AND HEALTH OF MINORMS

Nudel S.L.,
Doctor of Jurisprudence Sciences, Associate Professor
(Institute of Legislation and Comparative Law under the Government of the Russian Federation)

Abstract: in a scientific article, the author analyzed some problems of criminal responsibility for crimes in the information sphere that infringe on the life and health of minors. In particular, the issues of criminalization of the inclination to commit suicide or the promotion of suicide (Article 110.1 of the Criminal Code of the Russian Federation), the organization of activities aimed at encouraging the commission of suicide (Article 110.2 of the Criminal Code of the Russian Federation) and the involvement of a minor in actions that pose a danger to the life of a minor (article 151.2 of the Criminal Code of the Russian Federation). Also in the work a number of actual problems of qualification of these crimes was analyzed.

Key words: crime, minors, suicide, information security.

В Доктрине информационной безопасности Российской Федерации совершенно обоснованно отмечено, что «информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства» [1].

Вместе с тем необходимо отметить, что несмотря на то, что расширение областей использования информационных технологий – фактор развития экономики и повышения эффективности государственных и общественных институтов, синхронно рождаются и новые информационные угрозы. В частности, существующие объективные возможности трансграничного оборота информации применяются для достижения криминальных и иных противоправных целей.

При этом государство обязано обеспечить и информационную безопасность детей, то есть «защиту ребенка от дестабилизирующего воздействия информационной продукции, путем создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия» [2].

В качестве важнейшего элемента реализации государственной политики Российской Федерации в области информационной безопасности детей следует признать уголовно-правовой механизм, включающий, в первую очередь, нормы об уголовной ответственности за преступления в информационной сфере, посягающие на жизнь и здоровье несовершеннолетних.

Федеральным законом от 07.06.2017 № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессу-

ального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» [3] в Уголовный кодекс Российской Федерации (далее – УК РФ) включены ст.ст. 110.1 «Склонение к совершению самоубийства или содействие совершению самоубийства», 110.2 «Организация деятельности, направленной на побуждение к совершению самоубийства» и 151.2 «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего».

Разработка и принятие данного федерального закона были направлены на обеспечение безопасности жизни и здоровья несовершеннолетних посредством создания мер, способствующих предотвращению:

1) самоубийств среди детей и подростков и борьбы с различными формами содействия суицидам (в том числе широком распространении в сети Интернет негативной информации, побуждающей к совершению самоубийств или иной деструктивной деятельности);

2) «вовлечения несовершеннолетних в совершение противоправных действий, заведомо для виновного представляющих опасность для их жизни» [4].

1. В последние годы появились новые способы склонения к совершению самоубийства или содействия совершению самоубийства, оказывающие негативное влияние на сознание ребенка и мотивацию его поведения. При этом они ранее не прогнозировались наукой, «не были своевременно оценены криминологами и по факту приняли широкий масштаб, оказавшись вне уголовно-правовой оценки, а, значит, и вне мероприятий правоохранительных органов по выявлению организаторов такой деструктивной деятельности, своевременному пресечению их действий, а также защите потерпевших» [4].

Помимо этого и в Национальной стратегии действий в интересах детей на 2012-2017 годы отмечается, что «по распространенности суицидов среди подростков Россия занимает одно из ведущих мест в мире, уровень смертности детей значительно выше, чем в других европейских странах» [5][1].

Так, в статье 110.1 УК РФ установлена ответственность за «склонение к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом при отсутствии признаков доведения до самоубийства» (ч. 1) и за «содействие совершению самоубийства советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению или обещанием скрыть средства или орудия совершения самоубийства» (ч. 2).

Криминализация данных деяний обусловлена и тем фактом, что указанные деяния всегда влекут опасные последствия в отношении конкретных лиц, а также направлены на широкий круг лиц и вне зависимости от последствий имеют общественно опасный характер.

[1] По данным Следственного комитета Российской Федерации в 2016 году ушли из жизни в результате самоубийства 720 детей. За последние три года совершили суицид 2 205 детей.

Вместе с тем в правоприменительной практике возникают сложности, связанные с квалификацией данного преступления в связи с наличием в его конструкции значительного количества оценочных признаков.

Так, под *склонением к совершению самоубийства*, исходя из анализа разъяснений Верховного Суда Российской Федерации [6, 7], следует понимать любые умышленные действия, в том числе однократного характера, направленные на возбуждение у другого лица (группы лиц) желания самоубийства путем уговоров, предложений, подкупа, обмана или иным способом.

Необходимо согласиться с мнением, что «по своей сути склонение к самоубийству напоминает подстрекательство к совершению преступления. Однако поскольку самоубийство по уголовному закону не наказуемо, то и склонение к самоубийству не может считаться соучастием в самоубийстве путем подстрекательства» [8].

Как *содействие совершению самоубийства* в соответствии с диспозицией ч. 2 ст. 110.1 УК РФ следует определить умышленные действия (интеллектуальная или физическая помощь), связанные с предоставлением конкретному лицу (группе лиц) советов, указаний, сведений, средств или орудий совершения самоубийства; устранением препятствий к его совершению; обещанием скрыть средства или орудия совершения самоубийства.

Содействие совершению самоубийства также не может быть признано соучастием в преступлении в форме пособничества, так как самоубийство преступлением не является.

Следует отметить, что описанные деяния, совершенные в отношении несовершеннолетнего или в информационно-телекоммуникационных сетях (включая сеть Интернет) относятся к квалифицированному составу преступления (ч. 3 ст. 110.1 УК РФ).

При этом для признания преступления оконченным (для простого и квалифицированного составов) необходимо установить факт совершения описанных действий и не требуется факта совершения самоубийства или покушения на самоубийство.

В то же время для признания оконченным особо квалифицированного состава преступления (указанные деяния, повлекшие самоубийство или покушение на самоубийство несовершеннолетнего (ч. 5), повлекшие самоубийство двух или более лиц (ч. 6)) необходимо наступление определенных законом последствий.

В ч. 1 ст. 110.2 УК РФ устанавливается уголовная ответственность за «организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства».

В данном случае речь идет об установлении уголовной ответственности для так называемых «администраторов «групп смерти» и иных неформальных сообществ, деятельность которых связана с побуждением несовершеннолетних к совершению самоубийства. Анализ правоприменительной практики показывает, что, как правило, такими «администраторами» являются лица, хо-

рошо знающие подростковую психологию. Данная деятельность основывается на привлечении внимания подростков к указанным сообществам посредством ограниченного и ритуального характера вступления в них путем выполнения разработанного набора заданий («путь инициации») и, в конечном итоге, доводит подростка до самоубийства или попытки его совершения. О необходимости принятия мер по противодействию указанным деяниям свидетельствуют также официальные данные относительно выявления запрещенного суицидального контента в сети Интернет: с 2012 года органами Роспотребнадзора проведена экспертиза более 13 тыс. ссылок на страницы сайтов в сети «Интернет» с суицидальной тематикой, в 2016 г. выявлена 4 751 ссылка, содержащая запрещенные сведения о способах совершения самоубийства или призывы к их совершению [4].

Применительно к рассматриваемой статье УК РФ под *организацией деятельности, направленной на побуждение к совершению самоубийства*, следует понимать действия организационного характера, заключающиеся в распространении информации о способах совершения самоубийства или призывов к совершению самоубийства.

В данном случае также совершение противоправного деяния с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) относится к квалифицированному составу преступления (ч. 2 ст. 110.2 УК РФ).

Рассматриваемый состав преступления – формальный: для наступления уголовной ответственности достаточно осуществления действия, запрещенного законом.

2. В ч. 1 ст. 151.2 УК РФ установлена ответственность за «склонение или иное вовлечение несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, путем уговоров, предложений, обещаний, обмана, угроз или иным способом, совершенное лицом, достигшим восемнадцатилетнего возраста, при отсутствии признаков склонения к совершению самоубийства, вовлечения несовершеннолетнего в совершение преступления или в совершение антиобщественных действий».

Примером такой опасной деятельности являются случаи вовлечения лицами, достигшими восемнадцатилетнего возраста, подростков в «трейнсерфинг» (проезд на крыше поезда) или иные виды смертельно опасного «зацепинга», «руфинг» (незаконное проникновение на крыши высоких зданий). Также широкую распространенность приобрели «игры» «Беги или умри», в ходе которых детям предлагается перебежать дорогу максимально близко к движущемуся автомобилю. По данным МВД России в 2016 году получили травмы 253 подростка, из них 117 – со смертельным исходом. Следует обратить внимание, что описанные действия носят латентный характер и зачастую фиксируются как несчастный случай [4].

Под *склонением или иным вовлечением несовершеннолетнего в совершение противоправных действий*, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, следует понимать действия лица, дос-

тигшего восемнадцатилетнего возраста, направленные на возбуждение желания совершить преступление или антиобщественные действия. Действия взрослого лица могут выражаться в форме уговоров, предложений, обещаний, обмана, угроз или др. Обязательным признаком указанных деяний является отсутствие признаков склонения к совершению самоубийства (ст. 110.1 УК РФ), вовлечения несовершеннолетнего в совершение преступления или в совершение антиобщественных действий (ст.ст. 150-151 УК РФ) [9].

Следует отметить, что описанные деяния, совершенные в отношении двух или более несовершеннолетних или в информационно-телекоммуникационных сетях (включая сеть Интернет) относятся к квалифицированному составу преступления (ч. 2 ст. 110.1 УК РФ).

Таким образом, компьютеризация российского общества, увеличение числа несовершеннолетних пользователей международной компьютерной сети «Интернет» привели к необходимости совершенствования российского уголовного законодательства с целью обеспечения не только информационной безопасности детей, но и их жизни и здоровья.

Библиографический список

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

2. Распоряжение Правительства Российской Федерации от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей» // Собрание законодательства Российской Федерации. 2015. № 49. Ст. 7055.

3. Федеральный закон от 07.06.2017 № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» // Собрание законодательства Российской Федерации. 2017. № 24. Ст. 3489.

4. Пояснительная записка к проекту Федерального закона № 118634-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» // Текст документа приведен в соответствии с публикацией на сайте http://asozd.duma.gov.ru/.

5. Указ Президента Российской Федерации от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012-2017 годы» // Собрание законодательства Российской Федерации. 2012. № 23. Ст. 2994.

6. Постановление Пленума Верховного Суда Российской Федерации от 15.06.2006 № 14 (ред. от 16.05.2017) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильно-

действующими и ядовитыми веществами» // Бюллетень Верховного Суда Российской Федерации. 2006. № 8.

7. Постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 (ред. от 03.11.2016) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // Бюллетень Верховного Суда Российской Федерации. 2012. № 4.

8. Комментарий к Уголовному кодексу Российской Федерации: в 4-х т. (постатейный). Особенная часть. Разделы VII-VIII. Т. 2 / отв. ред. В.М. Лебедев. – Москва: Юрайт, 2017.

9. Постановление Пленума Верховного Суда Российской Федерации от 01.02.2011 № 1 (ред. от 29.11.2016) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних» // Бюллетень Верховного Суда Российской Федерации. 2011. № 4.

К ВОПРОСУ СОЗДАНИЯ ЕДИНОГО ОБРАЗОВАТЕЛЬНОГО ПРОСТРАНСТВА ОРГАНОВ ВНУТРЕННИХ ДЕЛ

УДК 37.013

Лемайкина С.В.,
Карпика А.Г.,
кандидат технических наук, доцент
(Ростовский юридический институт МВД России)

Аннотация: в статье проанализирован ход эволюции дистанционных образовательных технологий, рассмотрены подходы к их внедрению в образовательный процесс. Предложен подход к их комплексному внедрению в образовательный процесс образовательных организаций системы МВД России.

Ключевые слова: электронная информационно-образовательная среда, образовательное пространство, дистанционные образовательные технологии.

TO THE QUESTION OF CREATING A SINGLE EDUCATIONAL SPACE OF THE MINISTRY OF THE INTERIOR

Lemaykina S.V.,
Karpika A.G.,
Candidate of Technical Sciences, Associate Professor
(Rostov Law institute of Interior of Russian Federation)

Abstract: the article analyzes the evolution of distance educational technologies, examines approaches to their implementation in the educational process. An

approach to their integrated implementation in educational process of educational organizations of the Ministry of Internal Affairs of Russia is proposed.

Key words: electronic information and educational environment, educational space, distance educational technologies.

В настоящее время в Российской Федерации решается комплекс стратегических задач, направленных на развитие всех видов образования. Приоритетные направления государственной политики в этой области определяются нормами Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 07.03.2018) «Об образовании в Российской Федерации» [1], Указа Президента Российской Федерации от 07.05.2012 № 599 «О мерах по реализации государственной политики в области образования и науки» [2], Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года, утвержденной распоряжением Правительства Российской Федерации от 17.11.2008 № 1662-р [3].

В Прогнозе долгосрочного социально-экономического развития Российской Федерации на период до 2030 года [4], разработанном Министерством экономического развития Российской Федерации, предусмотрена необходимость формирования гибкой и диверсифицированной системы профессионального образования, отвечающей требованиям рынка труда и потребностям инновационной экономики как в части образовательных программ, так и в части условий и материально-технического оснащения процесса обучения.

Созданная к этому моменту перспективная система профессионального образования предполагает наличие типовой устойчивой инновационной модели деятельности вуза, предполагающей эффективное решение стоящих перед ним учебных, методических, научных и воспитательных задач. Степени свободы указанной модели должны допускать варьирование ее параметров в зависимости от содержания образовательных программ, целевой аудитории и условий, в которых реализуются эти программы.

Мировыми образовательными трендами в современном обществе являются: внедрение вариативных образовательных программ на основе индивидуализации образовательных траекторий с учетом личностных свойств, интересов и потребностей обучающегося, внедрение в профессиональную образовательную среду технологий проектного обучения, дистанционных образовательных технологий.

Основоположником одного из современных трендов – дистанционного обучения – считается Исаак Питман. В 1840 году для обучения стенографии на расстоянии он впервые использовал почту, при этом задания студентам и результаты их выполнения отправлялись и получались в письмах и посылках. Считается, что именно в этом году им был создан первый дистанционный образовательный курс.

Первый этап массового использования дистанционных образовательных технологий начался в 1850-е годы. Первым образовательным учреждением, внедрившим элементы дистанционных образовательных технологий, стал

Лондонский Университет в Великобритании. В нем впервые была предоставлена возможность студентам из других городов сдать квалификационные экзамены и получить диплом, при условии, что они учились в аккредитованных Лондонским Университетом высших учебных заведениях. Таким образом, студенты получили возможность получить высшее образование, обучаясь на расстоянии. В 1858 году образовательные услуги, предоставляемые указанным Университетом, охватили студентов из других стран. Считалось не принципиальным, какое образовательное заведение они посещали.

Подобный опыт получил распространение на всей территории Великобритании. Стало нормой открывать колледжи, осуществляющие обучение посредством почтовых сообщений, при этом программа обучения совпадала с программами университетов. Всего в течение XIX века новая технология охватила большинство развитых на тот момент государств: Великобританию, Германию, Францию, Соединенные Штаты Америки.

В начале XX века в 1910-1914 годах появились курсы дистанционного обучения в Австралии. Они были организованы Квинслендским университетом, при этом впервые дистанционные технологии были применены для обучения детей, которые проживали в районах, в которых школы отсутствовали. Дальнейшее развитие и внедрение в педагогическую практику рассматриваемых технологий можно условно разделить на ряд этапов.

Характерной чертой первого этапа было использование рукописных и машинописных учебных материалов. Это было связано в первую очередь с тем, что несмотря на то, что учебники уже издавались достаточно давно, их качество и количество не позволяли организовать полноценное обучение с их использованием.

На втором этапе (50-80-е годы прошлого века) качество полиграфии значительно улучшилось, книги получили цветные иллюстрации. В этот же период широкую популярность приобрели аудио-, фото- и киноматериалы. Также материалы дополнялись аудио- и видеозаписями. Параллельно проводились эксперименты по использованию в образовательных целях кино и телевидения.

Третий этап, начавшийся в конце 1980-х – начале 1990-х годов, характеризовался активным применением сервисов электронной почты, электронных рассылок, электронных конференций. Для подготовки образовательных материалов использовались текстовые редакторы, средства разработки иллюстративных материалов [5, с. 29].

В Российской Федерации активное использование технологий дистанционного обучения началось в конце 1990-х – начале 2000-х годов. Отставание в общей сложности на 10 лет было обусловлено технологическим отставанием в области внедрения информационных технологий в образовательный процесс и сложной экономической ситуацией, связанной с изменением политического строя и экономической модели страны.

Старт применению дистанционных образовательных технологий в России был дан в 1995 году постановлением Государственного Комитета Российской Федерации по высшему образованию от 31.05.1995 № 6. Этим докумен-

том была утверждена «Концепция единой системы дистанционного образования России». В 2002 г. в Закон Российской Федерации от 10.07.1992 № 3266-1 «Об образовании» были внесены соответствующие изменения.

Однако вопрос о законодательном закреплении необходимых положений все еще находился в повестке дня вследствие неоднозначного толкования понятия «дистанционное обучение».

В следующем 2003 г. Федеральным законом от 10.01.2003 № 11-ФЗ «О внесении изменений и дополнений в Закон Российской Федерации "Об образовании"» и Федеральным законом «О высшем и послевузовском профессиональном образовании» было закреплено следующее определение: дистанционные образовательные технологии – это образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Способы организации обучения посредством дистанционных образовательных технологий были зафиксированы в приказе Министерства образования России от 18.12.2002 № 4452 «Об утверждении Методики применения дистанционных образовательных технологий (дистанционного обучения) в образовательных учреждениях высшего, среднего и дополнительного профессионального образования Российской Федерации».

Развитию дистанционных электронных образовательных технологий способствовал взрывной рост интереса к ним как со стороны государственных структур, заинтересованных в подготовке новых кадров, переподготовке и повышении квалификации сотрудников, так и со стороны бизнеса, заинтересованного в обучении персонала с целью быстрого внедрения в передовых технологий в производство и управление.

На сегодняшний день в мире электронное образование используется повсеместно, при этом развитие аналогичного рынка в России, по некоторым оценкам [6], отстает на 5-7 лет, что несколько лучше той ситуации, которая имела место в начале 2000-х годов. Неформальная периодизация становления электронного обучения в Российской Федерации может быть представлена на сегодняшний день следующими периодами:

Первый (1990-1999 гг.) характеризуется развитием электронных образовательных технологий как элементом заочного обучения. В этот период в качестве средства организации участников образовательного процесса активно используется электронная почта. Учитывая неразвитость системы широкополосного доступа к сети Интернет, для распространения образовательных материалов, содержащих файлы значительного по меркам того времени объема, применяется технология, базирующаяся на протоколе FTP.

Второй (2000-2009 гг.) – отмечен активизацией рынка корпоративного обучения на основе развития услуг бизнес-образования. Период не случайно совпал с повышением качества и значительным снижением стоимости аренды высокоскоростных каналов доступа в Интернет, развитием мобильных техно-

логий и технологии Веб2.0. Обучающиеся, работодатели и педагогические работники получили возможность равного, интерактивного взаимодействия.

В этот период появились первые электронные системы управления обучением, позволяющие образовательным организациям разрабатывать и поддерживать собственные электронные образовательные ресурсы, что также существенно снизило их стоимость и способствовало их более широкому внедрению в педагогическую практику.

Третий (с 2010 года) – характеризуется окончанием формирования рынка электронного образования как самостоятельной области, повсеместным проникновением образовательных технологий во все сферы человеческой деятельности.

В настоящее время поддержка развития дистанционного обучения в Российской Федерации является одним из приоритетных направлений государственной политики. С 2014 года в Российской Федерации реализуется государственная программа «Развитие образования» (2013-2020 гг.), утвержденная постановлением Правительства Российской Федерации от 15.04.2014 № 295 «Об утверждении государственной программы Российской Федерации "Развитие образования на 2013-2020 годы"».

Заявленная основная цель реализации программы – повышение образовательных результатов обучающихся за счет эффективного встраивания электронных ресурсов в образовательный процесс с целью его качественного изменения. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (ред. от 07.03.2018) содержит ст. 16, посвященную общим требованиям к организации образовательного процесса, где определены общие для Российской Федерации правовые нормы в области реализации образовательных программ с применением дистанционных образовательных технологий.

Для органов внутренних дел вопрос создания единой электронной информационно-образовательной среды, несомненно, является актуальным, поскольку его решение позволяет создать в образовательных организациях системы МВД России единое образовательное пространство. Платформой, на базе которой оно в принципе может быть развернуто, может стать интегрированная мультисервисная телекоммуникационная сеть МВД России.

Как отмечают исследователи [7, с. 194], задача объединения разнородных информационных ресурсов в единую систему, безусловно, относится к сложным организационно-техническим задачам и требует затрат времени, интеллектуального труда и материальных ресурсов.

Коллекции учебно-методических материалов, базы данных и программное обеспечение поддержки образовательного процесса, накопленные образовательными и научными организациями системы МВД России, для их интеграции в перспективное образовательное пространство требуют реструктуризации и унификации с точки зрения программно-аппаратной совместимости.

Стандартизация и унификация информационных ресурсов образовательных организаций системы МВД России является первоочередным и, безусловно, необходимым этапом их интеграции.

Решение этой перспективной задачи, безусловно, требует ее периодизации и декомпозиции на отдельные этапы. С учетом существующей структуры образовательных организаций может быть предложен следующий вариант периодизации.

На первом этапе устанавливается стандарт электронной информационно-образовательной среды образовательной организации в рамках единого образовательного пространства МВД России, ранее созданные среды приводятся в соответствие с ним.

На втором этапе разворачиваются стандартизированные электронные информационно-образовательные среды всех образовательных организаций системы МВД России, участвующие в функционировании образовательного пространства.

На третьем этапе проводится опытная эксплуатация каждого компонента, корректируются решения, осуществляются необходимые доработки. Цель данного этапа – обеспечение полной совместимости электронных информационно-образовательных сред в рамках образовательного пространства.

На четвертом этапе происходит выход на опытную эксплуатацию в масштабе региона. На этом этапе координирующими центрами могут стать университеты и академии МВД России.

Пятый этап – подготовка к штатной эксплуатации и внедрение единого образовательного пространства в педагогическую практику.

Ожидаемый эффект от подобной системы – повышение эффективности системы образования МВД России за счет интеграции электронных информационно-образовательных сред в единое образовательное пространство, что позволит реализовать единый подход к подготовке, переподготовке и повышению квалификации сотрудников МВД России.

Библиографический список

1.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=240687810053551927796041 01&cacheid=A45109620EF68A6835778753C180E36E&mode=splus&base=LAW&n=292679&rnd=80AE5B4822069E84F9138DFB2C544637#08746970371470024

2.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=824068781005355192779604101&cacheid=3BF954FEEBF336CAA969EFE6A7F5225C&mode=splus&base=LAW&n=129346&rnd=80AE5B4822069E84F9138DFB2C544637#07841344293328985.

3.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=824068781005355192779604101&cacheid=6E256F82745C3BDEB2B6BCA3B2FDF257&mode=splus&base=LAW&n=212832&dst=100007&rnd=80AE5B4822069E84F9138DFB2C544637#05525570373241211

4.URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=824068781005355192779604101&cacheid=6FFC890D22585A761B60AA078D437F74&mode=splus&base=LAW&n=144190&rnd=80AE5B4822069E84F9138DFB2C544637#035211763511114214

5 . *Маслакова Е.С.* История развития дистанционного обучения в России / Теория и практика образования в современном мире: материалы VIII Международной научной конференции (г. Санкт-Петербург, декабрь 2015 г.). – Санкт-Петербург, 2015.

6. URL:http://www.logrusit.com/ru/glavnaya/articles/razvitie-elearning-v-rossii/.

7. *Лемайкина С.В., Арбузов П.В., Карпика А.Г.* Электронная информационно-образовательная среда как форма реализации дистанционных технологий образовательных организаций системы МВД России / Подготовка кадров для силовых структур: современные направления и образовательные технологии: сборник материалов двадцать второй всероссийской научно-методической конференции: в 2-х ч. – Иркутск, 2017.

МИРОВОЗЗРЕНЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ У ОБУЧАЮЩИХСЯ В ВУЗЕ

УДК 37.03

Исаева К.В.
(Воронежский институт ФСИН России);
Ласточкина О.А.
(Московский университет МВД России им. В.Я. Кикотя);
Остапенко В.С.,
доктор педагогических наук, профессор
(Центральный филиал Российского государственного университета правосудия);
Амир Абдулхуссейн Хашим,
аспирант
(Воронежский государственный технический университет)

Аннотация: в статье рассматривается актуальная проблема мировоззренческих аспектов формирования информационной культуры у обучающихся, играющей важную роль в повышении эффективности и качества образовательного процесса вуза.

Ключевые слова: информационная культура, мировоззренческие аспекты, процесс формирования, обучающиеся в вузе.

PHILOSOPHICAL ASPECTS OF FORMATION OF INFORMATION CULTURE AMONG STUDENTS AT THE UNIVERSITY

Isaeva K.V.
(Voronezh Institute of the FPS of Russia);
Lastochkina O.A.
(Kikot Moscow University of the Ministry of the Internal Affairs of the Russian);
Ostapenko V.S.,
Doctor of Pedagogical Sciences, Professor
(Central branch of the Russian state University of justice);
Amir Abdulhussein Hashim,
Post-graduate Student
(Voronezh State Technical University)

Abstract: the article deals with the actual problem of ideological aspects of the formation of information culture in students, which plays an important role in improving the efficiency and quality of the educational process of the University.

Key words: information culture, ideological aspects, the process of formation, studying at the University.

Информационная культура – историческое понятие. Как часть общей культуры она появилась тогда, когда человек стал обмениваться смысловой информацией. Само понятие «информационная культура» характеризует одну из граней культуры, связанную с информационным аспектом жизни людей. В Федеральном законе от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» (ст. 8) подчеркивается, что «граждане и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами» [7]. Информация всегда имеет мировоззренческое значение и в этом аспекте играет большую роль в формировании личности в образовательном процессе вузов [4].

Существует множество определений понятия «информационная культура», которые рассматривают Е.А. Евтюхина, Т.А. Кудрина, Н.Б. Зиновьева, Ю.С. Зубов, В.А. Минкина и другие, исходя из цели своих исследований и сферы научных интересов. Так, В.А. Минкина полагает, что «становление информационной культуры человека осуществляется в его повседневной деятельности под влиянием усвоенных бытовых знаний и умений, информации средств массовых коммуникаций, в ходе самообразования, при обучении в семье и на работе» [5, с. 82]. По определению одного из ведущих специалистов в области информатизации Э.П. Семенюка, информационная культура – это «информационная компонента человеческой культуры в целом, объективно характеризующая уровень всех существующих в обществе информационных процессов и существующих информационных отношений» [8, с. 2].

В широком понимании информационная культура личности – это одна из составляющих общей культуры человека, формирующая информационное мировоззрение и обеспечивающая удовлетворение информационных потребностей личности и общества с использованием как традиционных, так и новых информационных коммуникационных технологий. Одним из основных факторов повышения эффективности системы образования является развитие информационной культуры в образовательных организациях, которая определяет уровень интеллектуального развития обучающихся, их материальные и духовные потребности. В процессе формирования информационной культуры обучающихся решается социально-педагогическая задача, состоящая в том, чтобы подготовить будущих специалистов к самостоятельной практической деятельности, в которой они способны реализовывать индивидуальные творческие способности, применять на практике полученные знания, умения и навыки, а также продолжать свое образование. *Информационная культура современности в вузах характеризуется сложностью, разнообразием. Это определяется близостью расположения вузов к информационным центрам, доступностью интернет-ресурсов для большинства пользователей: студентов и педагогов, замещением реальных научных мероприятий виртуальными (научно-методические и научно-практические конференции и т.п.), увеличением количества студентов, обучающихся посредством дистанционного образования и т.п.*

В связи с этим следует указать базовые принципы развития информационного общества, провозглашенные ЮНЕСКО, которые напрямую связаны с формированием информационной культуры личности: всеобщий доступ к информации и на этой основе равный доступ к качественному образованию; уважение культурного многообразия и свобода выражения мнений в информационном пространстве.

Информатизация образования должна опережать информатизацию других сфер общественной жизни, так как в образовательных организациях закладываются социальные, психологические, общекультурные, а также профессиональные предпосылки информатизации всего общества. Осуществлять эффективную информационную деятельность в современном обществе способен человек, обладающий широким мировоззренческим кругозором, эрудицией, и прежде всего информационной культурой. Наиболее эффективное формирование информационной культуры человека в современном обществе возможно через систему образования. Согласно Н.И. Гендиной, под информационной культурой понимается совокупность информационного мировоззрения и системы знаний и умений, получаемых в образовательных организациях и обеспечивающих целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных информационных потребностей [2].

Информационно-культурное пространство вуза формируется в первую очередь людьми (преподавателями, студентами и др.), которые являются носителями определенной культуры. В своей повседневной жизни люди привыкли пользоваться разными источниками получения информации (телевизор, радио, газета, книга, Интернет и др.). В педагогической практике данные ис-

точники информация используются по необходимости в учебной и научно-исследовательской деятельности. Расположенные в интернет-ресурсе образовательные сайты, порталы позволяют работать с большими объемами информации, что помогает выводить студентов на качественно иной, новый уровень анализа и обработки получаемой ими информации. Поэтому, следует выделить особую роль медиаобразования в учебно-воспитательном процессе вуза с целью формирования информационной культуры обучающихся. В социокультурной сфере информация предполагает получение людьми знаний и понимание значения информации в будущем. Инновационные технологии повышают информированность обучаемых в несколько раз, кардинально меняя объем и глубину знаний и культурный уровень в целом.

Таким образом, информационную культуру мы будем рассматривать как определенный уровень организации информационных процессов, как удовлетворенность в информационном общении и степень эффективности создания, сбора, хранения, переработки, передачи и использования информации, обеспечивающей целостное восприятие мира, анализ и оценку последствий принимаемых решений. В информационном пространстве вуза обучающийся выступает одновременно в качестве создателя, приемника, хранителя и передатчика информации. Реализация идеи информационной культуры направлена на преодоление основного противоречия современной системы образования: между стремительными темпами роста знаний в современном мире благодаря развитию информационных технологий и ограниченными возможностями их усвоения обучаемыми в таком объеме в вузах. Данное противоречие заставляет образовательные организации формировать у студентов умение к самостоятельному обучению, поиску информации, ее переработке, трансформации в профессиональные умения и навыки. Опираясь на тесную взаимосвязь информационной культуры и профессиональной деятельности, а также на теорию формирования творческих умений в процессе профессионального обучения, выделим три уровня информационной культуры обучающихся: общий (базовый), профессиональный, высший (логический).

Общий (базовый) уровень информационной культуры студента характеризуется таким набором знаний, умений и навыков, который применим почти неизменно в различных видах деятельности, то есть имеет обобщенный характер. Профессиональный уровень информационной культуры личности характеризуется специфичностью знаний, умений и навыков, большей сложностью, но и вместе с тем ограниченностью области применения. На этом уровне они будут привязаны к профессиональной деятельности личности, а при обучении в вузе – к дисциплинам, формирующим ее основы. Многие показатели профессионального уровня включают в себя и показатели общего (базового) уровня. Поэтому у нас есть основание считать профессиональный уровень информационной культуры выше общего (базового). В высшем (логическом) уровне информационной культуры обучаемого знания, умения и навыки также имеют межпредметный характер и отличаются от базовых степенью сложности, обусловлены творческим мышлением, креативностью, гибкостью, воз-

можностью осуществления анализа и синтеза, комбинирования ранее усвоенных знаний, умений и навыков, принятием решений в нестандартных ситуациях, ведением альтернативного поиска средств и способов решения поставленных задач. Знания, умения и навыки высшего уровня включают в себя аналогичные компоненты профессионального уровня информационной культуры. Данный уровневый подход, способствующий трансформации знаний в информацию и обратно, соответствует современным потребностям информатизации общества и может стать необходимым условием развития мировоззрения личности в информационном обществе.

Ю.С. Зубов пишет о тесной взаимосвязи информационной культуры и информационного мировоззрения и полагает, что важной частью, а по сути дела, ядром будущего информационного общества станет его образовательная система, которая и будет формировать информационное мировоззрение [3, с. 6].

К современным средствам информационной культуры относятся средства, обеспечивающие доступ к большим объемам информации, знаниям (компьютерная техника, мультимедийные технологии, сотовая связь). Однако применение в образовательной среде данных средств способно лишь создать условия для формирования информационной культуры в вузе. Продукты информационной культуры осваиваются студентами, педагогами и при этом своеобразная информационная аккультурация происходит уже при поступлении абитуриентов в вуз, однако это происходит при условии уделения большого количества времени на освоение информационных технологий, коммуникативному взаимодействию друг с другом и с педагогом. Так, например, по мере развития Интернета обостряется парадокс – вероятность существования нужной информации возрастает, а возможность ее нахождения уменьшается. Во многих случаях трудно или невозможно сформулировать ключевые слова, но если тематика точно известна, наиболее подходящим инструментом поиска оказываются каталоги (предметные указатели). Поэтому педагог не только должен сам владеть особыми информационными знаниями и умениями, но и быть профессионально готов транслировать их студентам, формируя у них основные компоненты информационной культуры – знания, навыки и умения потребления учебной информации. Таким образом, организация информационного образования и повышение информационной культуры обучающихся представляет задачу первостепенной важности, а сами педагоги становятся ключевыми фигурами, от которых зависит возможность реального повышения уровня рассматриваемого феномена у обучающихся в вузе [1].

Эффективность процесса формирования информационной культуры обучающихся в вузе обуславливается реализацией таких ведущих дидактических принципов, как научность, связь теории с практикой, систематичность, последовательность, наглядность, доступность, дифференцированный подход.

Являясь важнейшим фактором предстоящей успешной профессиональной деятельности, информационная культура обучающегося в вузе проявляется:

- в интересе обучаемых к информационным технологиям в учебном процессе;

- в осознании значения информации в вузах в образовательных целях;
- в осознанном выборе источников информации и владении алгоритмами их переработки по изучаемым предметам;
- в комплексном использовании традиционных, электронных, сетевых информационных ресурсов;
- в осознании себя как потребителя, носителя и распространителя информации, в активном информационном поведении.

Достижение цели формирования информационной культуры обучаемых осуществляется в ходе решения следующих образовательных задач в вузе:

- освоение рациональных приемов и способов самостоятельного ведения поиска информации в соответствии с возникающими в ходе обучения задачами;
- овладение методами формализованного свертывания (аналитико-синтетической переработки) информации;
- изучение и практическое использование информационных технологий при оформлении результатов самостоятельной учебной и научно-исследовательской работы (подготовка научных статей, рефератов, докладов и т.п.).

Выделим основные направления, по которым реализуется процесс формирования информационной культуры у обучающихся в вузе:

- опережающее развитие информационной насыщенности образовательного процесса;
- знание и понимание информационно-поисковых задач и алгоритмов их решения в процессе обучения;
- внедрение новых медиатехнологий во все сферы вуза с целью повышения эффективности работы по формированию информационной культуры обучающихся [6].

Анализируя вышесказанное, рассматривая информационную культуру личности как часть общечеловеческой культуры, сделаем вывод, что она является необходимым звеном образовательной деятельности педагогов и обучающихся, качественной характеристикой их информационной грамотности. Информационная культура проявляется в заинтересованности личности к информационной деятельности, в осознании ее важной роли в образовательном процессе вузов, в осознанном выборе источников информации и владении алгоритмами их переработки, в комплексном использовании традиционных, электронных, сетевых и других информационных ресурсов, в осознании себя как личности, как потребителя и распространителя информации.

Библиографический список

1. *Безруков А.А., Безрукова Н.П.* Формирование информационной культуры студентов естественнонаучных факультетов педагогического вуза // Информатика и образование. 2004. № 2. С. 86-94.

2. *Гендина Н.И., Стародубова Г.А., Уленко Ю.В.* Формирование информационной культуры личности: теоретическое обоснование и моделирование

содержания учебной дисциплины. – Москва: Межрегиональный центр библиотечного сотрудничества, 2006. – 512 с.

3. *Зубов Ю.С.* Новое знание о проблеме взаимосвязи информационной культуры и информационного мировоззрения / Проблемы информационной культуры: сборник статей. – Москва, 1996. С. 6-13.

4. *Исаева К.В., Остапенко В.С.* Основные методологические подходы к формированию мировоззрения обучаемого в вузе // Вестник Воронеж. гос. техн. ун-та. 2014. Т. 10. № 32. С. 31-34.

5. *Минкина В.А.* Информационная культура и способность к рефлексии // Высшее образование в России. 1995. № 4. С. 82-92.

6. *Мухина Н.Н.* Информационная культура студента: учебное пособие для студентов высших учебных заведений. – 2-е изд., перераб. и доп. – Казань, 2017. – 234 с.

7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31.

8. *Семенюк Э.П.* Информационная культура общества и прогресс информатики // НТИ. Сер. 1. 1994. № 1. С. 2-14.

О РАЗРАБОТКЕ КОМПЬЮТЕРНЫХ ПРОГРАММ ДЛЯ АВТОМАТИЗАЦИИ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО РАЗДЕЛУ «ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА» ДИСЦИПЛИНЫ МАТЕМАТИКА

УДК 519.688

Михайленко Е.В.,
кандидат физико-математических наук, доцент
(Краснодарский университет МВД России)

Аннотация: в статье представляется созданный автором комплекс программ для выполнения практических заданий по разделу «Теория вероятностей и математическая статистика» дисциплины прикладная математика. Автор раскрывает предпосылки, описывает основные методы и технологии, применяемые при разработке комплекса программ. Описываемые приложения иллюстрируются рисунками.

Ключевые слова: VBA, автоматизация, комбинаторика, математическая статистика, программный модуль, случайная величина, теория вероятностей, учебный процесс.

ON THE DEVELOPMENT OF SOFTWARE APPLICATIONS FOR THE IMPLEMENTATION OF PRACTICAL ASSIGNMENTS IN THE SECTION «METHODS OF OPTIMIZATION» DISCIPLINE APPLIED MATHEMATICS

Mikhaylenko E.V.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Krasnodar University of Ministry of the Interior of Russia)

Abstract: the article presents a set of programs created by the author for performing practical tasks in the section «Probability theory and mathematical statistics» of the applied mathematics discipline. The author reveals the prerequisites, describes the basic methods and technologies used in the development of a complex of programs. The applications described are illustrated by figures.

Key words: VBA, automation, combinatorics, mathematical statistics, program module, random variable, probability theory, educational process.

При подготовке специалистов органов внутренних дел информационно-технических и экономических направлений для формирования общекультурных, общепрофессиональных, профессиональных и профессионально-специализированных компетенций большое значение уделяется изучению различных математических дисциплин. Особенность изучения этих дисциплин состоит в усвоении курсантами и слушателями теоретического материала, получаемого на лекциях, а также в приобретении устойчивых навыков решения типовых задач по каждой из изученных тем.

В работах [5, 6, 8, 12, 13, 14, 15, 16, 19] уже были подняты вопросы оптимизации образовательного процесса с использованием информационных технологий. В них был описан процесс подготовки тестовых заданий [5, 6, 14], представлены некоторые методы и приемы реализации обучающих и контролирующих программных приложений в среде Visual Basic for Application [12, 15], рассмотрены технологии использования шрифтов [16], графических форм и объектов [13, 19], приведено обоснование выбора среды VBA [8].

Настоящая статья посвящена особенностям использования некоторых методических приемов и технологий при разработке компьютерных программ для подготовки практических заданий и анализа их выполнения обучаемыми по дисциплине математика, изучаемой на первом и втором курсах курсантами Краснодарского университета МВД России, обучающихся по специальностям 10.05.05 Безопасность информационных технологий в правоохранительной сфере, 38.05.01 Экономическая безопасность.

Рассмотрим пример разработки на кафедре информатики и математики Краснодарского университета МВД России программного обеспечения для проведения практических занятий и самостоятельной работы по разделу «Теория вероятностей и математическая статистика».

Суть проекта заключается в генерации числовых и символьных значений для подобранных преподавателем типовых задач. Специально подготовленный документ с незаполненным шаблоном заданий и ответов помещается в виртуальный учебно-методический кабинет кафедры информатики и математики, размещенный на сервере компьютерного центра университета [8]. Кроме того, задания распространяются преподавателями с использованием облачных технологий, и доступ к заданиям на самостоятельную подготовку открыт через Интернет для всех обучаемых круглосуточно. В этом случае преподаватель создает виртуальную интерактивную группу, к ней подключаются все курсанты, которые в последствии могут использовать выложенные преподавателем актуальные учебные ресурсы: мультимедийные слайды, тексты лекций, индивидуальные задания на самостоятельную подготовку, примеры решения задач, справочные материалы [16].

Представляемый Комплекс программ обеспечивает практические работы и самостоятельную подготовку по темам: «Комбинаторика», «Основы понятия теории вероятности», «Схемы повторных испытаний», «Случайные величины» и «Элементы математической статистики» и состоит из 14 программных модулей:

1. Конфигурации без повторений.
2. Конфигурации с повторениями.
3. Комбинаторные уравнения.
4. Классическое определение вероятностей.
5. Вероятность суммы и произведения событий.
6. Формула полной вероятности формула Байеса.
7. Комплексное задание по теории вероятностей.
8. Схемы повторных испытаний. Формулы Бернулли и Пуассона.
9. Локальная и интегральная формулы Муавра-Лапласа.
10. Числовые характеристики случайных величин.
11. Законы распределения дискретных случайных величин.
12. Числовые характеристики непрерывных случайных величин.
13. Элементы математической статистики.
14. Статистические исследования выборки.

Тема «Комбинаторика» представлена тремя программными модулями, соответствующими двум практическим занятиям и самостоятельной подготовке курсантов. Модуль «Конфигурации без повторений» (см. рис. 1) предназначен для решения курсантами стандартных задач с использованием теорем сложения и умножения, а также формул расчета количества перестановок, сочетаний и размещений без повторений [9]. Представленные задачи нарастающей сложности и формируют у курсантов умение производить трудоемкие расчеты с факториалами.

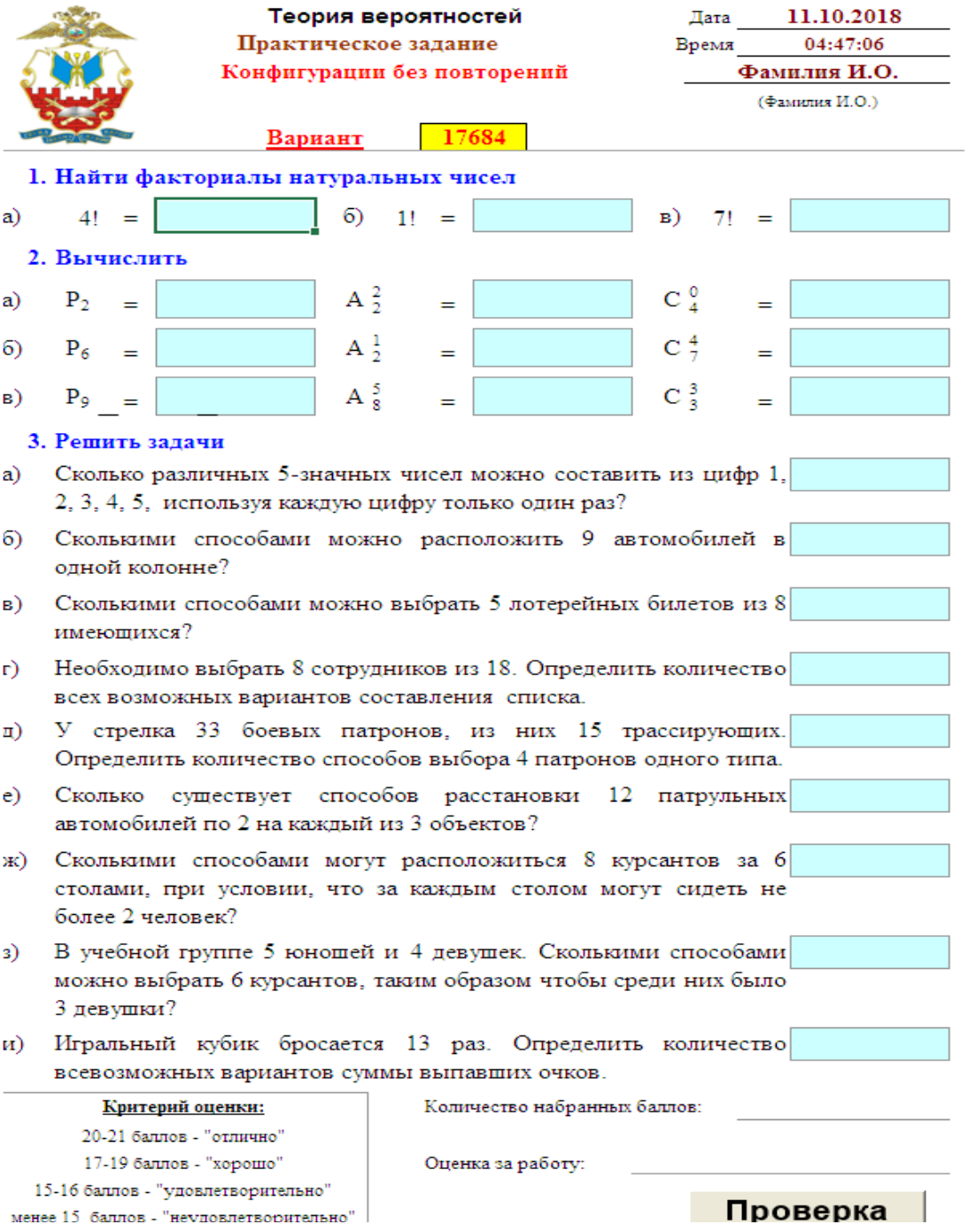


Рисунок 1.
Модуль «Конфигурации без повторений»

Модуль «Конфигурации с повторениями» (см. рис. 2) посвящен решению курсантами задач с использованием формул расчета количества перестановок, сочетаний и размещений с повторениями [7]. Кроме того, в заданиях предлагается найти количество разбиений некоторых множеств на упорядоченные группы. Задачи здесь также представлены в аналитической и текстуальной форме. Логика некоторых задач достаточно сложна и требует поэтапного выполнения нескольких действий.

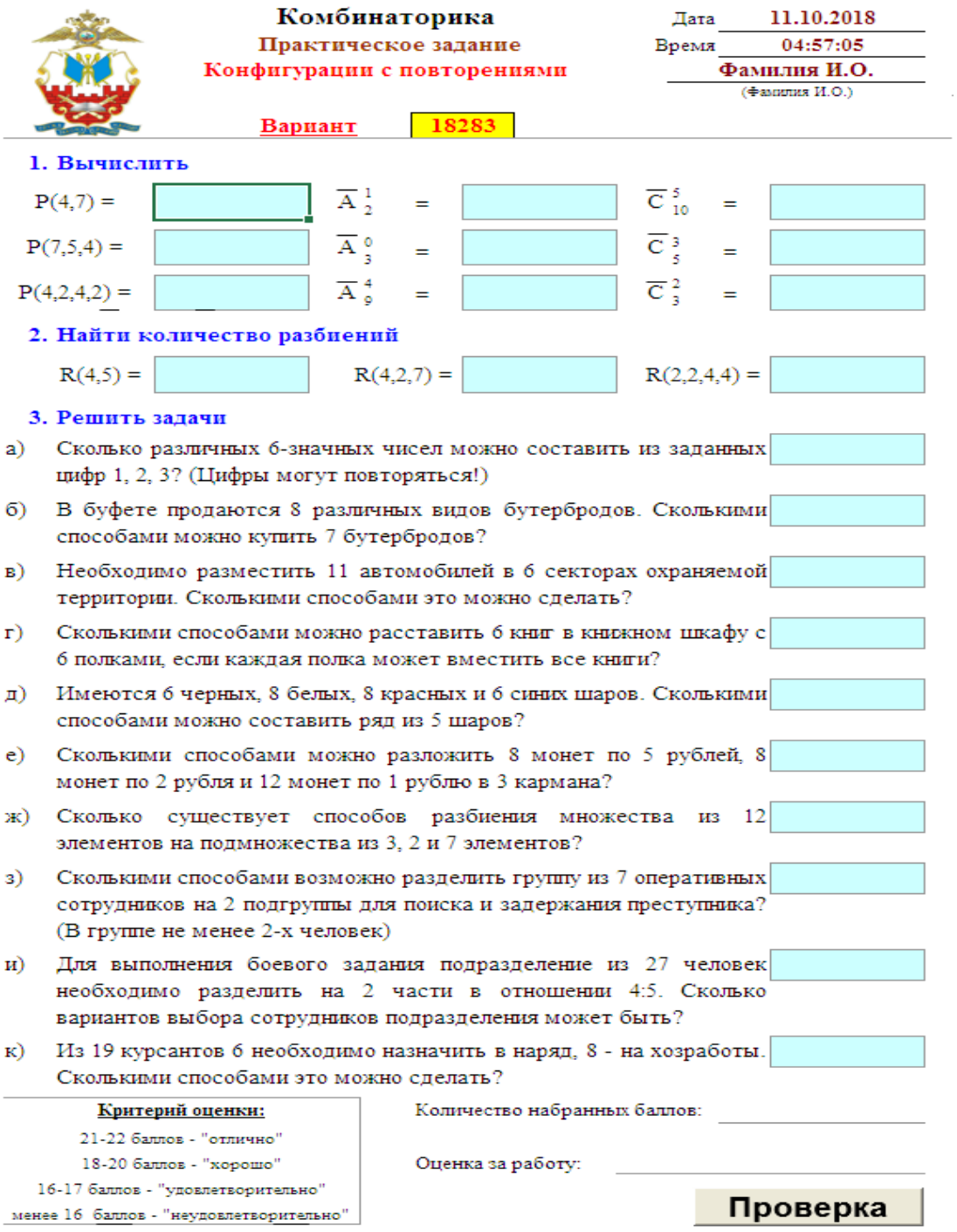


Рисунок 2.
Модуль «Конфигурации с повторениями»

В работе с модулем «Комбинаторные уравнения» (см. рис. 3) курсанты решают уравнения, в которых присутствуют изученные формулы перестановок, сочетаний и размещений с повторениями и без повторений. Решение комбинаторных уравнений связано со сложным процессом расчетов представления величин, большим количеством сокращений в дробях. Также здесь представлены задачи на вычисления коэффициентов разложения степеней двучленов с помощью формулы бинома Ньютона и треугольника Паскаля [10].

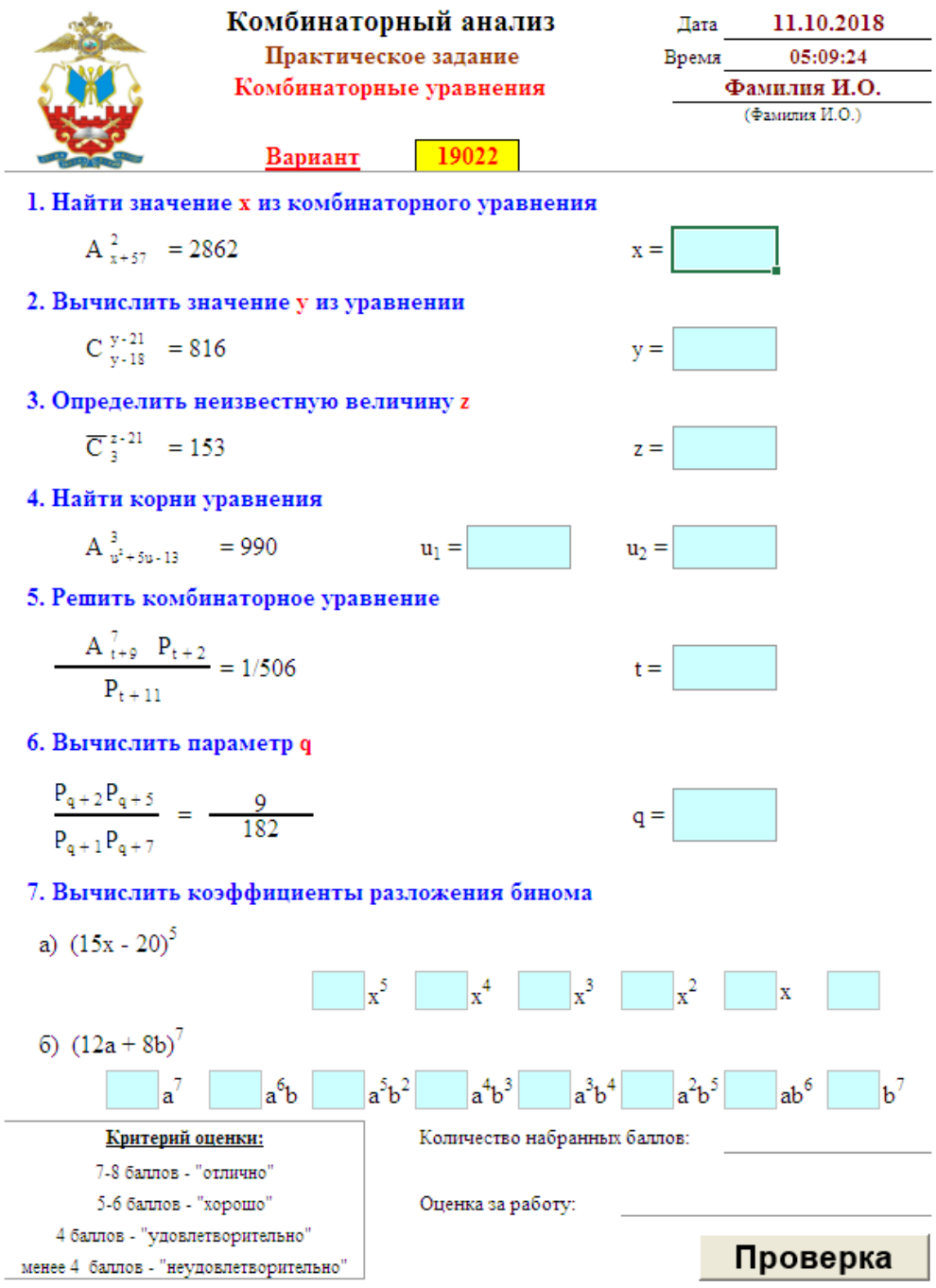


Рисунок 3.
Модуль «Комбинаторные уравнения»

Тема «Основные понятия теории вероятности» представлена четырьмя программными модулями, которые используются на трех практических занятиях и самостоятельной подготовке курсантов. В модуле «Классическое определение вероятностей» (см. рис. 4) обучаемые решают задачи с использованием формул классической вероятности. Здесь используются понятия элементарных событий, противоположного события, свойства вероятности [11]. Кроме того, для расчета количества исходов курсантам необходимо использовать ранее изученные формулы комбинаторики.

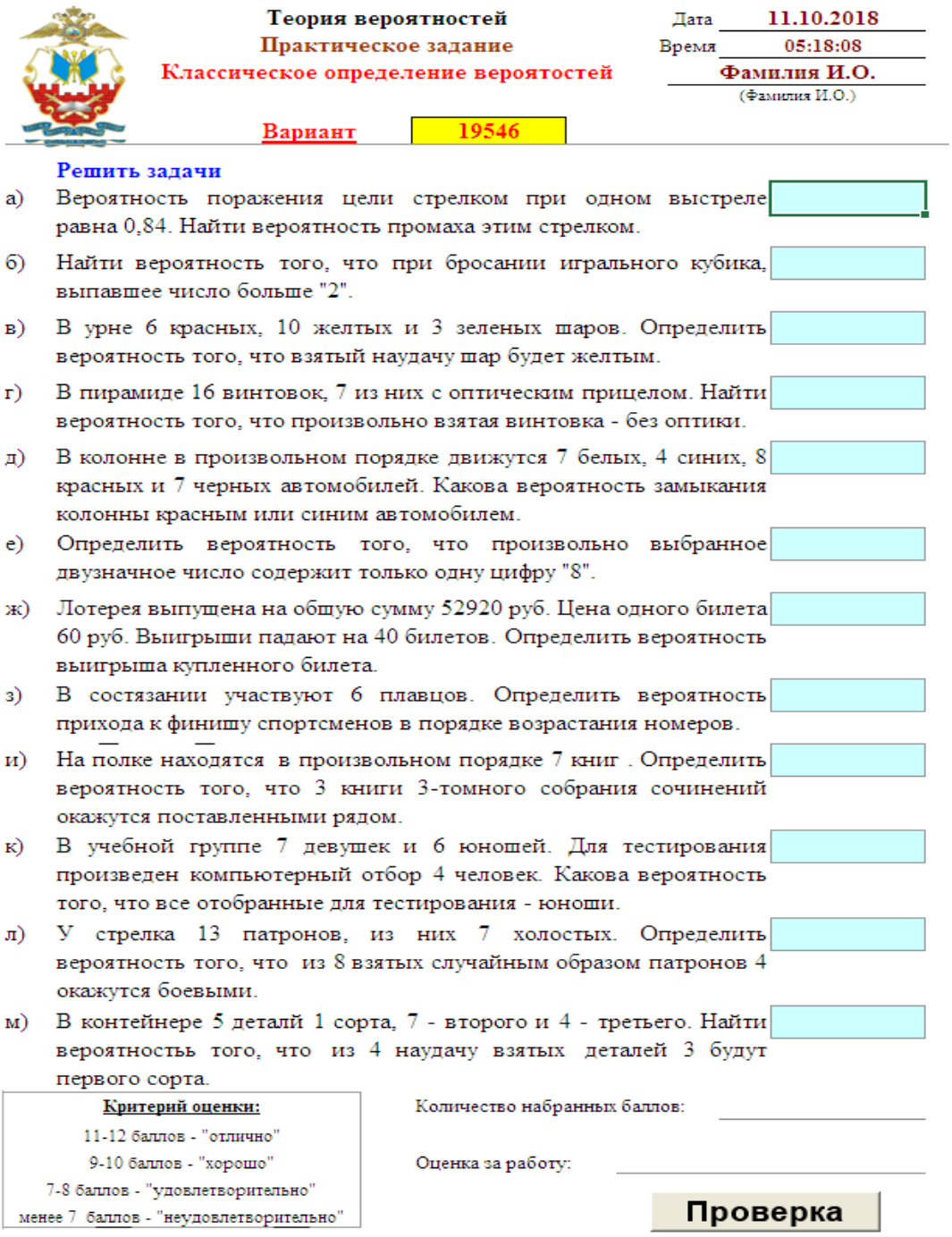


Рисунок 4.
Модуль «Классическое определение вероятностей»

Достаточно трудоемким для выполнения является модуль «Вероятность суммы и произведения событий» (см. рис. 5). Эта группа задач по теории вероятности является логически сложной. Прежде чем решить задачу, обучаемый должен определить описываемые события, выяснить, являются ли эти события совместными или несовместными, зависимыми или независимыми, выбрать соответствующие формулы условной вероятности суммы или произведения событий для решения [2].

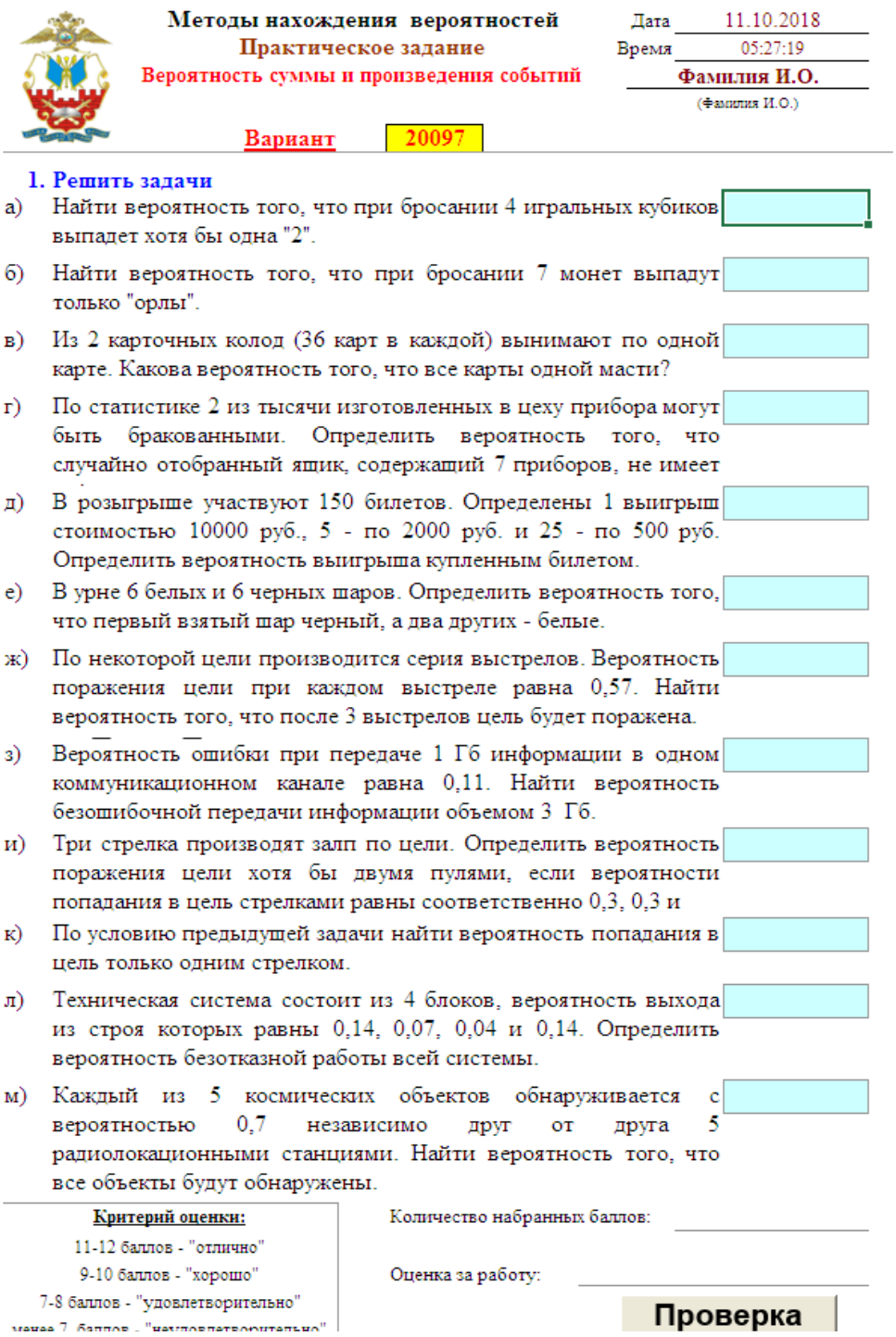


Рисунок 5.
Модуль «Вероятность суммы и произведения событий»

Модуль «Формула полной вероятности и формула Байеса» (см. рис. 6) содержит 5 задач, в которых события образуют полную группу, и решение которых предполагает использование формулы полной вероятности. Следствием теоремы умножения и формулы полной вероятности является формула гипотез Байеса [3]. Для изучения этой формулы представлены 3 задачи.

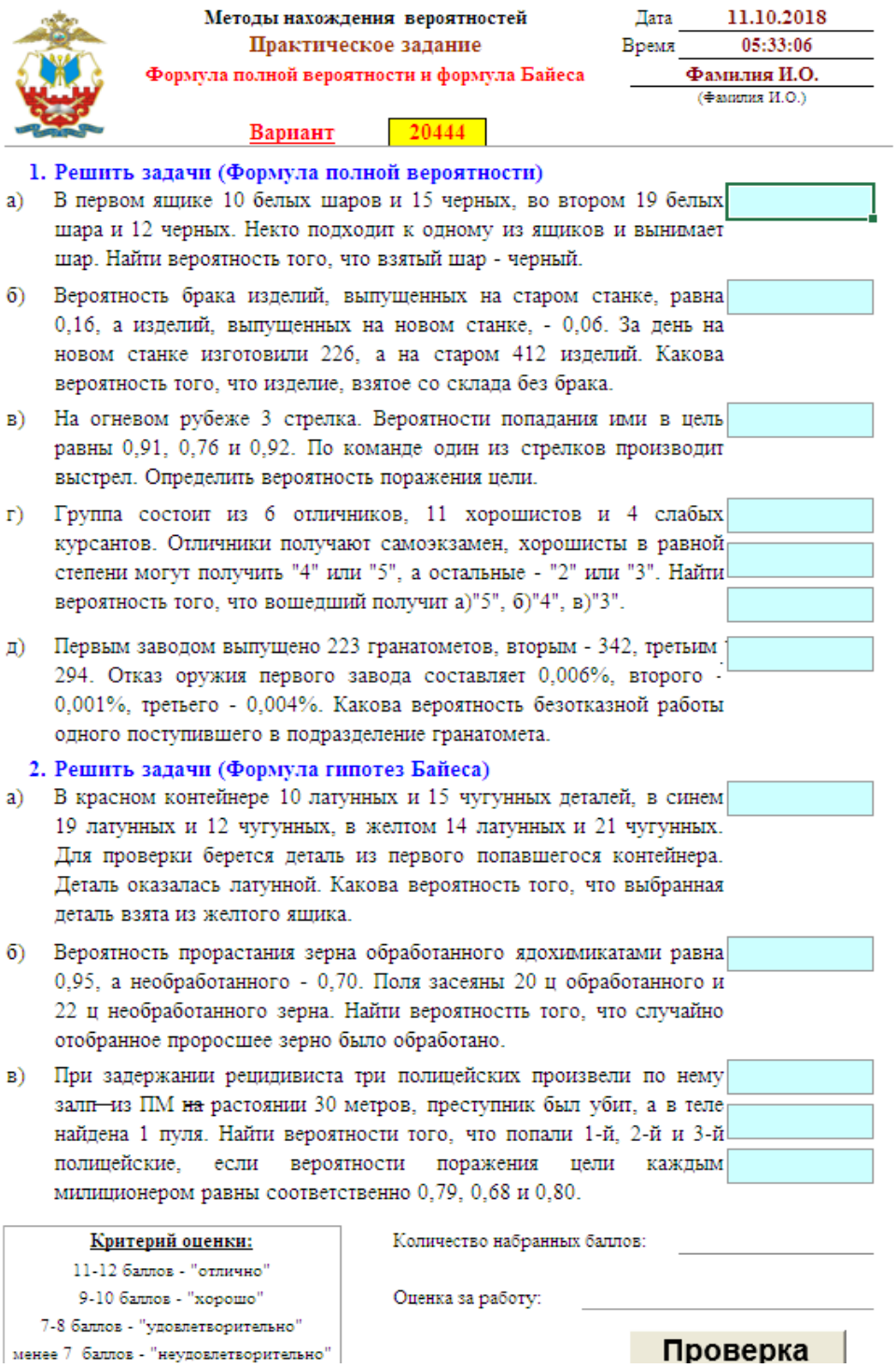


Рисунок 6.
Модуль «Формула полной вероятности и формула Байеса»

В завершение темы «Основные понятия теории вероятности» курсанты выполняют комплексную работу по теме (см. рис. 7), включающую задачи на разные теоремы и формулы. Здесь используются все изученные формулы комбинаторики, классическое определение вероятности события, формула условной вероятности, теоремы суммы и произведения событий, формула полной вероятности и формула гипотез Байеса.

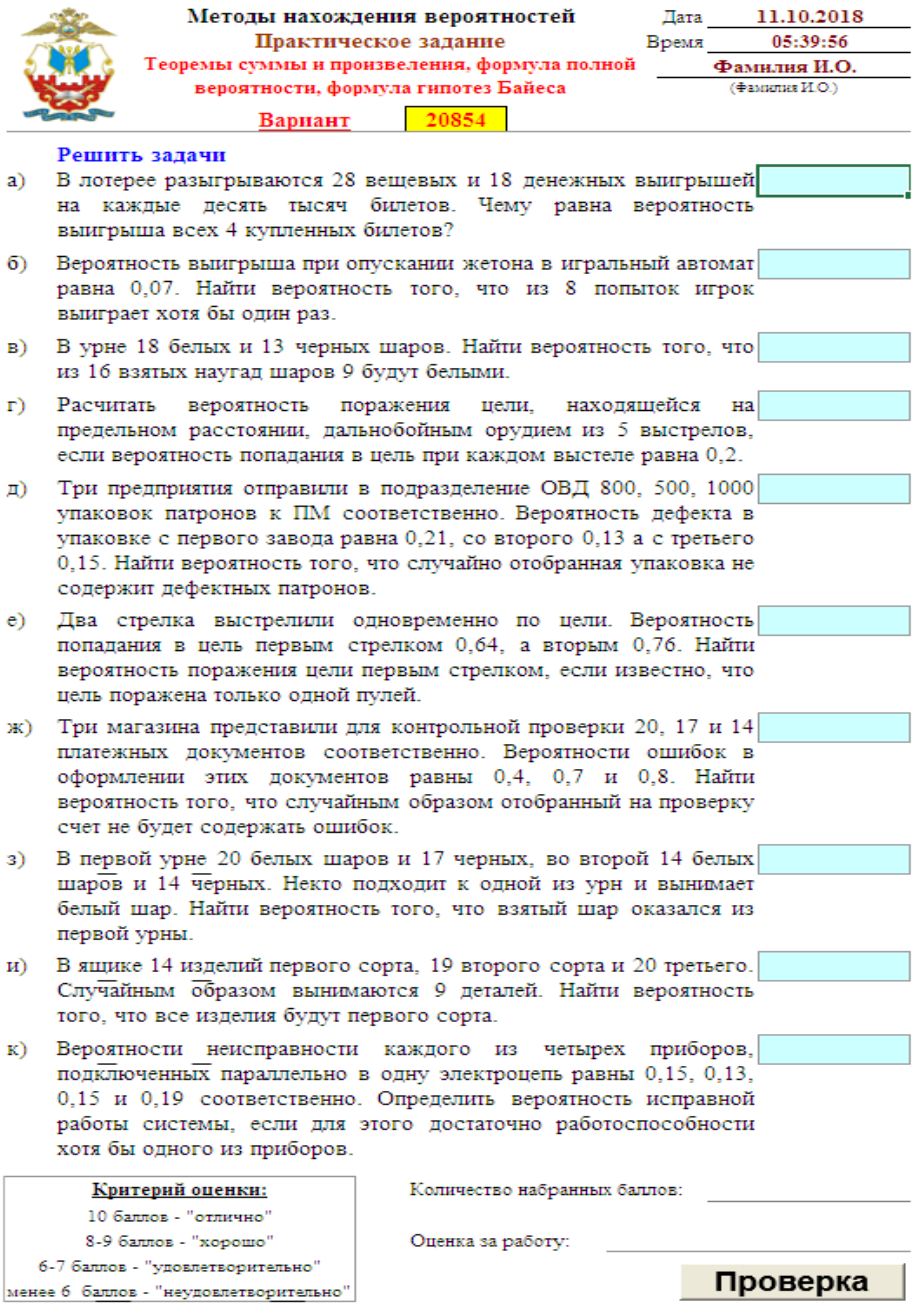


Рисунок 7.
Модуль «Комплексное задание»

Тема «Схемы повторных испытаний представлена двумя модулями. В первом используются задачи на формулы Бернулли и Пуассона (см. рис. 8). В этих задачах рассчитываются вероятности появления событий в многократно повторяющихся испытаний при данном комплексе условий. Формула Бернулли является предельной и используется, когда вероятность наступления события в каждом из испытаний стремится к нулю, а число испытаний сравнительно велико [17].

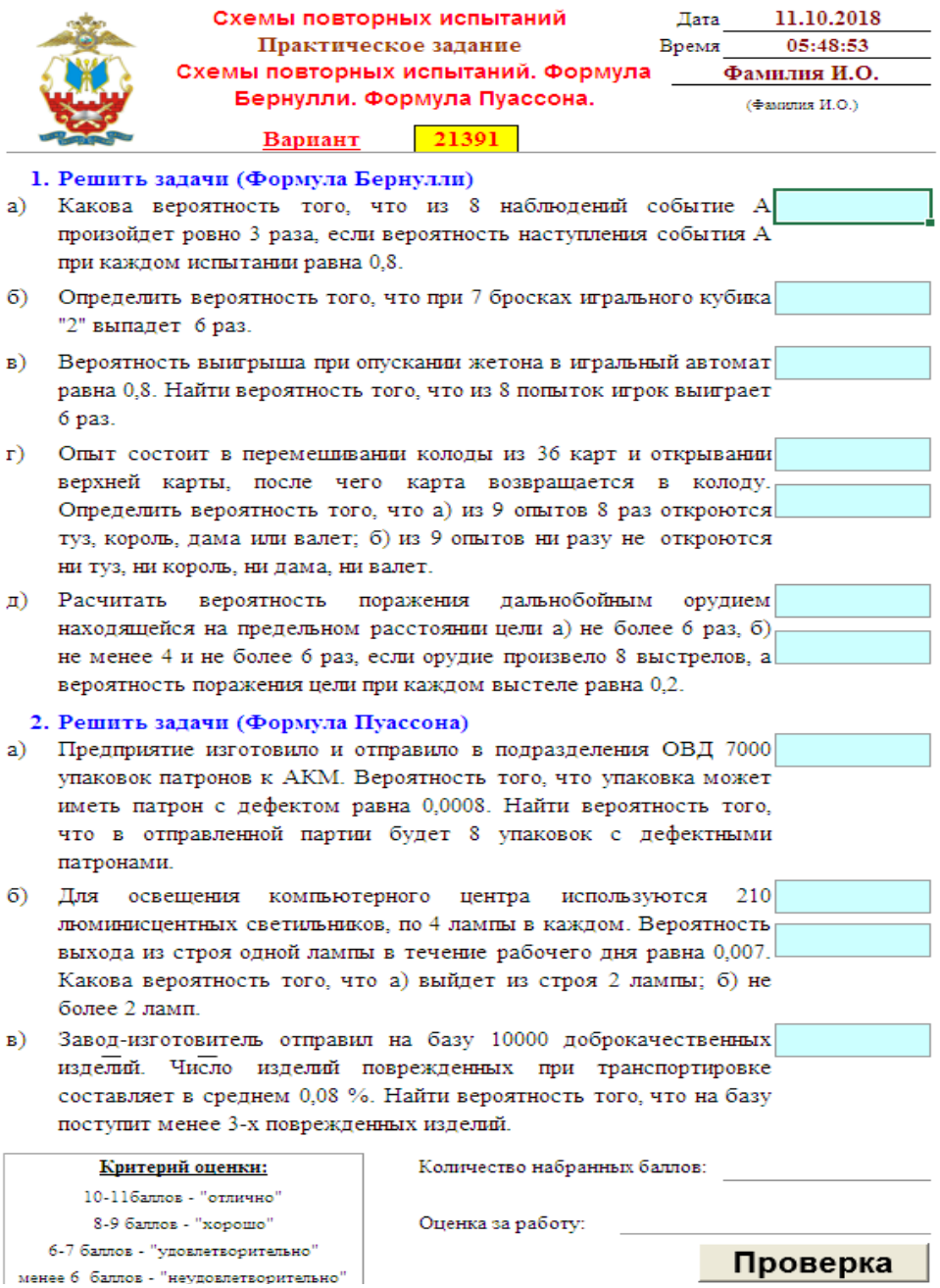


Рисунок 8.
Модуль «Формулы Бернулли и Пуассона»

При выполнении модуля «Локальная и интегральная формулы Муавра-Лапласа» (см. рис. 9) для использования обучаемым представлены задания, в которых вероятность наступления некоторого события в каждом из независимых испытаний отлична от нуля и единицы, а число испытаний достаточно велико. Для решения задач курсанты используют функции Гаусса и Лапласа, значения которых вычисляют с помощью представленных в программе таблиц [20]. В этом модуле также содержатся задачи на определение наивероятнейшего числа в многократно проводимых испытаниях [1].

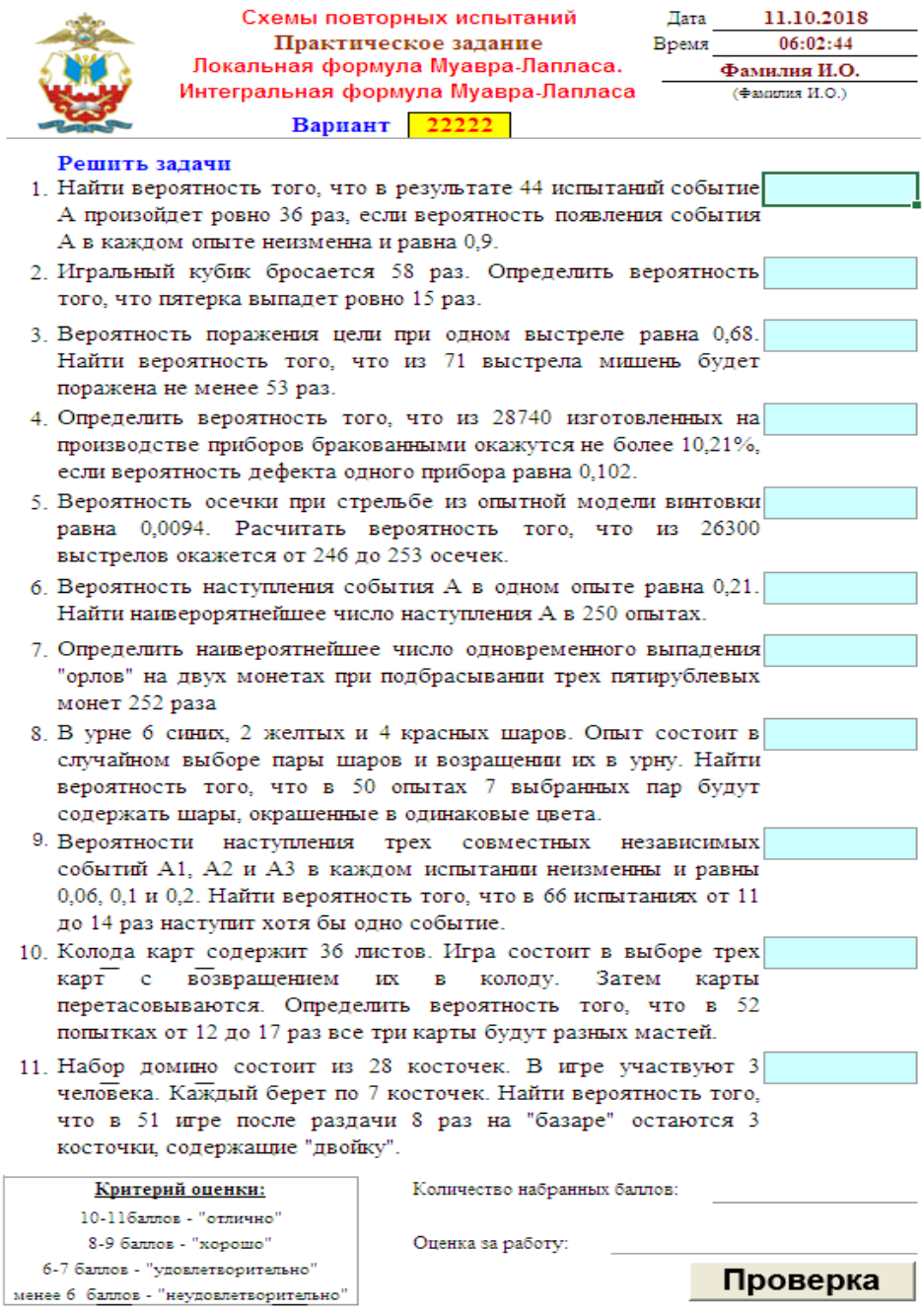


Рисунок 9.
Модуль «Локальная и интегральная формулы Муавра-Лапласа»

Тема «Случайные величины» представлена тремя модулями. Модуль «Числовые характеристики случайных величин» (см. рис. 10) предлагает обучаемым выполнить математические операции над случайными величинами, определить законы распределения дискретных случайных величин, вычислить числовые характеристики случайных величин: математическое ожидание, дисперсию и среднее квадратическое отклонение [3]. По представленному вариационному ряду построить функцию распределения и ее график, найти решение текстовой задачи.

x_i	2	4	6	12
p_i	0,17	0,53		0,19

y_i	0	2	4
p_i		0,68	0,29

$5x_i$				
p_i				

y_i^2			
p_i			

$x_i - y_i$								
p_i								

$x_i \cdot y_i$								
p_i								

z_i	0	1	2	3	4	5
p_i	0,125	0,037	0,19	0,035	0,184	0,429

Рисунок 10.
Модуль «Числовые характеристики случайных величин»

В модуле «Законы распределения дискретных случайных величин» (см. рис. 11) рассматриваются задачи с использованием биномиального закона распределения, закона распределения Пуассона, геометрического и гипергеометрического распределения [17]. Здесь же курсантам предлагается определить функцию распределения дискретной случайной величины, построить полигон и изобразить функцию распределения графически.

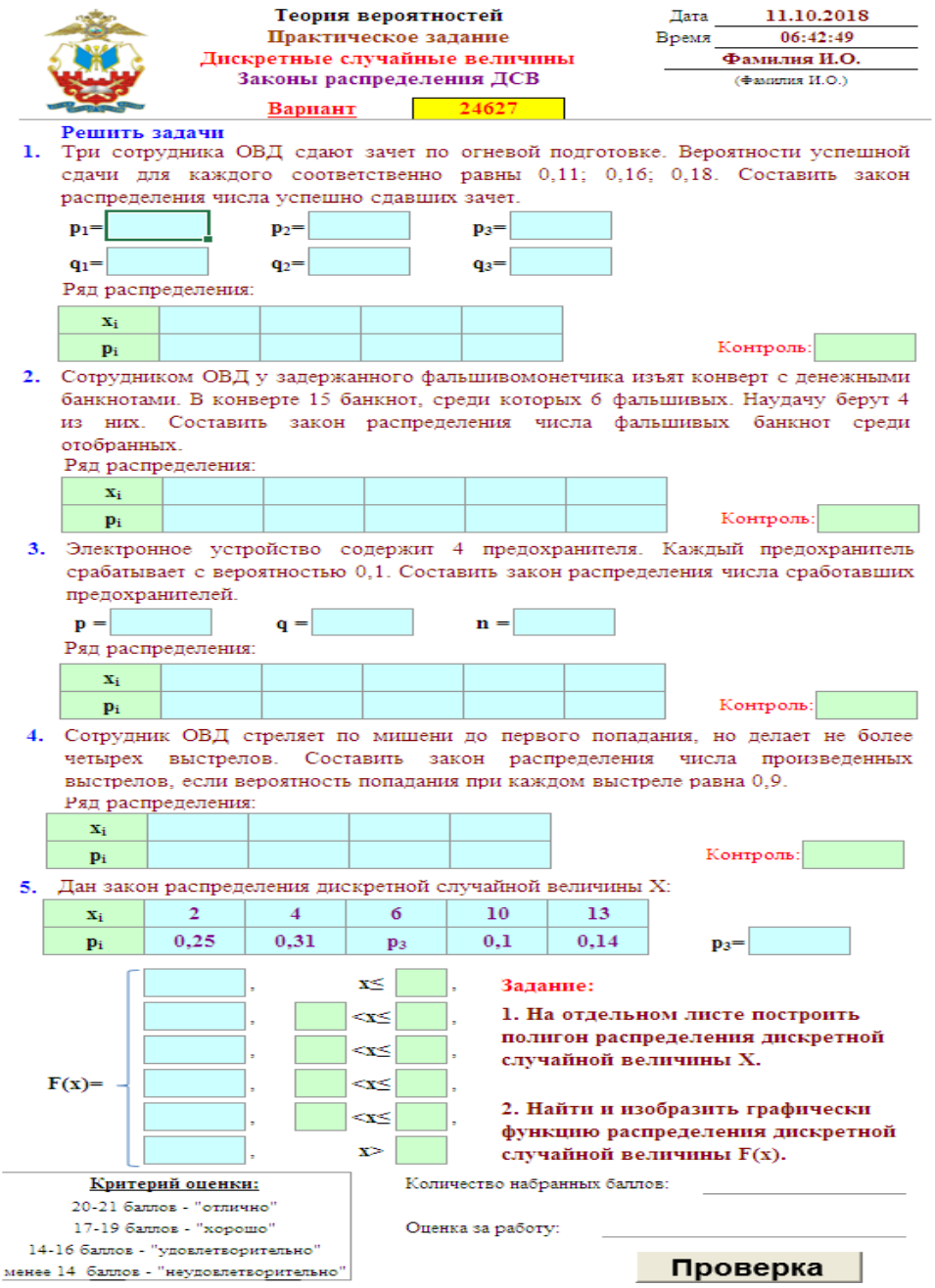


Рисунок 11.
Модуль «Законы распределения дискретных случайных величин»

Третий модуль темы «Числовые характеристики непрерывных случайных величин» (см. рис. 12) предназначен для действий с непрерывными случайными величинами. Курсантам предлагается найти вероятность принятия случайной величиной значения из заданного интервала, определить значения плотности распределения непрерывной случайной величины в заданных точках, по известной плотности распределения, найти вероятность попадания случайной величины в заданный интервал, вычислить числовые характеристики непрерывной случайной величины из заданного интервала по известной плотности распределения [20].

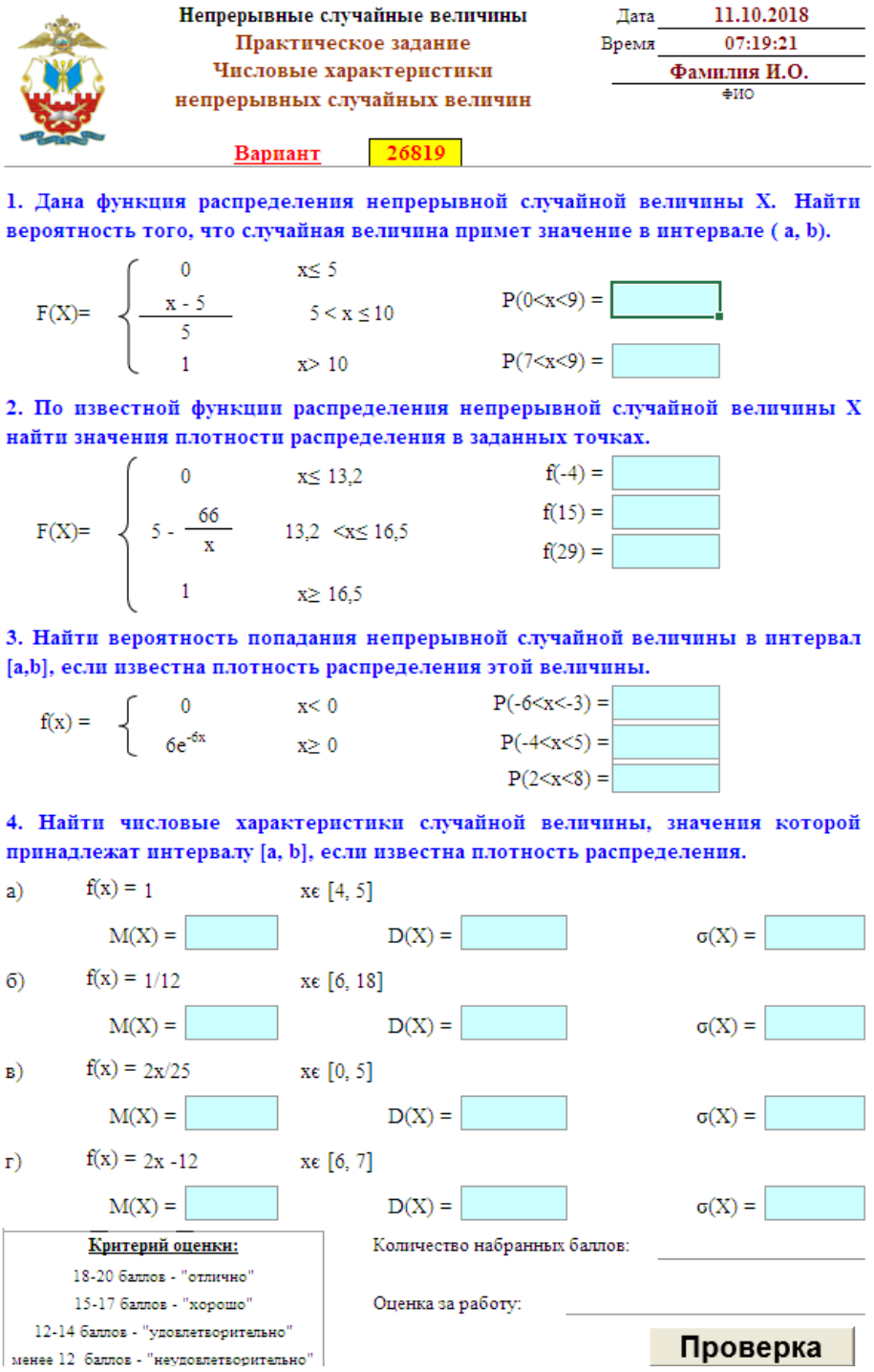


Рисунок 12.
Модуль «Числовые характеристики непрерывных случайных величин»

В завершение – два программных модуля по теме «Элементы математической статистики». Модуль «Элементы математической статистики» (см. рис. 13) предлагает по имеющейся выборке найти распределение часто и относительных частот в порядке их появления, построить вариационный ряд, вычислить эмпирическую функцию распределения, изобразить полигон и кумуляту частот, относительных частот, а также эмпирическую функцию распределения [4, 18].

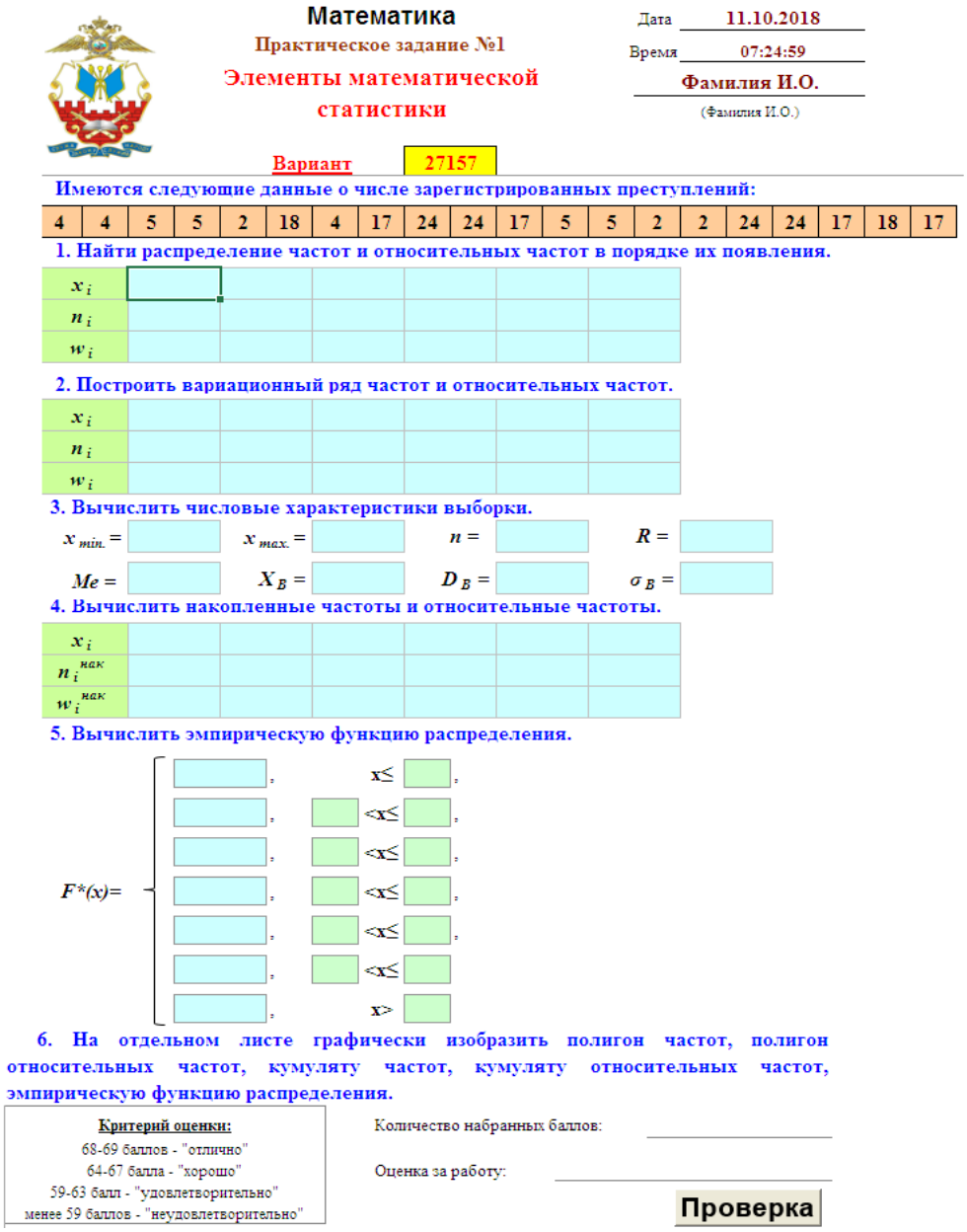


Рисунок 13.
Модуль «Элементы математической статистики»

И, в завершении, модуль «Статистические исследования выборки» (см. рис. 14) включает задания построения ранжированного ряда выборки, нахождения таких количественных показателей, как объем выборки, относительный показатель выборки, мода, медиана, размах. Курсантам предлагается составить дискретный вариационный ряд, построить эмпирическую функцию распределения, построить полигоны и кумуляты частот и относительных частот, вычислить выборочную среднюю, выборочную дисперсию, среднеквадратическое отклонение, «исправленную» выборочную дисперсию, «исправленное» выборочное отклонение [4, с. 18]. Обучаемые составляют интервальное статистическое распределение и графически отображают его.

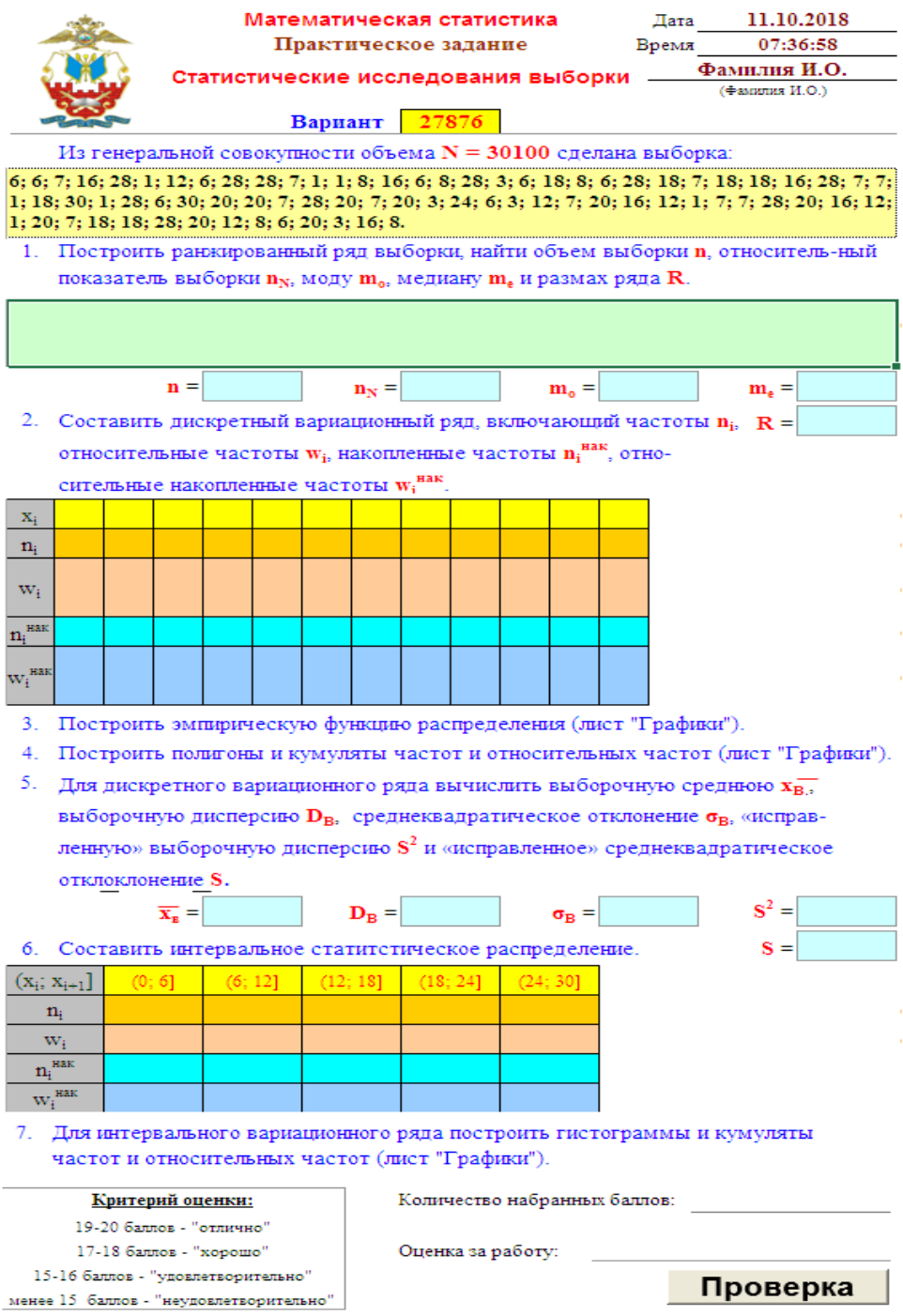


Рисунок 14.
Модуль «Статистические исследования выборки»

Представленный комплекс программ внедрен в образовательную деятельность кафедры информатики и математики. Опыт использования его в учебном процессе дал положительные результаты. В настоящее время ведутся работы над созданием ряда подобных программ для обеспечения дисциплин «Прикладная математика», «Математика и информатика», «Статистика», «Эконометрика», «Математические основы обработки информации», «Численные методы», «Программирование: языки, методы и технологии», «Базы данных».

Библиографический список

1. *Астафьев Е.Р., Арбузов П.В., Гуде С.В.* [и др.]. Информатика и математика. Часть 1. Математика: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2006. – 300 с.

2. *Астафьев Е.Р., Василенко В.В., Михайленко Е.В.* [и др.]. Математика: курс лекций. – Краснодар: Краснодарский университет МВД России, 2006. – 347 с.

3. *Астафьев Е.Р.*, *Михайленко Е.В.* Основы теории вероятностей и математической статистики: учебно-метод. пособие. – Краснодар: Краснодарская академия МВД России, 2004. – 58 с.

4. *Астафьев Е.Р., Михайленко Е.В.* Статистические методы обработки экспериментальных данных: учебное пособие. – Краснодар: Краснодарская академия МВД России, 2006. – 105 с.

5. *Лаптев В.Н., Михайленко Е.В.* Методы разработки тестовых заданий в автоматизированной контролирующей системе «Контроль» // Научный журнал КубГАУ [Электронный ресурс]. 2015. № 09 (113). С. 826-840. – IDA [article ID]: 1131509061. – Режим доступа: http://ej.kubagro.ru/2015/09/pdf/61.pdf.

6. *Лаптев В.Н., Михайленко Е.В.* Организация тестирования в автоматизированной контролирующей системе «Контроль» // Научный журнал КубГАУ [Электронный ресурс]. 2016. № 10 (124). С. 461-471. – IDA [article ID]: 1241610026. – Режим доступа: http://ej.kubagro.ru/2016/10/pdf/26.pdf.

7. *Михайленко Е.В., Хромых А.А.* Прикладная математика: курс лекций. – Краснодар: Краснодарский университет МВД России, 2014. – 192 с.

8. *Михайленко Е.В.* Автоматизация подготовки заданий и проверки выполненных работ по математическим и естественнонаучным дисциплинам / Проблемы информационного обеспечения деятельности правоохранительных органов: материалы Международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России, 2015. С. 107-114.

9. *Михайленко Е.В., Хромых А.А.* Дискретная математика: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2016. – 104 с.

10. *Михайленко Е.В.* Комбинаторный анализ: лекция. – Краснодар: Краснодарский университет МВД России, 2014. – 26 с.

11. *Михайленко Е.В., Старостенко И.Н.* Математика и информатика: курс лекций. – Краснодар: Краснодарский университет МВД России, 2009. – 420 с.

12. *Михайленко Е.В.* О разработке компьютерных обучающих программ в среде Visual Basic for Application / Математические методы и информационно-технические средства: материалы XII Всерос. науч.-практ. конф. 17 июня 2016 г. / редкол.: И.Н. Старостенко, Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодарский университет МВД России, 2016. С. 179-184.

13. *Михайленко Е.В., Макуха А.Ю.* О создании программных приложений реализации методов матричных игр для решения задач оптимизации / Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Ми-

хайленко, М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. С. 199-203.

14. *Михайленко Е.В.* Об автоматизации проведения контрольно-проверочных и итоговых занятий по определению уровня профессиональной подготовленности сотрудников органов внутренних дел к выполнению служебных задач / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 3-й Международной научно-практической конференции (14 октября 2016 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2017. С. 185-193.

15. *Михайленко Е.В.* Особенности разработки в VBA программных приложений для генерирования практических заданий и анализа их выполнения / Математические методы и информационно-технические средства: материалы XI Всерос. науч.-практ. конф., 19 июня 2015 г. / редкол.: И.Н. Старостенко, Е.В. Михайленко, Ю.Н. Сопильняк, А.В. Еськов, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2015. С. 159-162.

16. *Михайленко Е.В.* Особенности разработки компьютерных программ для подготовки практических заданий и анализа их выполнения по разделам булевой алгебры / Проблемы информационного обеспечения деятельности правоохранительных органов: материалы 2-й международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2016. С. 268-274.

17. *Михайленко Е.В., Жукова М.А., Бараненко Ф.Ф.* Теория вероятностей и математическая статистика: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2011. – 142 с.

18. *Михайленко Е.В., Новосельцева А.В.* Технологии исследования характеристик вариационного ряда в среде VBA / Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко, М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. С. 204-209.

19. *Михайленко Е.В.* Технологии разработки программных приложений для генерации и проверки выполнения практических заданий по математическим дисциплинам / Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко, М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. С. 192-199.

20. *Михайленко Е.В., Жукова М.А., Бараненко Ф.Ф.* Экономико-математические методы и модели: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2011. – 252 с.

ХАРАКТЕРИСТИКИ И РАЗНОВИДНОСТИ ИНТЕРНЕТ-ПРЕСТУПЛЕНИЙ И ИХ РАЗВИТИЕ

УДК 343

Савотченко С.Е.,
доктор физико-математических наук, доцент;
Дрога А.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Файоми Пол Оладеле,
аспирант
(Курская государственная сельскохозяйственная академия имени И.И. Иванова)

Аннотация: рассмотрены криминалистические свойства интернет-преступности в условиях развития информационного общества. Проанализированы появившиеся новые виды и способы совершения интернет-преступлений. Приведены примеры наиболее распространенных схем интернет-мошенничества. Указано, что выяснено, что наиболее часто совершаемым преступлением в сетях является неправомерный доступ к сети Интернет посредством использования чужих реквизитов.

Ключевые слова: информационная безопасность, Интернет, интернет-преступность, интернет-мошенничество, интернет-преступления, киберпреступления.

CHARACTERISTICS AND TYPES OF INTERNET CRIME AND THEIR DEVELOPMENT

Savotchenko S.E.,
Doctor of Physical and Mathematical Sciences, Associate Professor;
Droga A.A.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Fayomi Pol Oladele.
Post-qraduate Student
(I.I. Ivanov Kursk State Agricultural Academy)

Abstract: the forensic properties of Internet crime in the conditions of the development of the information society are considered. The new types and methods of committing Internet crimes are analyzed. Examples of the most common Internet fraud schemes are given. It has been indicated that it has been clarified that the most frequently committed crime in networks is unlawful access to the Internet through the use of someone else's details.

Key words: information security, Internet, Internet crime, Internet fraud, Internet crimes, cybercrime.

Повсеместное внедрение современных информационных технологий создает новые возможности для активного и эффективного развития экономики, политики, государства, общества, социального сознания и гражданина. Однако совершенствование технологий приводит не только к укреплению индустриального общества, но и к появлению новых источников опасности для него [1].

Активное применение информационных технологий привело к серьезным проблемам. Так, в настоящее время преступления в интернете совершаются чаще, появляются новые разновидности интернет-преступлений, наносящие серьезный ущерб обществу и государству. Для более точной характеристики интернет-преступлений необходимо описать следующие свойства интернет-преступности [2].

1. Удаленность интернет-преступлений. В отличие от физического мира, где человек при совершении преступления может находиться в определенный момент времени только в одном месте, преступления, совершаемые в Интернете, не могут характеризоваться нахождением субъекта преступления на месте его совершения. Это обуславливается тем, что глобальная сеть Интернет связывает тысячи компьютеров по всему миру и позволяет виртуально присутствовать в нескольких местах одновременно.

В связи с этим возникают проблемы при определении субъекта интернет-преступления, поскольку механизмы идентификации глобальной сети позволяют человеку совершать операции анонимно или выдавать себя за другое лицо, изменять биографические данные или свой социальный статус.

2. Неперсонофицированность и анонимность интернет-преступлений. Неперсонофицированность и анонимность проявляется во всех отношениях и действиях, совершаемых в сети Интернет. При совершении каких-либо действий преступник может сохранять свою анонимность, что позволяет ему остаться незамеченным. Анонимность становится причиной чувства вседозволенности у преступника, в связи с этим происходит размытие некоторых моральных принципов и «деформация» восприятия.

3. Интеллектуальный характер интернет-преступности. Совершение интернет-преступления требует определенного набора знаний. Чтобы совершить преступление в Интернете необходимо уметь работать с компьютером и Глобальной сетью, иметь представление об их физических и логических принципах работы. В свою очередь для совершения преступления в Интернете не требуется никаких способностей (достижение определенного возраста, социального положения), кроме интеллектуальных. Об этом свидетельствует тот факт, что в большинстве случаев интернет-преступниками являются люди, не достигшие совершеннолетия.

4. Высокая латентность интернет-преступности. Одной из причин высокой скрытой преступности в Интернете является то, что ущерб от преступления в большинстве случаев жертве кажется незначительным по сравнению с затратами на расследование данного преступления, в конечном итоге которого преступник может быть не найден. Еще одной из причин является нежелание отдельных компаний и пользователей предоставлять доступ к своим конфи-

денциальным данным, что является обязательным условием для раскрытия некоторых видов преступлений [3].

Оценить уровень латентности преступлений в Интернете достаточно сложно, но существуют исследования, свидетельствующие о высокой латентности отдельных подвидов компьютерной и интернет-преступности. Так, М.В. Старчиков называет уровень латентности, равный 99,7% по ст. 272 УК РФ и 99,8% по ст. 273 УК РФ как для всех преступлений в сфере компьютерной информации, так и для преступлений, совершенных посредством сети Интернет [3].

Быстрый рост преступлений в Интернете предопределил появление различных видов и способов их совершения.

Одним из видов современных киберпреступлений является кардинг. Кардинг – это вид интернет-преступления, представляющий собой способ мошенничества с банковскими картами. Мошенником осуществляется похищение реквизитов банковской карты с помощью взлома серверов интернет-магазинов, систем платежей или персонального компьютера пользователя банковской карты.

Одной из разновидностей картинга является фишинг. Фишинг – это очень серьезное интернет-преступление. Преступники отправляют пользователю сообщения якобы от администратора системы платежей или от банка, почтовых серверов или социальных сетей с просьбой перейти по указанной ссылке. Целью таких сообщений является получение логина и пароля пользователя, для того чтобы воспользоваться его счетом в банке, учетной записью в платежных системах, электронной почтой или социальными сетями.

«Нигерский спам» – один из видов интернет-преступлений. Этот вид мошенничества является довольно старым. Схема действия преступников основывается на том, что мошенник уверяет пользователя в том, что у него есть крупная сумма денег, которая была выручена незаконным путем и предлагает жертве оказать помощь в выводе средств через свой счет в банке за границу и обещает за оказание этой услуги хороший процент. В конечном итоге, после того как мошенник получает доступ к счету в банке, на нем не остается средств.

В Уголовном кодексе Российской Федерации интернет-преступности посвящена целая глава, а также данный вид преступлений своим составом подходит под многие другие виды преступлений [4].

Преступления против жизни и здоровья (глава 16 УК РФ). Интернет все чаще используется в жизненно важных системах, что открывает новые возможности для совершения преступлений. Первым зарегистрированным интернет-преступлением против жизни является убийство, произошедшее в феврале 1998 г. в США. Тяжело раненный свидетель преступления находился в закрытой больнице, преступники через Интернет изменили работу кардиостимулятора и аппарата вентиляции, вследствие чего он скончался.

По мнению Р.И. Дремлюги, способы причинения вреда и лишения жизни посредством сети Интернет можно разделить по типу воздействия на ЭВМ:

• нарушение работы ЭВМ или ее полная остановка, например, остановка системы обеспечения жизнедеятельности;

• изменение характеристик и порядка работы системы ЭВМ, например, изменение параметров работы бортового компьютера автомобиля;

• запуск программ ЭВМ, которые угрожают жизни и здоровью людей, например, запуск электроцепи во время электромонтажных работ.

Интернет позволяет воздействовать как на целую систему ЭВМ, так и на ее отдельные составляющие (на отдельный компьютер или программу жизнеобеспечения на нем). Преступник может создать «вирус», который выведет из строя отдельный компьютер, либо программу на этом компьютере, отвечающую за работу кардиостимулятора.

В настоящее время наиболее распространенными преступлениями против жизни людей являются преступления, совершаемые под эгидой «Синий кит». Это смертельно опасная игра, которая широко распространена в социальных сетях. В соцсетях «ВКонтакте» и в «Инстаграм» в январе-феврале 2016 года стали появляться картинки с китами, плывущими в океане, и хештегами «синий кит», «разбуди меня в 4.20», «Я в игре», «Тихий дом». Хештег является средством выхода на контакт с преступником, нажав на него вы попадаете на страницу или сообщество в социальной сети. После того как вы попали в группу «синий кит», с вами связывается куратор, который дает задания, чтобы проверить, готова ли жертва «поиграть». Но в самом начале «куратор» при помощи переписки выясняет, из какой семьи новый участник, его настроение, узнает информацию, чтобы составить психологический портрет «игрока», а также по возможности узнает его геоданные. Игра рассчитана на 50 дней, каждый из которых содержит новое задание. Для начала игроку предлагается нарисовать на руке кита в знак принадлежности, не разговаривать весь день, сменить статус на #якит, далее идут уже более серьезные задания: вырезать на руке f57, проснуться в 4.20 и пойти на крышу, сидеть вниз ногами на краю крыши, встретиться с китом, в 50-й день игрок должен совершить самоубийство. Если же участник игры отказывается выполнять задания, ему начинают угрожать жизнью и здоровьем его семьи.

В большинстве случаев под влияние этой игры попадают подростки в возрасте от 12 до 16 лет.

Последствием такого широкого распространения групп смерти явилось большое количество самоубийств. По неофициальным данным зарегистрировано 90 суицидов подростков.

Преступления против свободы, чести и достоинства личности (гл. 17 УК РФ). Анонимность, широкие возможности распространения информации в сети делают Интернет средством доставки информации большому количеству людей. Отсутствие фактического контроля интернет-услуг со стороны государства делают сеть сферой распространения оскорбительной, ложной клеветнической информации.

Так, например, «Российская газета» пишет, что 30-летний житель Красноярска отправил клеветническое сообщение на электронную почту ГУВД, в

котором указал на неблаговидную и незаконную деятельность своего знакомого. В ходе расследования мужчина сознался, что со своим знакомым находился в конфликте и таким образом хотел доставить ему неприятности (ст. 129 УК РФ) [5].

Интернет предоставляет большие возможности для оскорбления личности. Оскорбительные действия могут быть совершены при помощи сети Интернет: устно – при отправке голосовых сообщений в социальных сетях; письменно – в виде текстового сообщения; телодвижениями – жестами в видеоконференциях или видеочатах; пересылкой файла – видео или графического изображения.

Преступления против половой неприкосновенности и половой свободы личности (гл. 18 УК РФ). Глобальная сеть дает широкие возможности для совершения преступления против половой неприкосновенности и половой свободы, Интернет является серьезным подспорьем насильникам и педофилам в совершении преступления. Посредством сети Интернет происходит подготовка для совершения ряда половых преступлений.

Схема действия интернет-педофилов очень проста. Они входят в детские чаты и начинают общение с ребенком. Завоевав доверие ребенка, преступник назначает ему встречу под каким-либо отвлеченным предлогом, а, чтобы жертва от него не «ускользнула», он предлагает ему вознаграждение [6].

В.А. Голубев утверждает, что каждый пятый ребенок в возрасте от 10 до 17 лет получал предложения сексуального характера, каждому четвертому ребенку, вступившему в переписку с преступником, были присланы фотографии или видео порнографического характера [6].

Преступления против собственности (гл. 21 УК РФ). Этот вид преступлений является наиболее распространенным в интернет-пространстве. С каждым днем появляются новые формы, виды и способы интернет-мошенничества. В большинстве случаев, злоумышленниками создаются интернет-сайты физического или юридического лица, на которых производится сбор средств обманным путем. Также в Интернете можно найти жертву, ввести ее в заблуждение и осуществить мошенническую финансовую операцию. Примером может послужить пресс-релиз с сайта по борьбе с компьютерными преступлениями департамента юстиции США. Гражданин Казахстана, при помощи доступа в Интернет скачал базы данных с личной информацией клиентов Bloomberg L.P.’s и вымогал 200000 долларов США, угрожая опубликовать эти базы данных в сети Интернет.

Преступления в сфере экономической деятельности (гл. 22 УК РФ). В настоящее время в Глобальной сети появилось огромное количество сайтов, занимающихся проведением кредитных, валютных операций, которые осуществляют свою деятельность без каких-либо разрешений и лицензий. Они позволяют мгновенно переводить денежные средства с одного счета на другой, с одной валюты в другую и даже незаметно вывезти деньги из страны без каких-либо документов. При совершении операций с интернет-деньгами зачастую не остается бумажных следов, а только временные электронные. Так как часто

возникают трудности при определении компьютера, с которого была совершена операция, установить личность, совершившую эту операцию, не представляется возможным.

О.С. Гузеева приводит примеры наиболее распространенных схем интернет-мошенничества [7]:

1) схема «увеличить и сбросить» (Pump&dump) – вид рыночной манипуляции, заключающейся в извлечении прибыли за счет продажи ценных бумаг, спрос на которые был искусственно сформирован. Первоначально создается повышенный спрос на определенные ценные бумаги, затем осуществляется их продажа по завышенным ценам. После совершения подобных манипуляций цена на рынке возвращается к своему исходному уровню, а рядовые инвесторы оказываются в убытке;

2) схема финансовой пирамиды (Pyramid Schemes) при инвестировании денежных средств с использованием интернет-технологии полностью повторяет классическую финансовую пирамиду. Инвестор получает прибыль исключительно за счет вовлечения в игру новых инвесторов;

3) схема «надежного» вложения капитала (The «Risk – free» Fraud) или «инвестиционная схема» заключается в распространении через Интернет инвестиционных предложений с низким уровнем риска и высоким уровнем прибыли. Например, вложение в якобы высоколиквидные ценные бумаги неизвестных компаний;

4) «экзотические» предложения (Exotic Offerings), например, распространение через Интернет акций коста-риканской кокосовой плантации, имеющей контракт с сетью американских универмагов и гарантирующей получение сверхдоходов;

5) мошенничества с использованием банков (Prime Bank Fraud) заключаются в том, что мошенники, прикрываясь именами и гарантиями известных и респектабельных финансовых учреждений, предлагают инвесторам вложение денег в ничем не обеспеченные обязательства с нереальными размерами доходности;

6) интернет-попрошайничество. В Интернете могут появиться объявления, например, от благотворительной организации с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, и меняют реквизиты для перечисления денег;

8) аукционы и розничная торговля в режиме онлайн. Отличительная черта этого вида мошенничества – низкая цена на определенный товар и отсутствие фактического адреса или телефона продавца. В этом случае предлагается подделка, некачественный товар либо деньги покупателей просто присваиваются, а товар не доставляется [7].

Преступления в сфере компьютерной информации (гл. 28 УК РФ). Повышение ценности информации в новом высокотехнологичном обществе предопределило необходимость ее защиты. Можно с уверенность сказать, что неправомерный доступ – наиболее распространенное преступление в Интернете. Глобальная сеть позволила совершать данный тип преступлений, не выходя из

дома. Большинство улик для установления местоположения и личности преступника хранится в атакуемой системе, поэтому совершая преступление, он не только совершает преступление, но и стирает его следы. Компьютерная система, в которую вторгается злоумышленник, может быть любой: будь это персональный компьютер, ЭВМ банковской сети и даже компьютерная система министерства обороны какого-либо государства.

Основной проблемой при подсчете статистики интернет-преступлений является то, что подсчет количества преступлений ведется за счет косвенных показателей. В России ведется статистика компьютерных преступлений, но не все общественно опасные деяния, подразумевающие уголовную ответственность, совершаются посредством сети Интернет. Но анализ преступлений, совершенных посредством сети Интернет, все же ведется. Это доказывают некоторые региональные и общероссийские исследования. В ходе проведенных исследований было выяснено, что наиболее частосовершаемыми преступлениями является неправомерный доступ к сети Интернет посредством использования чужих реквизитов.

Такие данные не могут адекватно отразить складывающуюся на тот промежуток времени ситуацию. Подобные процессы могут быть объяснены как проводимой реформой в органах внутренних дел, которая привела к ослаблению контроля учетно-регистрационной дисциплины, так и снижением активности правоохранительных органов по выявлению преступлений данного вида, поскольку факторы, влияющие на совершение компьютерных преступлений, не уменьшились, а только еще больше увеличились. Также необходимо отметить, что рост преступлений в 2012 году напрямую связан с увеличением числа интернет-пользователей до 68 млн по сравнению с 2011 годом (60,4 млн).

Сокращение количества преступлений в 2009-2011 гг. носит искусственный характер, о чем свидетельствует наглядное сравнение динамики зарегистрированных преступлений в сфере компьютерной информации и число интернет-пользователей за вышеуказанный период.

Рассмотрев наиболее распространенные виды преступлений в Интернете, можно сделать вывод, что интернет-преступность обладает некоторыми свойствами: высокая латентность интернет-преступлений, отсутствие в Российской Федерации официальной статистики интернет-преступности в силу ее скрытости. Использование сети Интернет в преступлениях должно иметь уголовно-правовое значение, так как увеличивает общественную опасность деяния.

Библиографический список

1. *Тропина Т.Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. – Владивосток, 2005. С. 235.

2. *Кесареева Т.П.* Криминологическая характеристика и предупреждение преступности в российском сегменте сети Интернет: дис. … канд. юрид. наук. – Москва, 2002. С. 25.

3. *Старичков М.В.* Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. … канд. юрид. наук. – Иркутск, 2006. С. 109-112.

4. Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 27.06.2018) // Собрание законодательства Российской Федерации. 1994. № 25. Ст. 2654.

5. *Корзун В.* Красноярца привлекут к уголовной ответственности за клевету [Электронный ресурс] // Российская газета. – Режим доступа: http://www.rg.ru/2006/12/08/kleveta.htm

6. *Голубев В.А.* Компьютерная преступность – проблемы борьбы с интернет-педофилией и детской порнографией [Электронный ресурс] // Центр исследования компьютерной преступности. – Режим доступа: http://www.-crime%research.ru/articles/golubev2106/

7. *Гузеева О.* Квалификация мошенничества в российском сегменте сети интернет // Законность. 2013. № 3. С. 22.

ОСОБЕННОСТИ СЕТЕВОЙ РЕАЛИЗАЦИИ СИСТЕМ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

УДК 004.41

Старостенко И.Н.,
кандидат физико-математических наук, доцент
(Краснодарский университет МВД России)

Аннотация: в статье рассматривается система сетевой и компьютерной безопасности, обнаруживающая нарушения безопасности и автоматически защищающая от них – система предотвращения вторжений (IPS), обосновывается актуальность IPS, приведен алгоритм настройки сетевой IPS на маршрутизаторе.

Ключевые слова: вредоносный трафик, компьютерная сеть, маршрутизатор, межсетевой экран, сетевая защиты, сигнатура, угроза.

FEATURES OF THE NETWORK IMPLEMENTATION OF INTRUSION PREVENTION SYSTEMS

Starostenko I.N.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Krasnodar university of MIA of Russia)

Abstract: the article discusses a network and computer security system that detects security breaches and automatically protects against them – the Intrusion

Prevention System (IPS), substantiates the relevance of IPS, and provides an algorithm for setting up network IPS on a router.

Key words: malicious traffic, computer network, router, firewall, network protection, signature, threat.

В современном динамично развивающемся информационном обществе сетевая безопасность приобретает решающее значение. Одна из основных задач любой организации заключается в предоставлении своим сотрудникам непрерывного и безопасного доступа к сетевым ресурсам. Для этого стратегия обеспечения сетевой безопасности должна учитывать такие факторы, как повышение степени надежности компьютерной сети, эффективное управление безопасностью, защита от стремительно распространяющихся и эволюционирующих угроз.

Существующие основные механизмы сетевой защиты (контроль доступа с помощью аутентификации, авторизации и учета, межсетевые экраны) должны быть дополнены системами для обнаружения и предотвращения угроз в каждой входящей и исходящей точке сети. К таким системам относятся системы обнаружения вторжений (IDS) или более масштабируемые системы предотвращения вторжений (IPS).

Реализация IDS предполагает пассивный мониторинг трафика в сети. Устройство с IDS копирует поток трафика и выполняет анализ копируемого трафика вместо фактически пересылаемых пакетов. Работая вне сети, устройство сопоставляет поток трафика с известными вредоносными сигнатурами. Преимущество работы с копией трафика выражается в том, что IDS не оказывает негативного влияния на поток пакетов пересылаемого трафика. Недостатком такой работы является то, что IDS не в состоянии остановить распространение вредоносных однопакетных атак к целевой системе до момента принятия мер против этих атак. Системам IDS, как правило, требуется наличие вспомогательных сетевых устройств, таких как маршрутизаторы и межсетевые экраны, чтобы противодействовать атакам.

Более оптимальным решением является устройство, которое может незамедлительно определять и предотвращать атаки. Такие функции выполняют IPS.

IPS анализирует определенные шаблоны атак и рассылает оповещения или выполняет превентивные действия, когда такие шаблоны обнаруживаются. IPS реализуются во встроенном режиме. Это означает, что для обработки весь входящий и исходящий трафик должен проходить непосредственно через это устройство. IPS не допускает попадания пакетов в доверенную часть сети без выполнения их анализа. Это позволяет незамедлительно выявлять и принимать меры для решения сетевых проблем. IPS выполняет мониторинг трафика на сетевом и транспортном уровнях эталонной модели OSI. При этом выполняется анализ содержимого и полезной нагрузки пакетов для выявления более изощренных атак, проводимых с помощью вредоносных данных на уровнях с канального до прикладного. IPS реагирует на угрозы мгновенно и не

допускает распространение вредоносного трафика, в то время как IDS пропускает такой трафик до принятия специальных мер.

Одной лишь системы IPS недостаточно для того, чтобы маршрутизатор являлся надежным межсетевым экраном для Интернет. В сочетании с другими средствами обеспечения безопасности возможно организовать эффективную и надежную систему защиту информации.

Хостовая реализация IPS (HIPS) представляет собой программное обеспечение, устанавливаемое на отдельном хосте для мониторинга и анализа подозрительной активности. Важным преимуществом HIPS является возможность контроля и защиты операционной системы, а также критически важных системных процессов на каждом хосте сети. HIPS может предотвращать несанкционированные обновления реестра, осуществление изменений в системном каталоге, выполнение установки программ, а также операции, которые могут привести к переполнению буфера.

Сетевая IPS может быть реализована с помощью выделенного или невыделенного IPS-устройства. Именно сетевая реализация IPS является критически важным компонентом системы предотвращения вторжений. Существующие решения, основанные на локальных системах IDS/IPS, необходимо интегрировать с сетевыми вариантами IPS для того, чтобы добиться гарантированного обеспечения надежности архитектуры безопасности. Сетевая модель IPS предполагает развертывание сенсоров в определенных точках сети, что позволяет отслеживать сетевую активность вне зависимости от места нахождения объекта атаки. Сенсоры определяют вредоносные и несанкционированные действия в режиме реального времени и при необходимости могут принять надлежащие действия.

Сетевая модель IPS должна иметь возможность определять входной вредоносный трафик, чтобы блокировать его. Для обнаружения вредоносного трафика IPS использует набор правил – сигнатур, однозначно идентифицирующих конкретных червей, вирусов, аномалий протоколов. Сенсоры IPS настроены на поиск соответствующих сигнатур или необычных характеристик трафика. Сенсоры IPS анализируют поток данных с помощью разных сигнатур. В случае обнаружения в потоке данных какой-либо сигнатуры сенсор выполняет заранее определенные действия, например, фиксирует это событие в журнале или посылает сигнал тревоги программам, управляющим системой IPS.

Сенсоры IPS могут быть реализованы несколькими способами. Рассмотрим алгоритм настройки IPS на маршрутизаторе в режиме интерфейса командной строки (CLI) с помощью программного обеспечения Cisco IOS IPS.

Перед настройкой IPS необходимо загрузить с сайта cisco.com файлы с пакетами сигнатур IOS IPS (IOS-Sxxx-CLI.pkg) и открытый криптографический ключ (realm-cisco.pub.key.txt). Криптографический ключ проверяет цифровую подпись для главного файла сигнатур (sigdef-default.xml). Содержимое подписывается с помощью закрытого ключа, чтобы гарантировать подлинность и целостность при каждом выпуске. Выбор конкретных файлов IPS для загрузки определяется текущей версией. Во флеш-памяти в привилегиро-

ванном режиме необходимо создать каталог для размещения файлов сигнатур и настроек:

Router# mkdir ipsdir

Create directory filename [ipsdir]? <Enter>

Created dirflash:ipsdir

Текст, содержащийся в файле открытого ключа, необходимо скопировать и вставить в командную строку глобальной конфигурации маршрутизатора. Этот текстовый файл запускает на исполнение различные команды для генерации ключа RSA.

На следующем шаге выполняется настройка IPS. Первоначально в глобальном режиме маршрутизатора указывается название правила IPS:

Router(config)#ipips name rule_1

Файлы IPS будут храниться в каталоге ipsdir:

Router(config)#ip ips config location flash:ipsdir

После указания имени правила включается сервер Security Device Event Exchange (SDEE) и уведомление о событии регистрации в журнале. Сервер SDEE построен на основе протокола Simple Object Access Protocol (SOAP), спецификации формата оповещений IDS и транспортных протоколов.

Для использования SDEE необходимо включить HTTP-сервер. Если HTTP-сервер не включен, маршрутизатор не увидит запросы и не сможет отвечать клиентам SDEE. Уведомления SDEE по умолчанию отключены.

Router(config)#ip http server

Router(config)#ip ips notify sdee

Сообщения о фиксировании в журнале информации, касающейся системы IPS, отправляются на сервер службы syslog, если он настроен. При необходимости поддержку syslog для IPS можно включить с помощью команды:

Router(config)#ip ips notify log

SDEE и Syslog могут использоваться независимо друг от друга или работать одновременно для отправки уведомлений о событиях IOS IPS.

Далее осуществляется настройка IOS IPS на использование одной из предварительно заданных категорий сигнатур. Сигнатуры в IPS используются для обнаружения вредоносной активности, наиболее распространенных типов сетевых атак и для сбора информации.

Все сигнатуры предварительно разбиты по категориям, категории имеют иерархическую структуру. Это позволяет классифицировать сигнатуры для более простой настройки и группирования.

Сигнатуры, применяемые системой IOS IPS при сканировании трафика, могут быть удалены или восстановлены. Удаление сигнатуры означает, что IOS IPS не компилирует эту сигнатуру в память для сканирования. При восстановлении сигнатуры IOS IPS выполняет ее компилирование в память и применяет для сканирования трафика. При первом конфигурировании IOS IPS все сигнатуры из категории *all* удаляются. Затем необходимо восстановить отдельные сигнатуры, относящиеся к категории тех, которые меньше всего потребляют ресурсы оперативной памяти.

Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit

В примере сигнатуры категории all выведены из использования, а затем введена в использование категория basic.

Имеет значение последовательность, в которой на маршрутизаторе настраиваются категории сигнатур. Система IOS IPS обрабатывает команды категорий в том порядке, в котором они приводятся в конфигурации. Некоторые сигнатуры принадлежат нескольким категориям. Если настроены несколько категорий и какая-либо сигнатура принадлежит более чем одной из них, то IOS IPS будет использовать свойства сигнатуры из последней указанной категории.

После настройки IOS IPS на использование сигнатур необходимо применить правило IPS к требуемому интерфейсу и указать направление трафика: входящий и/или исходящий.

Router(config)#interface g0/0
Router(config-if)#ip ips rule_1 in
Router(config-if)#exit
Router(config)# interface g0/1
Router(config-if)#ip ips rule_1 in
Router(config-if)#ip ips rule_1 out

Правило rule_1 применяется к входящему трафику на интерфейсе G0/0 и к входящему и исходящему трафику на интерфейсе G0/1.

На заключительном шаге пакет сигнатур IOS IPS с помощью протоколов FTP или TFTP необходимо загрузить на маршрутизатор.

Router#copy tftp://192.168.1.1/IOS-S327-CLI.pkg idconf

Использование FTP сервера для копирования файла сигнатур на маршрутизатор выполняется с помощью следующей команды:

copy ftp://<ftp_user:password@Server_IP_address>/<signature_package> idconf

Если к серверу FTP или TFTP доступа нет, то для загрузки пакета сигнатур на маршрутизатор можно использовать USB-накопитель. В этом случае команда будет выглядеть следующим образом:

Router#copy usbflash0:IOS-S327-CLI.pkg idconf

После внедрения системы IPS необходимо проверить конфигурацию и убедиться в корректности функционирования системы. В этом случае используются различные команды *show*.

Команда *show ip ips all* отображает все данные конфигурации IPS. Длина результата зависит от конфигурации IPS. Выполнение команды *show ip ips configuration* позволяет получить дополнительные данные конфигурации, которые не отображаются при использовании команды *show running-config*. Команда *show ip ips interfaces* позволяет отобразить данные конфигурации ин-

терфейса. Команда *show ip ips signatures* выполняет проверку конфигурации сигнатур. Команда *show ip ips statistics* отображает количество проверенных пакетов, а также количество отправленных сигналов тревоги. Дополнительный ключ *reset* позволяет обновить результат с целью отображения самых новых данных. Команда *clear ip ips configuration* используется для отключения системы IPS, удаления всех параметров конфигурации IPS и высвобождения динамических ресурсов. Команда *clear ip ips statistics* выполняет сброс статистических данных о проанализированных пакетах и отправленных сигналов тревоги.

Библиографический список

1. *Старостенко И.Н., Сопильняк Ю.Н.* Информационная безопасность. – Краснодар: Краснодарский университет МВД России, 2012.

2. *Старостенко И.Н.* Целенаправленные атаки (APT) и методы защиты от них / Проблемы информационного обеспечения деятельности правоохранительных органов: материалы 3-й Международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2017.

МУЛЬТИМЕДИЙНЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКЕ

УДК 378.1

Макото Курита
(фабрика AVC Networks Company, Panasonic Corporation в России);
Акапьев В.Л.,
кандидат технических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Акапьев В.В.
(Балтийский государственный технологический университет
имени Д.Ф. Устинова)

Аннотация: актуализация федерального образовательного стандарта высшего образования, реализация принципов системно-деятельностного подхода в обучении и решение проблем формирования информационно-технологической компетентности специалиста приводит к необходимости активизации применения цифровых образовательных ресурсов на базе мультимедийных технологий.

Ключевые слова: визуализация информации, мультимедийная инфозона, мультимедийность, повышение квалификации, профессиональная подготовка, цифровые образовательные ресурсы.

MULTIMEDIA TECHNOLOGIES IN PROFESSIONALNOY TRAINING

Makoto Kurita
(factory AVC Networks Company, Panasonic Corporation in Russia);
Akapyev V.L.,
Candidate of Technical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Akapyev V.V.
(Baltic state technological University named after D.F. Ustinov)

Abstract: the actualization of the Federal educational standard of higher education, the implementation of the principles of system-activity approach in training and the solution of problems of formation of information and technological competence of the specialist leads to the need to enhance the use of digital educational resources based on multimedia technologies.

Key words: information visualization, multimedia infozone, multimedia, training, training, digital educational resources.

Педагогические работники учебных заведений системы МВД России должны четко понимать, что разработка цифровых образовательных ресурсов для реализации всех видов и форм профессионального образования базируется на реализации двух ключевых аспектов: мультимедийности и интерактивности.

Остановимся на одном из самых популярных терминов современности – мультимедийности или мультимедиа. Принято считать, что мультимедиа представляет собой одновременное комбинированное применение с помощью компьютерных систем нескольких форм представления информации (media), к которым относятся: звук, изображение, видео. То есть речь идет об интерактивных диалоговых системах, реализующих одномоментное использование звука, компьютерной графики, анимации, видеокадров, статистических изображений, графических и текстовых документов и т.д.

В настоящее время мультимедийность, как правило, увязывают с интернет-ресурсами. Вряд ли с таким подходом можно согласиться, так как мультимедийность, не став еще научным понятием, получила широкое распространение во всех сферах человеческой деятельности. Не осталась в стороне и педагогика.

Какие возможности открывает мультимедийность в профессиональном образовании? Не секрет, что современный молодой (да и не только) человек с большим трудом воспринимает учебный материал, представленный в вербальной форме. В первую очередь, необходимо визуализировать эту информацию, но простая ее оцифровка не даст искомого результата. Предпочтение должно отдаваться не статическим, а динамическим форматам представления, так как здесь актуализируется один из психологических аспектов восприятия: человек лучше видит и, соответственно, запоминает движущийся объект.

Ключевым здесь выступает тот факт, что человек мыслит образами, а визуализация информации облегчает построение зрительных образов и, тем самым, открывает возможность увеличения качества образовательного процесса.

Таким образом можно сказать, что в рамках решения образовательных задач под *мультимедийностью* понимается подача учебного материала по нескольким каналам восприятия обучаемого. И чем больше будет таких каналов, тем больше вероятность запоминания курсантами и слушателями новых учебных сведений. При этом требуется учитывать специфику детской психики, андрагогики и ряд других психолого-педагогических моментов.

Современная педагогическая наука отмечает, что традиционные принципы и методы обучения молодежи крайне неэффективны. Почему это происходит? Одним из объяснений указанной ситуации может быть рассмотрение информационной составляющей процесса обучения. В какой форме и из каких источников получает информацию современный молодой человек? В основном это анимация, компьютерная графика, 3D-графика, видео, персональные компьютеры, планшеты, сотовые телефоны и другие электронные гаджеты.

В каком же виде поступает к нему учебный материал в рамках обучения в высшем учебном заведении? Твердые носители информации (учебно-методическая литература), вербальное изложение достаточно сложных понятий и определений, плакаты, стенды и т.д. Он бы и рад учиться, но возникает двойная проблема восприятия: незнакомая информация представлена в форме, вызывающей отторжение. Поэтому занятие, проводимое в вербальной форме, не даст сколь-нибудь положительных результатов.

Научные исследования показывают, что даже подготовленная аудитория при такой форме проведения занятия в состоянии зафиксировать не более трети учебного материала. Сразу же по окончании занятия полученные знания можно делить на два, а если в течение недели эти знания не нашли прикладного значения, их объем сокращается до трех процентов от первоначального объема. Другими словами, все делали вид, что учат и учатся, но результат такого обучения практически нулевой.

В качестве инструмента решения поднятой проблемы могут выступить мультимедийные инфозоны в образовательных учреждениях. Мультимедийная **инфозона** – это информационное табло, представляющее современную замену информационного стенда и позволяющее решать широкий спектр задач (см. рис. 1).

Рисунок 1. Мультимедийная инфозона

Благодаря тому, что информация демонстрируется в мультимедийном виде, уже привычном для современного человека, она неизбежно привлекает внимание. Благодаря разнообразию форматов демонстрируемой информации, на нее, во-первых, обращают значительно больше внимания субъекты образовательного процесса (обучаемые – в первую очередь). Во-вторых, такая визуализация способствует улучшению запоминания нового учебного материала, что в итоге приводит к увеличению качества образовательного процесса.

Несколько слов о формах подготовки сотрудников правоохранительных органов. Следует обратить внимание и на опыт наших «заклятых друзей» из-за океана. Ведь у них практически отсутствует профессиональная подготовка и повышение квалификации в привычной для нас форме: никто никого никуда не посылает на какие-то курсы. Зато вас могут собрать на двадцать минут, и психолог изложит в доступной форме особенности общения с жертвой разбойного нападения, а социолог объяснит специфику взаимодействия с различными этническими группами и т.д. Остальная необходимая информация транслируется непрерывно с помощью инфозон. То есть процесс повышения профессионального уровня вплетен в повседневную профессиональную же деятельность и не отвлекает от нее. Повышение квалификации осуществляется на рабочем месте.

Библиографический список

1. *Акапьев В.Л., Савотченко С.Е.* К вопросу систематизации понятия профессиональной компетентности педагога и ее информационной составляющей // Вестник Белгородского института развития образования. 2016. № 2.

2. *Савотченко С.Е., Акапьев В.Л., Дрога А.А.* Модель информационной образовательной среды вузов МВД России в условиях корпоративного обучения // Проблемы правоохранительной деятельности. 2017. № 1.

3. *Козиоров Е.Л.* Интерактивные доски Panasonic для совместной работы // Справочник руководителя образовательного учреждения. 2010. № 9.

4. *Приезжая М.Н.* Цифровые образовательные ресурсы для интерактивных досок // Управление начальной школой. 2011. № 3.

РОЛЬ НЕПРОЦЕССУАЛЬНЫХ ФОРМ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

УДК 343.7

Чиненов Е.В.,
кандидат экономических наук, доцент;
Щукин В.И.,
кандидат юридических наук, доцент;
Журбенко А.М.,
кандидат юридических наук
(Белгородский юридический институт МВД России И.Д. Путилина)

Аннотация: в статье проанализирована роль непроцессуальных форм применения специальных знаний при получении информации, способствующей эффективному определению времени, места совершения противоправного деяния, а также подбор научно-технических средств и методов для раскрытия и расследования экономических преступлений.

Ключевые слова: специальные знания, непроцессуальные формы, информация, консультационная деятельность.

ROLE OF NOT PROCEDURAL FORMS OF USE OF SPECIAL KNOWLEDGE IN DISCLOSURE AND INVESTIGATION OF ECONOMIC CRIMES

Chinyonov E.V.,
Candidate of Economics Sciences, Associate Professor;
Schukin V.I.,
Candidate of Jurisprudence Sciences, Associate Professor;
Zhurbenko A.M.,
Candidate of Jurisprudence Sciences
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in article the role of not procedural forms of use of special knowledge when obtaining information promoting effective definition of time, the

place of commission of illegal act is analysed and also a selection of scientific and technical means and methods for disclosure and investigation of economic crimes.

Key words: special knowledge, not procedural forms, information, consulting activity.

Основной целью использования специальных знаний в ходе раскрытия и расследования преступлений являются эффективное собирание, проверка и объективная оценка доказательств. Существенными особенностями обладают специальные знания, используемые в расследовании экономических преступлений [9, с. 40]. С учетом специфики предмета проводимого нами исследования (экономические преступления в сфере железнодорожного транспорта) считаем необходимым более подробно рассмотреть и проанализировать особенности применения непроцессуальной формы специальных знаний, используемых при их раскрытии и расследовании.

Следует отметить, что данные формы не закреплены законодателем в Уголовно-процессуальном кодексе [2, с. 39]. В то же время необходимо заметить, что, несмотря на это, требования к такой форме знаний определяются вследствие сложившейся практики [10, с. 36].

Основной целью непроцессуальной формы применения специальных знаний является получение информации, способствующей эффективному определению места, времени совершения противоправного деяния, тактики производства отдельных следственных действий, а также подбору участников, научно-технических средств и методов [1, с. 263]. Из анализа цели мы можем сделать вывод о том, что к непроцессуальной форме применения специальных знаний следует отнести ряд действий:

– во-первых, консультацию у специалистов;

– во-вторых, справочную деятельность сведущих лиц;

– в-третьих, помощь специалистов при подготовке к отдельным процессуальным действиям;

– в-четвертых, непосредственное участие специалистов в реализации оперативно-розыскных мероприятий;

– в-пятых, проведение документальных проверок и ревизий.

Необходимо отметить, что специалист, осуществляющий консультации, вправе оформить результат в виде письменного документа, а также ответить на поставленные перед ним вопросы устно. Результаты консультаций, оформленные в письменном виде, могут быть приобщены к материалам уголовного дела или к материалам проверки первичной информации.

Под консультацией следует понимать научно обоснованный совет специалиста о специфике отдельных профессиональных вопросов в какой-либо деятельности. В частности, если совершенное преступление касается определенной профессиональной сферы, например, в области врачебной деятельности, компьютерной и т.д., следователь, который проводит предварительное расследование, может не обладать достаточным объемом знаний для успешного и эффективного раскрытия и расследования преступления [3, с. 131].

В том случае, если подозреваемый компетентен в определенной области знаний, которая непосредственно соприкасается с совершенным преступлением, то он может целенаправленно ввести в заблуждение лицо, осуществляющее предварительное расследование, тем самым может создаться впечатление случайности произошедших событий. В подобных случаях лицу, производящему предварительно расследование, рекомендуется обратиться за помощью к специалисту в соответствующей области знаний, что будет способствовать наиболее эффективному и объективному изучению всех обстоятельств совершенного преступления, выявлению и установлению причин и условий, способствующих его совершению.

Криминалистические учеты позволяют получить лицу, производящему предварительное расследование, справочную информацию об интересующих его событиях и фактах. Кроме названного позволяют получить ответы на запросы об особенностях технологий, технологических процессах и технических приемах, позволившим лицу добиться соответствующего преступного результата [6, с. 43].

К консультационной деятельности близка по своей специфике помощь специалиста при планировании проведения процессуальных действий. В данном случае специалист может посоветовать следователю применение каких-либо определенных технических средств. Также при проведении следственных действий необходимо учитывать психологические особенности проводимого следственного действия. В частности, при проведении следственных действий, направленных на получение информации (допрос, очная ставка, проверка показаний на месте и т.д.), необходимо учитывать психологическую специфику личности [4, с. 221].

Интеграция современных информационных технологий во все области человеческой жизнедеятельности повлекла интеллектуализацию экономической преступности. С помощью компьютерных средств, систем, технологий совершаются преступления против личности, против общественной безопасности и общественного порядка, собственности, большая часть преступлений в сфере экономики: отдельные виды преступлений, направленные против собственности; преступлений в сфере экономической деятельности; против интересов службы в коммерческих и иных организациях. Достижения в сфере информационных и компьютерных технологий лежат в основе механизма мошенничеств, присвоений и растрат, незаконного предпринимательства, криминальных банкротств, таможенных, финансовых и иных преступлений. К ним можно отнести фальсификацию платежных документов; хищение наличных и безналичных денежных средств, совершенное путем перечисления на фиктивные счета; отмывание денег; вторичного получения уже произведенных выплат; совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств; продажи секретной информации и др. [8, с. 331].

В процессе раскрытия и расследования экономических преступлений часто возникают вопросы, в решении которых требуются специальные знания

в какой-либо сфере деятельности. К специальным знаниям можно отнести приобретенные субъектом знания, полученные в процессе практической деятельности путем специальной подготовки или профессионального опыта, которые основываются на системе теоретических знаний в конкретной сфере деятельности (например, знание технологии железнодорожных перевозок и т.п.) [7, с. 236].

Использование специальных знаний происходит в процессуальной и в непроцессуальной формах. К субъектам использования специальных знаний относятся: следователь; лица, производящие дознание; начальник следственного отдела; прокурор; специалисты; эксперты; лица, обладающие познаниями в области науки, техники, искусства или ремесла, но не наделенные процессуальными правами эксперта или специалиста; оперативные работники.

К непроцессуальным формам использования специальных познаний можно отнести:

– консультативную и справочную деятельность сведущих лиц;

– производство ревизионных и аудиторских действий;

– участие сведущих лиц в оперативно-разыскных мероприятиях, в том числе производство так называемых предварительных исследований материальных объектов, оказание технической помощи следователю или оперативному сотруднику и т.п.

Несмотря на всю важность, ценность знаний, сведений, получаемых посредством непроцессуальной формы, эти знания не могут быть использованы в качестве доказательств по уголовному дела, так как не предусмотрены Уголовно-процессуальным кодексом, а регулируются законодателем в иных нормативно-правовых актах. Однако не стоит умалять значения непроцессуальной формы получения информации, так как именно она является в некотором роде первоисточником получения сведений о разыскиваемом лице, о способе совершения преступления и сокрытии его следов, установлении признаков, свидетельствующих о подготовке к совершению преступления [5, с. 96].

Цель как консультативной, так и справочной деятельности сведущих лиц заключается в передаче следователю некоторой предварительной информации, позволяющей правильно ориентироваться в создавшейся обстановке. Как консультации, так и справки могут даваться и в письменной, и в устной форме. Письменная информация приобщается к уголовному делу или первичному материалу проверки. Справочными сведениями могут снабдить следователя сотрудники экспертных подразделений, в ведении которых имеются специализированные картотеки и коллекции. Цель ревизионных и аудиторских проверок совпадает с целью консультаций и справочных данных.

В процессе расследования представляется важным правильно выбрать момент назначения экспертизы и осуществить эффективную ее подготовку.

Подготовка к назначению экспертизы состоит из формулирования задач экспертизы; определения материалов дела, содержащих исходные данные для нее; подбора объектов экспертизы; постановления (определения) о назначении экспертизы.

Именно на стадии подготовки назначения экспертизы и решения задач требуется привлечение в справочно-консультативной форме специальных знаний.

Библиографический список

1. *Аверьянова Т.В., Аминов Д.И., Архипова И.А*. [и др.]. Криминалистика: учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция». – 3-е изд. перераб. и доп. – Москва, 2017. – 799 с.

2. *Варданян А.В.* Дискуссионные вопросы формирования дефиниции понятия специалиста в уголовном судопроизводстве // ЮП. 2017. № 4 (83). С. 38-42.

3. *Волынский А.Ф.* Оперативно-розыскная деятельность как средство доказывания в уголовном процессе / Раскрытие и расследование преступлений серийных и прошлых лет: материалы Международной научно-практической конференции / под общ. ред. А.И. Бастрыкина. – Москва, 2017. С. 127-135.

4. *Гусев А.В.* Актуальные направления криминалистического исследования механизма реализации познаний специалиста // Общество и право. 2015. № 1 (51). С. 219-224.

5. *Еремин С.Г., Стешенко Ю.С.* Теория формирования методики расследования преступлений, совершенных в сфере экономики / Технико-криминалистическое обеспечение раскрытия и расследования преступлений: сборник тезисов и статей Международной научно-практической конференции. – Москва, 2018. С. 95-97.

6. *Лавров В.П.* Расследование преступлений по горячим следам. – Москва, 1989. – 87 с.

7. *Леханова Е.С.* Некоторые проблемы применения судебно-экономических знаний в уголовном процессе // Пробелы в российском законодательстве. 2009. № 4. С. 234-238.

8. *Чиненов Е.В., Воронов С.С.* Информационные технологии в системе криминалистического обеспечения раскрытия и расследования экономических преступлений, совершаемых на объектах железнодорожного транспорта // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 4 (44). С. 328-344.

9. *Шапиро Л.Г.* Специальные знания в уголовном судопроизводстве и их использование при расследовании преступлений в сфере экономической деятельности: автореф. дис. … д-ра юрид. наук. – Краснодар, 2008. – 51 с.

10. *Шаталов А.С.* Уголовный процесс : понятие, система, типы: учебно-методическое пособие. – изд. 2-е, стереотип. – Москва – Берлин: Директ-Медиа, 2016. – 72 с.

ИЗВЛЕЧЕНИЕ ДАННЫХ С МОБИЛЬНЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ANDROID DEBUG BRIDGE (ADB) В КРИМИНАЛИСТИЧЕСКИХ ЦЕЛЯХ

УДК 343:519.81

Иванов В.Ю.,
кандидат технических наук
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: расследование преступлений в сфере высоких технологий предполагает поиск цифровых доказательств противоправных действий пользователя в информационной системе. В качестве объектов исследования для формирования доказательной базы используются всевозможные устройства, способные хранить в себе цифровую информацию. Автором статьи рассмотрены различные программные, аппаратные и аппаратно-программные комплексы, используемые органами внутренних дел для расследования киберпреступлений. Показаны способы получения информации с мобильных устройств.

Ключевые слова: киберпреступление, следы на информационных носителях, образ оперативной памяти, мобильные устройства, органы внутренних дел.

DATA EXTRACTION FROM MOBILE DEVICES USING THE ANDROID DEBUG BRIDGE (ADB) IN FORENSIC PURPOSES

Ivanov V.Yu.,
Candidate of Technical Sciences
(Kikot Moscow University of the Ministry of the Internal Affairs of the Russian)

Abstract: investigation of crimes in the sphere of high technologies involves the search for digital evidence of the user's illegal actions in the information system. As objects of research for the formation of evidence base, all kinds of devices capable of storing digital information are used. The author of the article considers various software, hardware and hardware-software complexes used by law enforcement bodies to investigate cybercrimes. The methods of obtaining information from mobile devices are shown.

Key words: cybercrime traces on information carriers, the computer's memory, a mobile device, police.

ADB (Android Debug Bridge – «Отладочный мост для Андроид») представляет собой встроенный протокол операционной системы «Android», позволяющий разработчикам подключаться к устройству и выполнять команды низкого уровня, используемые для разработки. Эксперты же используют данный протокол для извлечения данных из мобильных устройств. Термин

«Android Debug Bridge» уже дает понять, что данный протокол является связующим звеном между Android-устройством и ПЭВМ.

Структура указанного протокола представляет собой клиент-серверную систему, включающую в себя три компонента:

– клиента, функционирующего на машине разработки и отправляющего команды. Вызов клиента из терминала командной строки осуществляется с помощью команды adb;

– демона (adbd), который запускает команды на устройстве. Он запускается как фоновый процесс на каждом устройстве;

– сервер, который управляет связью между клиентом и демоном. Он в свою очередь работает как фоновый процесс на вашей машине разработки. ADB входит в пакет Android-SDK. В общем случае при его помощи можно осуществлять следующие операции:

- выводить список подключенных к ПК устройств, работающих по протоколу ADB;
- просматривать лог-файлы работы Android ОС;
- устанавливать и удалять приложения;
- создавать и восстанавливать пользовательские данные;
- выполнять unix-команды на устройстве. Запускать скрипты;
- прошивать Android-устройство;
- копировать файлы с аппаратуры или на аппарат.

В рамках экспертной деятельности указанный протокол можно использовать при реализации как логического, так и физического извлечения данных.

В случае логического извлечения применяется резервное копирование посредством Android Debug Bridge, которое можно использовать, не прибегая к дополнительным операциям по получению root-доступа. Для этого в терминале ADB можно воспользоваться следующей командой:

adb backup -f "D:\logical_backup.ab" -apk -shared –all, где ключ -apk говорит о необходимости создать резервную копию APK-приложения; -shared, включает данные приложений и содержимое карты памяти, если последняя имеется; -all, добавит в резервную копию все приложения, в том числе системные.

Однако современные устройства позволяют сохранить в такую резервную копию далеко не все [1]. Например, сюда не входит ни список контактов, ни sms-сообщения, и чтобы побороть указанную проблему, необходимо предварительно установить приложение-агент от разработчиков криминалистического программного обеспечения, которое будет аккумулировать в себе различные данные.

Тем не менее, наибольший интерес в рамках проведения криминалистического исследования представляет собой физическое извлечение данных, которое реализовывается с помощью копирования файлов с android-устройства посредством утилиты dd.

dd (dataset definition) – команда UNIX, предназначенная как для побайтового копирования.

С ее помощью можно реализовывать довольно сложные операции без привлечения дополнительного программного обеспечения. В частности, можно создавать резервную копию MBR, зеркалировать носители информации, создавать дампы данных с различных накопителей и многое другое.

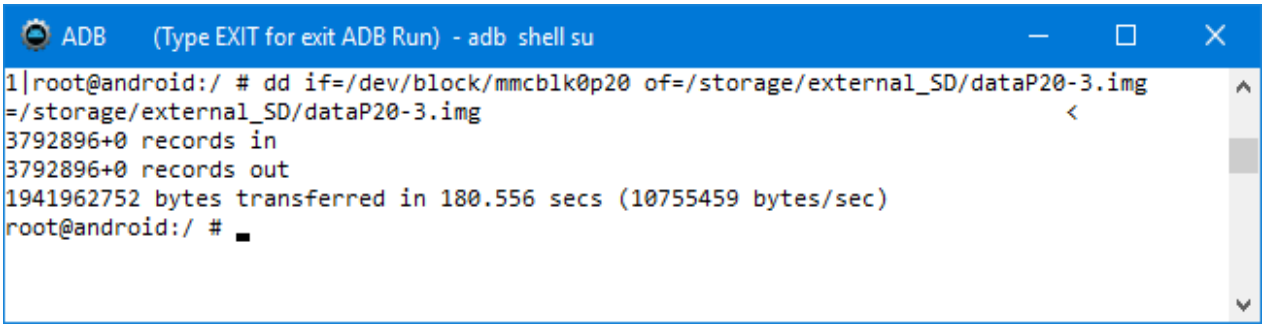


Рисунок 1.
Реализация посекторного копирования с помощью утилиты dd в терминале «ADB RUN»

Однако необходимо отметить, что для использования указанного протокола с целью посекторного копирования (физического извлечения) существует ряд определенных требований [2]:

- Наличие включенного параметра «Отладка по USB» (Меню> Настройки > Приложения >Разработка > Отладка USB);
- Доступ к устройству должен осуществляться с Root-правами.

Под Root-правами («правами суперпользователя») понимается процесс, позволяющий пользователям мобильных устройств получать привилегированный доступ (Root-доступ) к системным папкам, файлам и т.д., Root-доступ позволяет обойти ограничения, установленные производителями и операторами [3].

Основные способы получения root-доступа условно можно разделить на два типа: программы на ПЭВМ и программы на android-устройство (apk-приложение) [4]. При этом некоторые программы реализованы и на ПЭВМ, и на android-устройство. Примеры таких приложений:

- KingRoot;
- Framaroot;
- Baidu Root;
- Kingo Root;
- VRoot;
- Unlock Root;
- Towelroot;
- Root Dash;
- 360 Root и др.

Необходимо отметить, что процесс получения root-доступа для каждого устройства специфичен и индивидуален, поэтому общего алгоритма получения root-прав не существует, необходимо исходить из каждой конкретной ситуации.

После получение root-доступа и снятия посекторной копии возникает вопрос анализа. И здесь список используемого программного обеспечения стандартен:

- R-Studio;
- BelkasoftEvidenceCenter;
- Magnet IEF и др.

Библиографический список

1. *Слюнкина А.Д., Иванов В.Ю.* Исследование короткоживущих данных при расследовании компьютерных преступлений / Технологии информационной безопасности в деятельности органов внутренних дел: сборник научных трудов XIII научно-практической конференции. – Москва, 2016. С. 62-65.

2. Effective Email Borne Ransomware Responses // Сайт компании FireEye. – URL: https://www.fireeye.com

3. Empowering Collection to Analysis Excellence // Сайт компании AccessData. – URL: http://www.accessdata.com/product-download

4. Computer Forensic Tool Catalog // The National Institute of Standards and Technology (NIST) is an agency of the U.S. Commerce Department. – URL: https://toolcatalog.nist.gov

НЕКОТОРЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ФУНКЦИОНИРОВАНИЯ ЦЕНТРАЛИЗОВАННОГО УЧЕТА ТРУДОВЫХ МИГРАНТОВ НА СОВРЕМЕННОМ ЭТАПЕ

УДК 004:31

Прокопенко А.Н.,
кандидат технических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Стребков В.Н.,
старший инспектор отдела по вопросам миграции
(ОМВД России по Белгородскому району)

Аннотация: в статье рассматриваются вопросы правового регулирования миграционного учета иностранных граждан и лиц без гражданства в Российской Федерации. Анализируется состав и основы функционирования государственной информационной системы миграционного учета. Рассматриваются особенности интеграции информационных ресурсов ФМС России в информационные ресурсы МВД России. Кроме того, в статье кратко анализируются контрольно-надзорные функции МВД России в сфере миграционного учета.

Ключевые слова: миграционный учет, трудовая миграция, государственная информационная система миграционного учета.

SOME QUESTIONS OF THE ORGANIZATION OF FUNCTIONING OF THE CENTRALIZED ACCOUNTING OF LABOUR MIGRANTS AT THE PRESENT STAGE

Prokopenko A.N.,
Candidate of Technical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Strebkov V.N.,
Senior Inspector of Department Concerning Migration
(OMVD of Russia of the Belgorod district)

Abstract: in article questions of legal regulation of migration registration of foreign citizens and persons without citizenship in the Russian Federation are considered. The structure and bases of functioning of the state information system of migration registration is analyzed. Features of integration of information resources of FMS of Russia into information resources of the Ministry of Internal Affairs of the Russian Federation are considered. Besides, in article control and supervising functions of the Ministry of Internal Affairs of the Russian Federation in the sphere of migration registration are briefly analyzed.

Key words: migration registration, labor migration, state information system of migration registration.

Миграционный учет иностранных граждан на территории Российской Федерации является основным методом административно-правового регулирования внешней трудовой миграции и приобретает особую роль на современном этапе в связи с принятием 31 октября 2018 года Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы, утвержденной Указом Президента Российской Федерации от 31.10.2018 № 622 [1].

Необходимо отметить, что миграционный учет, в первую очередь, направлен на общий контроль за иностранными гражданами в целях обеспечения безопасности и правопорядка в Российской Федерации. И.В. Никитенко справедливо отмечает, что «миграционный учет является основным методом не только для регулирования трудовой миграции, но и для контроля всех миграционных процессов, а также обеспечения миграционной безопасности в целом» [2].

В соответствии со статьей 2 Федерального закона от 18.07.2006 № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» «миграционный учет иностранных граждан и лиц без гражданства (далее – миграционный учет) – государственная деятельность по фиксации и обобщению предусмотренных настоящим Федеральным законом сведений об иностранных гражданах и о лицах без гражданства и о перемещениях иностранных граждан и лиц без гражданства» [3].

В соответствии с ч. 2 ст. 4 Федерального закона «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» миграционный учет иностранных граждан осуществляется в России в уведомитель-

ном порядке. Постановлением Правительства Российской Федерации от 15.01.2007 № 9 установлены правила и порядок осуществления миграционного учета [4]. В соответствии с пунктом 3 Правил иностранный гражданин для осуществления регистрации по месту жительства подает непосредственно в территориальный орган МВД России в месте нахождения жилого помещения заявление о регистрации установленной формы. Форма заявления и порядок предоставления государственной услуги по осуществлению миграционного учета установлены Приказом МВД России от 23.11.2017 № 881 [5].

Ст. 8 Федерального закона «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» установила, что «основанием для постановки на миграционный учет является:

– факт въезда иностранного гражданина в Российскую Федерацию;

– факт регистрации рождения на территории Российской Федерации иностранного гражданина или иного лица, не приобретающих на момент рождения гражданства Российской Федерации;

– факт утраты гражданства Российской Федерации лицом, находящимся в Российской Федерации» [3].

Необходимо отметить, что количество поставленных на миграционный учет иностранных граждан и лиц без гражданства ежегодно растет. Сведения приведены в таблице 2.1 [6].

Поэтому для хранения и обработки сведений, предоставляемых иностранными гражданами в процессе миграционного учета, в соответствии со ст. 10 Федерального закона «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации», создана государственная информационная система миграционного учета. ГИСМУ функционирует на основании Постановления Правительства Российской Федерации от 14.02.2007 № 94 и включает в свой состав:

Таблица 2.1.

Количество поставленных на миграционный учет иностранных граждан и лиц без гражданства в период с 2001 по 2017 годы

	2011	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
всего поставлено на миграционный учет	9 921 010	10 796 588	11 958 770	14 063 002	14 086 490	14 337 084	15 710 227
зарегистрировано по месту жительства	277 971	354 897	385 037	487 136	597 038	622 750	606 279
поставлено на учет по месту пребывания	9 643 039	10 441 691	11 573 733	13 575 866	13 489 452	13 714 334	15 103 948

– «центральный банк данных по учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации;

– автоматизированные учеты подразделений МВД России;

– банки данных об осуществлении иностранными гражданами трудовой деятельности;

– базы биометрических персональных данных, полученных МВД России;

– банки данных по учету иностранных граждан и лиц без гражданства, ходатайствующих о признании беженцами, лиц, признанных беженцами, лиц, обратившихся с заявлением о предоставлении временного убежища, лиц, получивших временное убежище, и прибывших с ними членов их семей;

– иных информационных систем, содержащих информацию об иностранных гражданах и лицах без гражданства» [7].

Оператором информационной системы является МВД России. Непосредственно работу с ГИСМУ осуществляют подразделения по вопросам миграции МВД России. Кроме них, в соответствии с совместным приказом от 02.03.2009 г., в информационном обмене участвуют МИД России, ФСБ России и ФНС России [8].

ГИСМУ введена в эксплуатацию приказом ФМС России от 26.07.2013 № 324. Государственная информационная система миграционного учета – это комплексная специализированная межведомственная автоматизированная информационная система, содержащая информацию о российских и иностранных гражданах и лицах без гражданства, обеспечивающая выполнение всех государственных задач в сфере миграции путем единообразного и контролируемого выполнения сотрудниками подразделений МВД России в сфере миграции государственных функций и предоставления государственных услуг гражданам и организациям на основе административных регламентов по направлениям деятельности с использованием информационных ресурсов других ведомств. Система предназначена для комплексной автоматизации, информационной и технологической поддержки процессов в сфере миграции в МВД России, обеспечения их информационного взаимодействия на основе единой информационно-телекоммуникационной инфраструктуры и предоставления информационно-телекоммуникационных услуг должностным, юридическим и физическим лицам.

ГИСМУ обеспечивает хранение и обработку информации о физических лицах, находившихся, находящихся и планирующих находиться на территории Российской Федерации (российских гражданах, иностранных гражданах и лицах без гражданства), юридических лицах, ходатайствующих о въезде иностранных гражданин и лиц без гражданства на территорию Российской Федерации, а также использующих иностранную рабочую силу, аналитической информации, инфраструктурной информации и электронных документов.

ГИСМУ представляет собой совокупность взаимодействующих между собой объектов (автоматизированных систем, специального программного обеспечения и соответствующих подсистем и модулей), обеспечивающих выполнение функциональных задач по отдельным направлениям деятельности

подразделений по вопросам миграции территориальных органов МВД России, объединенных по целевому назначению при оказании государственных услуг.

ГИСМУ является трехуровневой системой, включающей федеральный, региональный и территориальный уровни. На федеральном уровне в «закрытом» сегменте функционируют информационные системы, обеспечивающие:

1. Автоматизацию процессов оказания государственных услуг и исполнения государственных функций в сфере миграции:

– прикладное программное обеспечение[1] «Территория» федерального уровня;

– ППО «Территория» регионального уровня;

– специальное программное обеспечение[2] «Портал ФМС России».

2. Функционирование федеральных банков данных и информационную поддержку деятельности:

– СПО «Мигрант-1» и СПО «Российский паспорт» – хранилища информации, в том числе исторических сведений, по иностранным гражданам и российским гражданам соответственно, предназначенные для информационного взаимодействия с другими ведомствами, информационно-аналитической деятельности, выполнения поисковых запросов;

– федеральное хранилище данных ППО «Территория» федерального уровня, содержащее сведения об оказанных государственных услугах и исполненных государственных функциях с 2014 года, используемые при организации информационного взаимодействия через Систему межведомственного электронного взаимодействия[3];

– единое хранилище данных автоматизированной системы аналитической отчетности ГИСМУ – консолидированное хранилище данных об оказанных государственных услугах и исполненных государственных функциях, в том числе обезличенных, применяемых для расчета статистических форм отчетности, мониторинга миграционной ситуации, оперативного анализа ключевых показателей деятельности, моделирования и прогнозирования развития миграционной ситуации на территории Российской Федерации.

3. Межведомственное информационное взаимодействие:

– СПО «Сервисный концентратор», обеспечивающее информационное взаимодействие информационных систем ГИСМУ регионального и федерального уровней с контрагентами СМЭВ.

4. Исторические унаследованные системы:

– СПО «Сервисы сайта», обеспечивающее функционирование применяемых информационных сервисов в сфере миграции;

– СПО «ASBASE», автоматизированная информационная система «Гражданство» – используемые для хранения архивной исторической информации в соответствии с регламентными сроками хранения данных в электронном виде;

[1] Далее – ППО.
[2] Далее – СПО.
[3] Далее – СМЭВ.

– СПО «Реадмиссия», комплексы программно-технических средств «Соотечественники» и «Вынужденные переселенцы», программное средство «Компенсация», обеспечивающие работу пользователей в переходный период на использование в работе ППО «Территория» и хранение архивной исторической информации в соответствии с регламентными сроками хранения данных в электронном виде.

Для обеспечения внутреннего информационного взаимодействия компоненты ГИСМУ функционируют в составе единой вычислительной сети. В настоящий момент осуществляется интеграция ГИСМУ в состав ИСОД МВД России в качестве отдельного сервиса обеспечения оперативно-служебной деятельности единой системы информационно-аналитического обеспечения деятельности МВД России[1].

МВД России, помимо осуществления первоначального миграционного учета, также осуществляет контроль за соблюдением иностранными гражданами правил миграционного учета. Для этого, в соответствии с Приказом ФМС России № 367, МВД России № 807 от 31.07.2015 осуществляется «проведение выездных плановых, внеплановых и документарных проверок в порядке, предусмотренном Административным регламентом» [9]. Проверки осуществляются сотрудниками подразделений по вопросам миграции МВД России и участковыми уполномоченными полиции.

Пункт 9 Административного регламента установил, что «проверки проводятся в отношении следующих объектов и лиц:

– места пребывания (проживания) либо осуществления трудовой деятельности иностранных граждан;

– жилого помещения, по адресу которого осуществлена постановка иностранного гражданина на учет;

– транспортное средство, в том числе осуществляющее перевозки по маршрутам международных направлений автомобильного, железнодорожного, морского, речного, авиационного транспорта;

– иностранный гражданин, пребывающий (проживающий) в России;

– наниматель (собственник) жилого помещения, принимающая сторона, осуществившие постановку иностранного гражданина на учет;

– юридическое или физическое лицо, у которого возникают обязанности, связанные с приглашением иностранного гражданина и (или) пребыванием (проживанием) его на территории РФ;

– юридическое лицо, индивидуальный предприниматель или физическое лицо, привлекающий и использующий иностранных работников» [9].

В последние годы наблюдалось усиление ответственности за нарушение правил и порядка миграционного учета. Так, для лиц, предоставляющих мигрантам жилые помещения, и пресечения фактов незаконной миграции с 2014 года введена уголовная ответственность за фиктивную регистрацию по месту жительства и месту пребывания иностранных граждан. Федеральным законом

[1] Далее – ИСОД МВД России.

от 21.12.2013 № 376-ФЗ ст. 2 Федерального закона «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» дополнена пунктами 10 и 11, вводящими указанные понятия [10]. В Уголовный кодекс Российской Федерации введены ст. 322.2. «Фиктивная регистрация гражданина Российской Федерации по месту пребывания или по месту жительства в жилом помещении в Российской Федерации и фиктивная регистрация иностранного гражданина или лица без гражданства по месту жительства в жилом помещении в Российской Федерации» и 322.3. «Фиктивная постановка на учет иностранного гражданина или лица без гражданства по месту пребывания в жилом помещении в Российской Федерации». Статьи предусматривают уголовную ответственность за фиктивную регистрацию или постановку на учет иностранных граждан с санкцией до трех лет лишения свободы.

Также необходимо отметить, что миграционный учет позволяет выявлять случаи нарушения правил пребывания в Российской Федерации иностранного гражданина, прибывшего без визы, называемого «суммарно не более 90 суток из 180 дней подряд». Федеральный закон от 28.12.2013 № 389-ФЗ ввел для иностранных граждан, приезжающих без визы, ограничения на нахождение на территории России, если они не зарегистрировались в качестве работников по патенту, не получили разрешения на работу или временное пребывание. Это было сделано для противодействия незаконному оформлению на работу, в частности, и незаконной миграции, в целом.

Подводя итог рассмотрению современной системы централизованного учета трудовых мигрантов, можно сделать следующие выводы.

Миграционный учет осуществляется на основании заполнения иностранными гражданами миграционных карт и последующей регистрации по месту жительства или месту пребывания на основании заявления установленного образца. Персональные данные, собранные в процессе миграционного учета, хранятся в государственной информационной системе миграционного учета, оператором которой является МВД России.

Подразделения МВД России помимо осуществления первоначального миграционного учета также осуществляют контроль за соблюдением иностранными гражданами правил и сроков миграционного учета. Проверяется нахождение мигрантов по месту их пребывания или проживания, сами жилые помещения и их собственники, работодатели мигрантов, транспортные средства для их перевозки. Основные обязанности по осуществлению контроля возложены на подразделения по вопросам миграции и участковых уполномоченных полиции МВД России.

Для повышения действенности миграционного контроля в последние годы существенно повышена ответственность владельцев жилых помещений, в которых осуществляется регистрация иностранных граждан по месту пребывания или по месту жительства. Для лиц, осуществляющих фиктивную регистрацию, предусмотрена уголовная ответственность с санкцией в виде лишения свободы на срок до трех лет.

Таким образом, миграционный учет позволяет выявить лиц, которые находятся на территории России незаконно, с целью не той, которая была указа-

на в миграционной карте, с нарушением времени пребывания. Миграционный учет является основой для применения в дальнейшем к мигрантам, нарушившим законодательство, мер административного принуждения.

Можно констатировать, что миграционный учет направлен как на создание достоверной статистической картины миграционной ситуации в России, так и на противодействие нарушениям законодательства в миграционной сфере и в сфере трудовой миграции. Интеграция ГИСМУ с ИСОД МВД России позволит более полно использовать возможности информационных ресурсов бывшего ФМС России и облегчить миграционный контроль за иностранными гражданами и лицами без гражданства для сотрудников МВД России.

Библиографический список

1. Указ Президента Российской Федерации от 31.10.2018 № 622 «О Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 31.10.2018.

2. *Никитенко И.В.* Миграционный учет как основная форма государственного контроля над миграционными процессами // Российский следователь. 2009. № 7. С. 29.

3. Федеральный закон от 18.07.2006 № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» // Российская газета. 2006. 20 июля.

4. Постановление Правительства Российской Федерации от 15.01.2007 № 9 «О порядке осуществления миграционного учета иностранных граждан и лиц без гражданства в Российской Федерации» // Российская газета. 2007. 27 января.

5. Приказ МВД России от 23.11.2017 № 881 «Об утверждении Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по осуществлению миграционного учета иностранных граждан и лиц без гражданства в Российской Федерации, форм заявления о регистрации иностранного гражданина или лица без гражданства по месту жительства, уведомления о прибытии иностранного гражданина или лица без гражданства в место пребывания, отметки о регистрации иностранного гражданина или лица без гражданства по месту жительства, отметок о подтверждении выполнения принимающей стороной и иностранным гражданином действий, необходимых для его постановки на учет по месту пребывания» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 21.12.2017.

6. Сводки основных показателей деятельности по миграционной ситуации в Российской Федерации за 2011-2017 годы: Официальный сайт ГУВМ МВД России [Электронный ресурс]. – Режим доступа: https://мвд.рф/Deljatelnost-/statistics/migracionnaya/item/12162186/ (дата обращения: 09.07.2018).

7. Постановление Правительства Российской Федерации от 14.02.2007 № 94 «О государственной информационной системе миграционного учета» // Российская газета. 2007. 21 февраля.

8. Приказ ФМС РФ № 39, МВД РФ № 179, МИД РФ № 2619, Минкомсвязи РФ № 30, ФСБ РФ № 69, ФНС РФ № ММ-7-6/100 от 02.03.2009 «О Типовом соглашении об информационном обмене сведениями в государственной информационной системе миграционного учета» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. 4 мая.

9. Приказ ФМС России № 367, МВД России № 807 от 31.07.2015 «Об утверждении Административного регламента по исполнению Федеральной миграционной службой, ее территориальными органами и органами внутренних дел Российской Федерации государственной функции по осуществлению федерального государственного контроля (надзора) за пребыванием и проживанием иностранных граждан и лиц без гражданства в Российской Федерации и трудовой деятельностью иностранных работников» // Российская газета. 2015. 2 ноября.

10. Федеральный закон от 21.12.2013 № 376-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета. 2013. 25 декабря.

11. Федеральный закон от 28.12.2013 № 389-ФЗ «О внесении изменений в статью 27 Федерального закона "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию" и статью 5 Федерального закона "О правовом положении иностранных граждан в Российской Федерации"» // Российская газета. 2013. 30 декабря.

АРХИТЕКТУРА ВЗАИМОДЕЙСТВИЯ МОДУЛЕЙ ПОДСИСТЕМЫ СБОРА МОНИТОРИНГОВОЙ ИНФОРМАЦИИ О ДЕЯТЕЛЬНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

УДК 004.41

Федосеев А.Э.,
Михайликов В.Л.,
кандидат юридических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Баранов В.М.,
кандидат педагогических наук, доцент
(Белгородский государственный технологический университет им. В.Г. Шухова)

Аннотация: в данной статье освещается вопрос программно-технического исполнения информационного процесса взаимодействия модулей при сборе мониторинговой информации о деятельности в образовательной организации. Предлагаются различные модули для построения подобных систем.

Ключевые слова: мониторинг, информационные системы, модули подсистем, управления образовательной организацией, система сбора мониторинговой информации.

ARCHITECTURE OF INTERACTION OF THE MODULES OF THE SUBSYSTEM OF COLLECTING MONITORING INFORMATION ON ACTIVITIES IN THE EDUCATIONAL ORGANIZATION

Fedoseyev A.E.,
Mikhaylikov V.L.,
Candidate of Jurisprudence Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Baranov V.M.,
Candidate of Pedagogical Sciences, Associate Professor
(Belgorod state technological university of V.G. Shukhov)

Abstract: this article is devoted to the issue of software and technical execution of the information process of interaction between modules at collecting monitoring information about activities in an educational organization. Various modules are offered for building such systems.

Key words: monitoring, information systems, modules of subsystems, educational organization management, a system for collecting monitoring information.

Современные тенденции формируют новые требования в области управления образовательной организацией. Наблюдается интенсивное развитие информационных систем, построенных по принципу интеграции различных функций планирования и управления между подсистемами [1]. Управление превращается в неотъемлемую функцию жизнедеятельности общества во всех его подсистемах, структурах, в закономерность развития и формирования новых структур и функций [2]. В условиях рыночной конкуренции возросли потребительские потребности [4]. Данные факторы повлияли на постоянное развитие менеджмента качества, изменили приоритет работы образовательных организаций на удовлетворение потребностей клиентов [3]. Подобное динамическое изменение актуализировало потребности в средствах самоанализа. Статья посвящена рассмотрению задач организации и построения систем сбора мониторинговой информации о деятельности образовательной организации.

Подходы и требования при проектировании системы

Проектирование информационных систем разбивается на несколько этапов. Вначале строится иерархическая модель, которая определяет концептуальную модель предметной области, а затем – физическая модель базы данных, которая привязана к данным в виде схемы взаимодействия сущностей и атрибутов [1]. Сама информационная система является структурированной, состоящей из связей и иерархий взаимодействий [5]. Такое рассмотрение модели системы называют концептуальной [6]. Также строят модели потоков данных, последовательность процессов, организационную структуру и прочее [1]. Методика и инструментарий применения методологии для всех видов систем достаточно под-

робно отражены в ряде источников [6, 7]. Подход для построения систем для каждой образовательной организации должен быть индивидуальным, так как типовые и готовые решения не позволяют полностью сократить расходы на решение разнообразных и специфичных задач предметной области вследствие ее большой разнообразности и уникальности [1]. Однако все же можно выделить следующие условия эффективного проведения мониторинга, которые определят фундаментальные требования к системе [8, 9]:

– использование системного подхода, обеспечивающего слаженную работу механизма по сбору, обработке, анализу и интерпретаций информации;

– корректную интерпретацию данных мониторинга с учетом различных влияний и связей между показателями;

– использование качественного инструментария и современного программного обеспечения для обработки и анализа данных мониторинга.

Вышеизложенный подход построения информационной системы сбора мониторинговой информации о деятельности в образовательной организации может позволить построить в дальнейшем систему поддержки принятия решений, так как это автоматизированная система, целью которой является поддержка пользователей, принимающих решение в сложных условиях [10]. Созданная система сбора информации будет являться фундаментом для аналитического обеспечения деятельности образовательной организации.

Реализация системы сбора мониторинговой информации о деятельности в образовательной организации

При построении информационной системы мониторинга на первом этапе реализуется подсистема сбора информации. В нашем случае она состоит из модулей ввода и редактирования информации, контроля и учета. Модуль ввода и редактирования предназначен для внесения новой информации либо правки уже внесенной. Модуль контроля предполагает проверку со стороны компетентных исполнителей на соответствие введенной информации. В случае неполноты либо необходимости корректировки введенная информация возвращается на редактирование. При соответствии введенной информации она направляется в модуль учета. Модуль учета принимает информацию, считая ее достоверной для возможности дальнейшего анализа и учитывая ее при подведении итогов.

При вызове модуля ввода и редактировании информации происходит построение формы, вызывающей выбор показателя мониторинговой информации. На основе выбранного показателя вызывается шаблон формы заполнения. Шаблон формы заполнения состоит из области исполнителей, полей формы показателя и инструментальной области. Область исполнителей по определенным правилам предоставляет выставить исполнителей подразделения либо непосредственно физических лиц. Для физических лиц предоставляется градация на непосредственный выбор из списка сотрудников образовательной организации и внешних исполнителей. Для каждого исполнителя предоставляется поле для ввода процента участия в показателе, к примеру, соавторства. При добавлении происходит программная проверка на неотрицательность участия и проверки на непревышение суммы 100%. Область по-

лей формы показателя на основании выбранного показателя выстраивает форму ввода и редактирования. Происходит загрузка из базы данных наименований полей с их типом, выстраивается список выбора спадающего меню, ранжируются поля в соответствии с порядковыми весами. Инструментальная область предназначена для предоставления кнопок для выполнения определенных операций с записями. К примеру, после успешного заполнения показателя передать сведения в модуль контроля для проверки со стороны компетентных исполнителей на соответствие введенной информации. В соответствии с операцией ввода либо редактирования в последнем случае из базы данных загружаются последние внесенные данные. А инструментальная область включает кнопку удаления записи.

В работе был описан процесс сбора мониторинговой информации о деятельности в образовательной организации. Рассмотрены составляющие программно-технической реализации информационной системы сбора мониторинговой информации. Обоснованно предложены модули системы. Были представлены схемы взаимодействия в модулях.

Библиографический список

1. *Боковой Ю.В.* Особенности методологии проектирования информационных систем для малого и среднего бизнеса // Прикладная информатика. 2006. № 5. С. 3-11.

2. *Елкин С.Е.* Процессный подход к проектированию системы управления организационными изменениями // Сибирский торгово-экономический журнал. 2012. № 16. С. 19-23.

3. *Попова Л.Ф.* Организационные аспекты совершенствования системы управления качеством на предприятии // Вестник Саратовского государственного социально-экономического университета. 2016. № 5 (64). С. 38-42.

4. *Игнатова Г.В.* Факторы повышения глобальной конкурентоспособности Российской Федерации в условиях внешних вызовов // Экономические, институциональные и технологические проблемы повышения конкурентоспособности национальной экономики в условиях внешних вызовов: мат. Междунар. науч.-практ. конф. / под ред. д-ра экон. наук, проф. А.А. Сытника. – Саратов: ССЭИ РЭУ им. Г.В. Плеханова, 2015. С. 90-91.

5. *Иванилов Э.Б.* Процессный подход в организационном проектировании // Вестник Саратовского государственного технического университета. 2010. № 1. Т. 3. С. 242-246.

6. *Черемных С.В., Семенов И.О., Ручкин В.С.* Структурный анализ систем: IDEF-технологии – Москва: Финансы и статистика, 2003. – 208 с.

7. *Марка Д.А., Клемент Л. МакГоуэн.* Методология структурного анализа и проектирования / предисл. Д.Т. Росса; пер. с англ. – Москва: Мета Технология, 1993. – 240 с.

8. *Звонников В.И., Челышкова М.Б.* Современные средства оценивания результатов обучения. – Москва: Академия, 2011. – 224 с.

9. *Фомин Н.В.* Концептуальные основы проектирования новых систем контроля и оценивания результатов образования // Вестник БГУ. 2013. № 1. С. 63-67.
10. *Терелянский П.В.* Системы поддержки принятия решений. Опыт проектирования: монография. – ВолгГТУ: Волгоград, 2009. – 127 с.

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ РАЗВИТИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

УДК 004

Акапьев В.Л.,
кандидат педагогических наук;
Гуржий А.А.,
Савотченко С.Е.,
доктор физико-математических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: рассмотрены аспекты применения перспективных информационных технологий в условиях развития электронного правительства. Проанализированы данные Росстата по мониторингу качества предоставления государственных и муниципальных услуг в электронной форме за последние годы. Выявлена необходимость создания условий для перехода к новой модели управления, основанной на «цифровой экономике». Показано, что для повышения качества работы системы управления электронным правительством следует усовершенствовать информационное обеспечение электронного правительства.

Ключевые слова: информационные ресурсы, информационная безопасность, информационные системы, электронное правительство.

INFORMATION AND TECHNOLOGICAL PROBLEMS OF E-GOVERNMENT DEVELOPMENT

Akapev V.L.,
Candidate of Pedaqoqical Sciences;
Gurzhiy A.A.,
Savotchenko S.E.
Doctor of Physical and Mathematical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the aspects of application of perspective information technologies in conditions of development of electronic government are considered. The data of Rosstat on monitoring the quality of providing state and municipal services in electronic form in recent years are analyzed. The need to create conditions for the transi-

tion from the government's industrial model to a new management model based on the «digital economy» has been identified. It is shown that for the effective functioning of the management system of the electronic government, it is necessary to improve the mechanism of information support for the implementation of e-government projects.

Key words: information resources, information security, information systems, e-government.

Концепция электронного правительства (в зарубежных странах – «E-government») получила свое развитие в течение последнего десятилетия. После окончания федеральной целевой программы «Электронная Россия (2002-2010 года)», реализованной не в полной мере, возникла необходимость формирования и принятия новой Государственной программы «Информационное общество (2011-2020 гг.)», одной из основных задач стало развитие концепции электронного правительства (ЭП), где и была обозначена необходимость перехода органов власти различных уровней на предоставление государственных услуг в электронной форме [1].

В связи с малым временем развития она еще не достаточно изучена, поэтому фундаментальных научных трудов о формировании электронного правительства крайне мало. Рассмотрение данной темы нашло отражение в зарубежной и отечественной периодической литературе [2-6].

Целью данной работы является моделирование возможности применения перспективных информационных технологий в условиях развития электронного правительства.

Эффективность в сфере формирования полноценного ЭП в России определяется в первую очередь от участия граждан и представителей бизнес-сообщества. Здесь отмечаются две основные трудности, тормозящие развитие гражданского участия в формировании ЭП: 1) обеспечение безпроблемного доступа к технологиям, 2) обеспечение оперативного доступа к информации.

В то же время ведомственные системы электронного документооборота часто не обеспечивают юридически значимый обмен документами, а обеспеченность государственных и муниципальных служащих сертификатами ключей проверки электронных подписей сохраняется на низком уровне. Доступ к широкополосному интернету низкий.

По данным Росстата [7] использование компьютерной техники и широкополосного доступа к сети Интернет в органах власти субъектов Российской Федерации, местного самоуправления, остается сравнительно низким, особенно в малонаселенных и удаленных районах.

Несмотря на значительные расходы, по данным мониторинга качества предоставления государственных и муниципальных услуг в электронной форме за 2013 год, проведенного Министерством экономического развития Российской Федерации, формы получения указанных услуг в федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» реализованы менее чем для 5,5 тыс. государственных и муниципальных услуг (что составляет 5 процентов общего ко-

личества услуг органов государственной власти субъектов Российской Федерации, размещенных на Едином портале), при этом значительная их часть неработоспособна, что приводит к невозможности дистанционного получения гражданами государственных и муниципальных услуг.

По состоянию на начало 2014 года 40 процентов региональных порталов государственных и муниципальных услуг (далее – региональные порталы) используют системы регистрации и авторизации, несовместимые с федеральной государственной информационной системой «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» [8], что приводит к невозможности для граждан использовать одну учетную запись для получения государственных и муниципальных услуг на разных порталах [9].

Помимо этого наблюдается высокая отраслевая и региональная дифференциация. Планировалась, что наша страна сможет попасть в первую десятку стран Международного рейтинга по уровню информационных технологий, но Россия вышла на 38-е место из 155 возможных [10].

Официальные сайты органов государственного управления благодаря бурному развитию телекоммуникационных и компьютерных средств сделали информационные мероприятия эффективным способом реализации своего взаимодействия с населением. Также следует отметить, что такой способ является самым экономичным и быстрым касаемо распространения информации о деятельности государственных органов и органов местного самоуправления, а также информирования общественности об официальной позиции государства [11]. Повсеместное использование органами власти своих официальных сайтов призвано обеспечить гражданам и организациям, независимо от мест проживания и расположения, равный доступ к информации о деятельности государственных органов и органов местного самоуправления.

Федеральный закон от 09.02.2010 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» должен играть роль наиболее эффективного средства для повышения эффективности и оперативности доступа к информации о деятельности органов государственной власти. Кроме того, должны быть приняты соответствующие подзаконные нормативно-правовые акты, регулирующие отношения в сфере официальной информации и организации доступа к ней.

Наибольшие трудности, касающиеся открытости и доступа к официальной информации, теперь будут относиться к вопросам технического обеспечения. Оперативное и качественное обновление содержания информации самих официальных сайтов органов государственной и муниципальной власти теперь не представляет особых проблем.

В результате мы можем утверждать, что процесс формирования полноценного электронного правительства давно начат. Первоначальные этапы в направлении обозначения присутствия в сети Интернет органов власти и информации об их деятельности давно и успешно пройдены. Теперь следует ак-

центировать внимание на формировании условий для перехода от классической модели взаимосвязи правительства с населением (которую иногда называют индустриальной моделью) к новой модели, базирующейся на самоорганизующихся межинституциональных структурах взаимодействия, позволяющих оперативно обмениваться информацией и функционирующих в рамках «цифровой экономики».

Полномочия по формированию государственной политики не следует оставлять одной организации, поскольку ни политические деятели, ни государственные служащие не должны единолично отвечать за разработку стратегий. Эффективность дальнейшего функционирования ЭП в рамках развивающегося информационного общества зависит от тесноты взаимодействия официальных представителей государственной власти и всех заинтересованных сторон: бизнеса, образовательных и исследовательских институтов, общественных групп, гражданских организаций.

В заключение следует отметить следующее. Для качественной работы ЭП следует развивать и модернизировать совершенствование средств его информационного обеспечения.

Электронное правительство не является дополнением или аналогом традиционного правительства, а лишь определяет новый способ взаимодействия на основе активного использования ИКТ для увеличения качества предоставляемых государственных услуг в электронной форме.

На наш взгляд, в будущем следует больше усилий сосредоточить на развитии «цифровой» экономики информационного общества в целом, чем на развитии ЭП в отдельности. Существенную роль следует отвести в таких процессах снижению различия между уровнями компьютеризации и информатизации, определяющими развитие информационного общества, а также доступности ИКТ в различных регионах России.

Библиографический список

1. *Борисова А.С.* Совершенствование информационного обеспечения реализации проектов электронного правительства регионов: дис. ... канд. экон. наук. – Волгоград, 2014. – 270 с.

2. *Belanger F., Carter L.D., Schaupp L.C.* U-government: a framework for the evolution of e- government // Electronic Government, an International Journal. 2005. № 2(4). P. 426-445.

3. *Целищева Е.Ф.* От электронного правительства к электронному государству // Экономика, государство, общество. 2011. № 2 (6). С. 19-22.

4. *Морозов А.В., Полякова Т.А., Филатова Л.В.* Этапы и проблемы формирования единого информационно-правового пространства России // Информационное право. 2012. № 1. С. 3-6.

5. *Антонов Я.В.* Конституционно-правовые перспективы развития электронной демократии в современной России // Конституционное и муниципальное право. 2016. № 9. С. 54-62.

6. *Архипова З.В.* Трансформация «электронного правительства» в «цифровое правительство» // Известия Байкальского государственного университета. 2016. Т. 26. № 5. С. 818-824.

7. Интернет в России и в мире [Электронный ресурс]. – Режим доступа: http://www.bizhit.ru/index/users_count/0-151.

8. *Талапина Э.В.* Модернизация государственного управления в информационном обществе: информационно-правовое исследование: автореф. дис. ... д-ра юрид. наук. – Москва, 2015. – 54 с.

1. Статистика использования ИКТ в госсекторе России [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Статистика_использования_ИКТ_в_госсекторе_России.

2. Рейтинг стран по уровню информационных технологий [Электронный ресурс]. – Режим доступа: http://basetop.ru/reyting-stran-po-urovnyu-informatsionnyih-tehnologiy/Топ Рейтинги Мира.

3. Национальный доклад о доступе к информации о деятельности органов власти в Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.svobodainfo.org/info/page/rus?tid=633200175.

МОБИЛЬНЫЕ СРЕДСТВА СВЯЗИ КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ И ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ГРАЖДАН

УДК343.791

Свистильников А.Б.,
кандидат юридических наук, доцент;
Моисеев Н.А.,
кандидат юридических наук, доцент;
Новоселов Н.Г.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются вопросы получения информации, содержащейся в сотовом телефоне при расследовании различных категорий уголовных дел. Ведется речь о двух способах ее получения (дистанционном и непосредственном). Исследуется порядок получения и содержание информации о детализации телефонных соединений, местонахождении абонентского устройства. Приводятся теоретические и практические аспекты получения информации, хранящейся в памяти телефона или sim-карты.

Ключевые слова: телефон, сотовый телефон, sim-карта, связь, мобильные устройства.

MOBILE COMMUNICATION FACILITIES AS A SOURCE OF EVIDENT INFORMATION AT THE DISCLOSURE OF CRIMES AND SECURITY OF CITIZENS

Svistilnikov A.B.,
Candidate of Jurisprudence Sciences, Associate Professor;
Moiseev N.A.,
Candidate of Jurisprudence Sciences, Associate Professor;
Novoselov N.G.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article deals with the issues of obtaining information, contained in a cell phone while investigating various categories of criminal cases. We are talking about two ways to get it (remote and direct). The order of reception and the maintenance of the information on detailed elaboration of telephone connections, a site of the user's device is investigated. Theoretical and practical aspects of obtaining information stored in the phone or sim-card memory are given.

Key words: phone, mobile phone, sim-card, communication, mobile devices.

На современном этапе развития общества обеспечению безопасности личности от различных видов угроз уделяется значительное внимание. Одной из таковых угроз является информационная сфера. Достижения в области радиоэлектроники, средств связи и компьютерной техники коренным образом изменили существующие информационные технологии: не только предоставили гражданам и юридическим лицам невиданные возможности в сфере коммуникации, но и явились системообразующим фактором нарастающих угроз правам и интересам субъектов информационного взаимодействия.

Одним из таковых видов технических средств, наиболее часто используемых в преступных целях, являются мобильные устройства сотовой связи (смартфоны, сотовые телефоны, планшетные компьютеры и др.). Россияне приобретают мобильные телефоны и иные гаджеты в огромных количествах. В 2017 году только на одном из самых популярных в России сайтов «Avito» было продано 1,6 млн телефонов. Подкатегория «Телефоны» стала лидирующей в разделе «Бытовая электроника» и доля от общего спроса составила около 50%. Кроме этого спросом пользуются и sim-карты. Численность населения в Российской Федерации составляет около 140 млн человек. С 2008 года российские операторы сотовой связи суммарно продали 1,1 млрд sim-карт, а общее число абонентов сотовой связи в стране составляет чуть более 250 млн.

Рассматриваемые технические средства могут выступать как объектами, в отношении которых совершаются преступления, так и средствами совершения этих криминальных деяний (наиболее часто фиксируют: телефонные мошенничества всех видов [2, с. 75-78], бесконтактный сбыт психоактивных веществ и др.).

В последнем случае они могут выступать носителями криминалистически значимой информации, позволяющей выявлять лиц, причастных к совершению преступлений. А зафиксированная на носителях информация в дальнейшем может использоваться в качестве доказательств при расследовании уголовных дел. Так, на территории Белгородской области в 2017 году было зарегистрировано 719 преступлений, где предметом преступного посягательства являлся мобильный телефон, а из числа раскрытых преступлений – 412 совершено с использованием средств сотовой связи [5, с. 78-83].

Современный сотовый телефон представляет собой многофункциональное, универсальное устройство, включающее в себя функции телефона, записной книжки, фотоаппарата, диктофона, видеокамеры, компьютера и иных возможностей. При таком разнообразии функций сотовый телефон становится источником информации, которую можно использовать как при документировании преступлений, так и при расследовании уголовных дел [1].

Бесспорно, получение и анализ такой информации позволит сделать вывод о причастности лиц к конкретному преступлению, совершении ими аналогичных преступлений в определенный период времени, установить их связи, места сбыта похищенного и т.д. [8, с. 108-112].

Подобную информацию можно получить двумя способами:

1. Дистанционно.

2. Непосредственно при наличии мобильного телефона.

Рассматривая первый способ получения информации, отметим, что она осуществляется на основании Федерального закона Российской Федерации «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ путем проведения оперативно-разыскных мероприятий (далее – ОРМ) либо следственных действий в рамках расследуемых уголовных дел. В любом случае необходимо получение судебного решения по конкретному номеру абонента или по IMEI-номеру телефона.

В рамках расследования уголовных дел у операторов сотовой связи запрашивается следующая информация:

– о лице, на чье имя зарегистрированы указанные абонентские номера;

– об электронных (IMEI) номерах абонентских устройств (сотовых телефонов), работавших с sim-картами;

– о других sim-картах, работавших в указанный период времени с установленным абонентским устройством (сотовым телефоном);

– о детализации соединений данных номеров с иными номерами, с указанием адресов расположения базовых станций.

При этом отметим, что получение детализации соединений возможно при проведении следственного действия [4] «получение информации о соединениях между абонентами и (или) абонентскими устройствами» [3] или ОРМ «наведение справок». В отдельных регионах России получение данной информации осуществляется путем проведения ОРМ «снятие информации с технических каналов связи», что принципиально неверно. Контроль технических каналов связи подразумевает осуществление контроля за определенными про-

цессами с помощью специальных технических средств. Наведение справок же предполагает сбор уже имеющихся сведений, содержащихся в базах данных.

Учитывая, что вышеуказанная информация уже содержится в базах данных операторов сотовой связи, значит, это информация об уже состоявшихся в прошлом соединениях. Для получения детализации о соединениях необходимо проводить ОРМ «наведение справок». На это обращала внимание Генеральная прокуратура России, которая еще 19 марта 1999 года в своем письме разъяснила, что получение информации об абонентах и оказание услуг связи следует рассматривать как «наведение справок».

Немаловажным для сотрудников полиции является определение местонахождения абонентского устройства. При нахождении абонента в радиусе действия сотовой сети возможно определение местонахождения абонента. Точность определения местонахождения зависит от многих причин: рельефа местности, наличия зданий, сооружений, расположения базовых станций, количества работающих в данный момент телефонов. Однако для получения подобных данных необходимо, чтобы абонент задействовал свой телефон в режиме приема либо передачи. В таком случае информация может быть получена у оператора сотовой связи и приобщена к материалам уголовного дела. Так, 22.10.2017 в 15.00 в подсобном помещении магазина «Калинка» г. Белгорода был обнаружен труп продавца – гр-ки Ч. – с множественными ножевыми ранениями, при этом у жертвы был похищен сотовый телефон. В ходе проведения ОРМ и на основании анализа данных базовых станций одного из операторов сотовой связи удалось установить местонахождение похищенного телефона в одном из районов области. В ходе поисковых мероприятий сотрудниками уголовного розыска преступник был установлен и задержан. Им оказался 33-летний гражданин Украины, не имеющий определенного места жительства.

Рассматривая получение интересующей информации непосредственно из мобильного телефона, отметим, что в нем могут быть зафиксированы следующие данные:

– контакты (ФИО, абонентские номера, адреса, иная информация в зависимости от модели телефона);

– о входящих и исходящих соединениях, с кем они осуществлялись, дате, времени и длительности разговора;

– текстовые сообщения с данными адресатов, датой, временем отправки или получения;

– фотоснимки;

– видеозаписи;

– звукозаписи;

– любые иные данные при наличии достаточного объема встроенной либо сменной флеш-памяти/карты и др.

Для правоохранительных органов могут представлять интерес компоненты сотового телефона, которые целесообразно также исследовать. При этом отметим, что структура меню у разных моделей телефонов различна и

для полного изучения и использования информации, находящейся в сотовом телефоне, следует осматривать его с обязательным привлечением специалиста.

При исследовании sms-сообщений необходимо помнить, что в ряде телефонов (устаревших моделей) хранение sms осуществляется в энергозависимой памяти, т.е. при отсоединении аккумуляторной батарей часть sms-сообщений либо все они могут быть безвозвратно утрачены. Аналогичная ситуация складывается со списками вызовов – при отключении аккумуляторной батареи списки либо теряются полностью, либо сохраняются только набранные номера, либо теряются данные о дате, времени и продолжительности звонков. Таким образом, следует помнить, что отключение аккумуляторной батареи может повлечь необратимую потерю информации. Поскольку извлечение аккумуляторной батареи необходимо для прочтения индивидуального номера сотового телефона (IMEI), сотруднику органов внутренних дел для его получения достаточно набрать на клавиатуре телефона комбинацию *#06# и нажать кнопку посыла вызова, после чего на экране телефона высветится 15-значный буквенно-цифровой код IMEI[1].

Специалисты в сфере ЭВМ имеют возможность программными средствами изменить IMEI («перепрошить» телефон), поэтому после осмотра, извлечения и сохранения всех интересующих данных следует сравнить полученный номер с номером, нанесенным внутри корпуса телефона.

При осмотре встроенной флеш-памяти, а также сменных карт памяти необходимо учитывать, что фактически данные объекты являются аналогами жестких дисков компьютера, и на них возможно хранение любых типов файлов – от фотографий и музыкальных файлов до скрытых текстовых и архивных файлов. При этом обнаружение скрытых данных на носителе возможно как по косвенным данным (различие в количестве общей, свободной и использованной памяти на носителе), так и с применением специальных познаний, программ и оборудования.

При расследовании уголовного дела или проведении оперативно-разыскных мероприятий сотрудник органов внутренних дел, исходя из обстоятельств совершенного преступления, целей и задач расследования, самостоятельно принимает решение о содержании и объеме информации, которая должна быть получена из мобильного устройства. Получить ее можно при проведении информационно-компьютерного исследования или компьютерной экспертизы средств мобильной связи (мобильного телефона, смартфона, планшетного компьютера).

В заключение отметим, что современные технические средства позволяют сотрудникам правоохранительных органов получить с мобильного телефона следующую информацию:

[1] IMEI – это собственный идентификационный номер для каждого телефона. Первые шесть цифр означают код модели телефона, седьмая и восьмая – страну-изготовителя, с девятой по четырнадцатую серийный номер телефона. Последняя цифра в IMEI-номере является проверочной и вычисляется на основе предыдущих 14 цифр (по алгоритму Луна).

1. Данные о сохраненных и удаленных текстах (sms) (например переписки между подозреваемым и потерпевшим, подозреваемым и его сообщником), иных текстовых документах, номеров из «абонентской» книжки, последних входящих и исходящих вызовах, фото-, видеофайлах прямо или косвенно указывающих на причастность пользователя устройства к использованию информации, сопряженной с рассматриваемыми преступлениями.

2. Наличие информации в памяти мобильного телефона об осуществлении сеансов доступа к сети Интернет за конкретный интересующий период времени.

3. Информацию об учетных данных, использовавшихся для выхода в сеть Интернет, а также файлах, в которых содержатся сведения о применяемых логинах и паролях.

4. Наличие в памяти мобильного устройства программного обеспечения, позволяющего без уведомления пользователя совершать какие-либо действия, передавать определенную информацию, а также выяснить, куда она передавалась.

5. Наличие информации о поиске через установленный на устройстве интернет-браузер (Opera, Google Chrome, Internet Explorer, Safarii пр.) сведений, имеющих отношение к факту совершенного преступления. Например, к существующим вредоносным программам, позволяющим совершать хищения денежных средств со счетов и банковских карт, способов распространения таких программ. Кроме того, могут быть обнаружены конкретные инструкции, позволяющие завладеть денежными средствами, носящие обучающий характер, в которых отражены последовательность действий преступников, заготовки диалогов, шаблоны sms-сообщений, которые необходимо использовать при разговоре с потерпевшим (при sms-общении).

6. Наличие установленных программ, предназначенных для мгновенной пересылки сообщений, например, ICQ (айсикью), а также переписки (чатов) в этих программах, а также программ, позволяющих осуществлять видеосвязь, например, Skype (скайп), в файлах истории которых могут содержаться также переданные текстовые сообщения [8, с. 108-112].

7. Информацию об использовании соответствующих интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки) [7, с. 103-107].

8. Сведения о регистрации в качестве пользователя в социальных сетях, на Интернет-ресурсах (форумах), в том числе внутренних сетевых ресурсах Интернет-провайдеров, на которых осуществляется обсуждение (обмен информацией), демонстрация, распространение и создание вредоносного программного обеспечения.

9. Информацию, подтверждающую регистрацию подозреваемого в качестве пользователя в локальной сети, организованной интернет-провайдером, локальной папке пользователя, где также может содержаться значимая информация.

С учетом вышеизложенного отметим, что в условиях прогрессирующих информационных угроз полиции необходимо обеспечить гражданам высокий уровень безопасности. Для этого сотрудники правоохранительных органов должны уметь грамотно документировать информацию криминального характера, содержащуюся в мобильных средствах связи.

Библиографический список

1. *Бабакова М.А.* Проблемы розыска при расследовании преступлений в сфере высоких технологий: автореф. дис. ... канд. юрид. наук. – Саратов, 2010. – 24 с.

2. *Лабутин А.А.* Характерные черты личности преступника, совершающего мошенничество с использованием средств сотовой связи (по материалам субъектов Приволжского федерального округа // Вестник Казанского юридического института МВД России. 2018. № 1 (31). С. 75-78.

3. *Муженская Н.Е., Костылева Г.В.* Руководство для следователя и дознавателя по расследованию отдельных видов преступлений: в 2-х ч. – Москва: Проспект, 2013.

4. *Цыкора А.А.* Тактико-криминалистические особенности производства следственных действий, связанных с получением и исследованием информации, передаваемой по техническим каналам связи: автореф. дис. ... канд. юрид. наук. – Ростов-на-Дону, 2013. – 25 с.

5. *Свистильников А.Б.* Некоторые вопросы терминологии и определений, используемых при раскрытии преступлений, совершаемых с помощью телекоммуникационных сетей // Ғылым – Наука (Международный научный журнал). Костанайская академия МВД Республики Казахстан. 2018. № 2 (57). С. 78-83.

6. *Свистильников А.Б., Дьяков Н.В.* Первоначальный этап раскрытия краж грузов как алгоритм деятельности транспортной полиции по обеспечению сохранности и безопасности грузов, перевозимых железнодорожным транспортом // Вестник ГБУ «НЦ БЖД». 2018. № 2 (36). С. 113-117.

7. *Свистильников А.Б., Чиненов А.В.* К вопросу обеспечения безопасности кредитно-финансовой системы России от фальшивомонетничества // Вестник ГБУ «НЦ БЖД». 2017. № 4 (34). С. 103-107.

8. *Свистильников А.Б.* Использование автоматизированных информационно-поисковых систем в идентификации личности террориста и предупреждении террористических актов на объектах транспорта // Проблемы правоохранительной деятельности. 2016. №. 2. С. 108-112.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРАВА ПОДОЗРЕВАЕМОГО НА ОДИН ТЕЛЕФОННЫЙ РАЗГОВОР

УДК 343.1

Жукова П.Н.,
доктор физико-математических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Золотухина Н.В.,
кандидат юридических наук
(Военный университет Министерства обороны)

Аннотация: в статье рассмотрены проблемные вопросы, связанные с реализацией права подозреваемого на один телефонный звонок.
Ключевые слова: подозреваемый, право на звонок, задержание.

THE PROBLEMS OF REALIZATION THE RIGHTS OF THE SUSPECT TO ONE PHONE CALL

Zhukova P.N.,
Doctor of Physical and Mathematical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Zolotukhina N.V.,
Candidate of Jurisprudence Sciences
(Higher Education Military University of the Ministry of Defense)

Abstract: the article considers the questions of the problems of realization the rights of the suspect to one phone call.
Key words: the suspect, right to call, detention.

Среди поправок, внесших существенный вклад в изменение ряда статей Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) и вступивших в силу в 2016 г., по мнению авторов, наиболее значимыми оказались изменения ст.ст. 46 и 96 УПК РФ[1].

Изменениям подверглась ч. 3 ст. 46 УПК РФ, ранее регламентировавшая обязанность следователя или дознавателя уведомлять близких родственников подозреваемого, а при отсутствии таковых – любых родственников в случае задержания подозреваемого по основаниям и в порядке ст.ст. 91, 92 УПК РФ.

[1] Федеральный закон от 30.12.2015 № 437-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2016. № 1.

Действующая редакция ч. 3 ст. 46 УПК РФ предоставляет задержанному подозреваемому право на один телефонный разговор обязательно в присутствии дознавателя, следователя (разговор должен проходить на русском языке) для оповещения о своем задержании и месте нахождения.

Новой редакцией закона[1] установлено, что подозреваемый в кратчайший срок, но не позднее 3 часов с момента его доставления в орган дознания или к следователю имеет право на один телефонный разговор с отметкой в протоколе задержания. В случае отказа подозреваемого от права на телефонный разговор или невозможности в силу его физических или психических недостатков самостоятельно осуществлять указанное право такое уведомление производится дознавателем, следователем, о чем также делается отметка в протоколе задержания[2].

Считаем необходимым отметить, что аналогичная норма, закрепленная в уголовно-процессуальном законодательстве зарубежных стран, является естественным правом задержанного, наряду со звонком защитнику и разъяснением прав задержанного сотрудником правоохранительных органов. В России долгое время не уделялось достаточное внимание данному вопросу, и после введения данной нормы в российское законодательство появилось больше количество вопросов, касающихся ее реализации.

Основываясь на правоприменительном опыте зарубежных стран, российский законодатель внес соответствующие изменения, которые, несомненно, имеют определенные гуманистические взгляды[3], а именно оповещение родственников задержанных, поскольку существовавший ранее механизм оповещения родственников подозреваемого со стороны правоохранительных органов зачастую сопровождался заявлениями о пропаже человека. Важно подчеркнуть, что ранее УПК РФ не содержал никаких норм, регламентирующих данное положение, обязывая дознавателя или следователя оповестить родственников в течение 12 часов с момента фактического задержания[4].

Необходимо отметить, что совершенствование юридической техники являлось не единственным положительным моментом в изменениях, рассматриваемых статей. Было устранено разногласие, существовавшее с февраля 2011 г., когда был принят Федеральный закон «О полиции»[5].

Задержанное лицо в кратчайший срок, но не позднее 3-х часов с момента задержания, если иное не установлено уголовно-процессуальным законодательством Российской Федерации, имеет право на один телефонный разговор в целях уведомления близких родственников или близких лиц о своем задержа-

---

[1] Федеральный закон от 30.12.2015 № 437-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2016. № 1.

[2] Ст. 96 УПК РФ.

[3] *Безлепкин Б.Т.* Комментарий к Уголовно-процессуальному кодексу Российской Федерации. – Москва: Проспект, 2015. С. 63.

[4] В редакции Федерального закона от 05.06.2007 № 87-ФЗ.

[5] Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 13.07.2015, с изм. от 14.12.2015) «О полиции» // Российская газета. 2011. № 25.

нии и месте нахождения. Такое уведомление по просьбе задержанного лица может сделать сотрудник полиции[1].

Анализируя данную норму, обратим внимание на то, что гражданину предоставляется право именно на «один телефонный разговор», а не на «один телефонный звонок» и, в связи с этим, возможно возникновение проблемы у следователя или дознавателя при обеспечении права подозреваемого на телефонный разговор, т.е. предоставить средство связи задержанному лицу для установления непосредственного соединения абонентов и разговора между ними.

Проблема видится в понятии формулировки «предоставляется право на один телефонный звонок», буквальное толкование нормы может позволить, в результате реализации рассматриваемого права, ограничить количество попыток дозвониться подозреваемому до абонента, т.е. фактический разговор может не состояться.

Изменения коснулись и перечня субъектов, которых может оповестить задержанный, а именно, добавлены «близкие лица». Также отсутствует условие об оповещении близких лиц только при «отсутствии близких и иных родственников», таким образом, перечень субъектов стал практически неограниченным[2], например, сожитель (п. 3 ст. 15 УПК РФ).

Кроме того, важным является сохранение обязанности следователя оповещения близких о задержании и местонахождении подозреваемого в случае отказа или физико-психологической невозможности оповещения самим задержанным (ч. 1 ст. 96 УПК РФ в ред. Федерального закона от 30.12.2015 № 437-ФЗ). Указанное в обязательном порядке должно быть отражено в протоколе задержания подозреваемого.

Еще одним проблемным вопросом является исключение дознавателя из числа лиц, к которым может быть доставлено задержанное лицо (ч. 1 ст. 92 УПК РФ), хотя в ст. 46 УПК РФ указано, что телефонный разговор осуществляется в присутствии «дознавателя или следователя».

Таким образом, считаем, что в целях формирования однозначного толкования момента исчисления срока уведомления о задержании подозреваемого следует руководствоваться ч. 1 ст. 91 УПК РФ, в которой в качестве субъектов, полномочных задерживать лицо по подозрению в совершении преступления, определены «орган дознания, дознаватель, следователь». Они же являются должностными лицами, на которых возлагается обязанность по обеспечению права подозреваемого на телефонный разговор с целью уведомления о задержании.

Одним из важных элементов установленного законом порядка производства по уголовным делам являются процессуальные сроки. Поэтому, помимо прочего, вызывает осложнение привязка к временному промежутку уведомления близких о задержании «в кратчайший срок, но не позднее 3 часов» к моменту доставления подозреваемого к следователю или в орган дознания

[1] Ч. 7 ст. 14 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции».

[2] Принцип 16 Свода принципов защиты всех лиц, подвергающихся задержанию или заключению, утвержденного Резолюцией Генеральной Ассамблеи ООН от 09.12.1988.

(ст. 96 УПК РФ). Законом не определено, в каком документе фиксируется момент доставления, с которого должен исчисляться срок уведомления близкого, что осложняет возможность проверить соблюдение установленного срока. Ранее, до введения упомянутого положения в УПК РФ, срок уведомления исчислялся с момента задержания, который отражался в протоколе.

Следует различать фактическое и уголовно-процессуальное (юридическое) задержание. Фактическое – означает физическое, принудительное ограничение личной свободы того или иного лица, ограничение свободы его передвижения и принудительное доставление в правоохранительный орган (п. 15 ст. 5 УПК РФ). Подобное задержание может иметь место, в том числе и за совершение дисциплинарного проступка, в целях составления протокола об административном правонарушении, выяснения личности и т.п. Предусмотренный 48-часовой срок задержания начинает истекать с момента фактического задержания. Уголовно-процессуальное задержание означает факт уголовного преследования в отношении конкретно определенного лица, удостоверенное процессуальным решением в виде постановления о задержании. Именно с этого момента лицо может стать подозреваемым.

В целях устранения ошибок, возникающих в практических органах при решении вопроса об исчислении срока задержания, необходимо на законодательном уровне, в нормах действующего уголовно-процессуального законодательства закрепить положения о том, что решение о задержании следует оформлять в виде постановления о задержании, а также следует указать, что момент фактического ограничения свободы передвижения лица возникает у органа, производящего задержание только после вынесения и ознакомления задержанного лица с постановлением о задержании. И с этого момента следует начинать отсчет времени в рамках реализации права на телефонный разговор.

Дальнейшее изучение рассматриваемой нормы «права на телефонный разговор» позволяет выявить некоторые проблемы реализации, в том числе, усомниться в соблюдении конституционных положений при реализации этой нормы.

Задержанному иностранному гражданину должно быть разъяснено его право связаться со своим консульством или посольством[1]. Посольство или консульство уведомляется через МИД.

Анализ нормы выявил несколько неурегулированных проблем, которые возникают в системной взаимосвязи с другими нормативными правовыми актами. В первую очередь, законодатель проигнорировал вопрос о том, каким образом должно данное нововведение реализовываться, если подозреваемый не владеет русским языком.

По смыслу анализируемой статьи следует, что в подобной ситуации лицо не может воспользоваться указанным правом на телефонный звонок, т.к. не владеет русским языком. Очевидно, что в этом случае ему должен быть предостав-

[1] Принцип 16 Свода принципов защиты всех лиц, подвергающихся задержанию или заключению, утвержденного Резолюцией Генеральной Ассамблеи ООН от 09.12.1988.

лен переводчик. Право на переводчика закреплено в ч. 2 ст. 18 УПК РФ, а порядок предоставления переводчика регламентирован ст.ст. 169 и 263 УПК РФ. При этом, ни в одной из указанных норм не предусмотрено участие переводчика с момента задержания или при реализации права на телефонный разговор.

Таким образом, законодатель лишает возможности подозреваемого, не владеющего языком уголовного судопроизводства, использовать иной язык для одного телефонного разговора, который ему должен быть предоставлен в силу ч. 3 ст. 46 УПК РФ. Это положение позволяет усомниться в возможности реализации положений ст. 19 Конституции Российской Федерации, гарантирующих равенство прав и свобод человека и гражданина независимо от каких-либо условий [2].

Следует отметить что ч. 5 ст. 14 Закона «О полиции» предусматривает возможность для задержанного лица пользоваться в соответствии с федеральным законом услугами адвоката (защитника) и переводчика с момента задержания [3]. В указанном случае отсутствует уточнение о необходимости разговора исключительно на русском языке, но в то же время имеет место отсылка к нормам УПК РФ, которые устанавливают такое требование. Положения Закона «О полиции» куда более четко регламентируют возможность лица воспользоваться своим правом на один телефонный разговор, т.к. предоставляют задержанному лицу право воспользоваться помощью переводчика с момента фактического задержания, следовательно, и телефонный разговор, как предполагается исходя из анализа норм действующего законодательства, может быть осуществлен с участием переводчика. В то же время уголовно-процессуальное законодательство не содержит такой оговорки [6].

В связи с этим не владеющие русским языком находятся в менее выгодном положении по отношению к лицам, владеющим русским языком.

Интересный вопрос возникает, если учесть, что родственники подозреваемого также могут не владеть русским языком. Решение этой проблемы также требует внимание законодателя.

В конце работы хотелось бы отметить еще одну проблему, которая носит скорее технический характер, а именно: установленное право о сообщении своего местонахождения предоставляется только посредством телефонного разговора. Но современное развитие средств связи подразумевает использование различных приложений, в том числе интернет-ресурсов.

Таким образом, по-нашему мнению, необходимо внести дополнения в ст. 46 и 96 УПК РФ, касающиеся использования мобильных приложений и видеосвязи.

Таким образом, для реализации права на телефонный разговор необходимо разрешить несколько вопросов:

– определить право участия переводчика в процессе телефонного разговора, если таким правом решило воспользоваться лицо, не владеющее языком уголовного судопроизводства;

– расширить круг возможностей дознавателя, предоставив ему возможность организовать телефонный звонок для подозреваемого;

– расширить возможности подозреваемого связаться с близкими посредством современных технических средств и мобильных приложений;

– разъяснить вопрос о результате реализации рассматриваемого права при ограничении количества попыток дозвониться до нужного для подозреваемого человека.

В целом мы видим позитивные изменения в деле по реформированию уголовно-процессуального законодательства Российской Федерации и уголовного судопроизводства, его гуманизации, но, тем не менее, введенные изменения не лишены ряда недостатков и нуждаются в дальнейшей доработке.

Библиографический список

1. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» // Российская газета. 2016. № 1.

2. *Артемова В.В.* Проблемы законодательного регулирования и практической реализации права задержанного на телефонный разговор // Российский следователь. 2016. № 15. С. 12-15.

3. *Артемова В.В., Самолаева Е.Ю.* Задержание лица по подозрению в совершении преступления в условиях реформирования современного законодательства // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2016. № 3. С. 73-80.

4. *Безлепкин Б.Т.* Комментарий к Уголовно-процессуальному кодексу Российской Федерации. – Москва: Проспект, 2015. С. 63.

5. *Волосова Н.Ю., Журкина О.В.* О некоторых проблемах реализации права лица на телефонный разговор в свете положений Конституции Российской Федерации и Уголовно-процессуального кодекса Российской Федерации // Российская юстиция. 2016. № 7. С. 25.

6. *Орлова А.А.* О реализации принципа «Язык уголовного судопроизводства» в российском уголовном процессе // Проблемы правоохранительной деятельности. 2016. № 2. – URL: http://cyberleninka.ru/article/n/o-realizatsii-printsipa-yazyk-ugolovnogo-sudoproizvodstva-v-rossiyskom-ugolovnom-protsesse.

КИБЕРПРЕСТУНОСТЬ – НОВАЯ УГРОЗА ТРЕТЬЕГО ТЫСЯЧЕЛЕТИЯ

УДК 343:004

Дорошин А.А.,
Николаева А.В.,
курсант
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье дается оценка современного состояния преступлений в сфере информационной безопасности, определена дефиниция «киберпреступность», классификация данного вида преступлений, общая тенденция развития законодательства в сфере информационной безопасности, приведены различные виды органов и организаций по предупреждению киберпреступности, а также способы борьбы с ней.

Ключевые слова: общественная безопасность; охрана правопорядка; информация; Информационная безопасность; киберпреступность; киберпреступления; компьютерные преступления; международное сотрудничество; информационные технологии.

KIBERPRESTUNOST – NEW THREAT OF THE THIRD MILLENNIUM

Doroshin A.A.,
Nikolaeva A.V.,
Cadet
(Kikot Moscow University of the Ministry of the Internal Affairs of the Russian)

Abstract: the article gives an assessment of the current state of crimes in the field of information security, defines the definition of «cybercrime», the classification of this type of crime, the general tendency of the development of legislation in the field of information security, various types of bodies and organizations for the prevention of cybercrime, and ways to combat it.

Key words: public safety; law enforcement; information; Information Security; cybercrime; cybercrime; computer crimes; the international cooperation; Information Technology.

Проблема обеспечения правопорядка, общественной безопасности существует на протяжении многих тысячелетий. Еще в древности, в таких возникших полисных государствах, как Вавилон, Греция, Индия, Рим в связи с появлением преступлений, затрагивающих права, законные интересы личности, членов семьи, управленцев государств, религии, имело место обеспечение об-

щественного порядка. В связи с этим создавалось достаточно большое количество нормативной базы, регулирующей отношения между членами различных сословий: Законы Хамураппи в древнем Вавилоне, законы Ману в Индии и др. Помимо законов существовали и специальные органы, осуществлявшие обеспечение общественной безопасности и неукоснительное соблюдение всеми жителями полисов установленных законов, для которого необходимы охрана правопорядка путем организации и структурированного взаимодействия государственных органов. На сегодняшний день существует множество законов и различных органов, осуществляющих борьбу с преступлениями и административными правонарушениями.

Статистика МВД России[1] о состоянии преступности, начиная с 2003 года, показывает, что наибольшее количество преступлений составляют кражи и мошенничество, данные на 2018 г. гласят нам о том же (почти половина всех зарегистрированных преступлений составляют кражи и мошенничества).

Но как известно, наше общество не стоит на месте, оно динамично: находится в постоянном развитии, свершая открытия в различных сферах жизни. Так, важную роль играют открытия в сфере информационных технологий.

Всем нам известно, что в современном XXI в. информация представляет огромнейшую ценность для каждого из нас. Не зря существует суждение: «Человек, владеющий информацией, владеет миром». Именно поэтому преступления, связанные с посягательством на информацию, стали не редкостью в 3-м тысячелетии, а угроза Информационной безопасности стала одной из самых актуальных проблем на сегодняшний день, ведь большинство различной конфиденциальной информации граждан хранится в электронном виде в сети Интернет. Дефиниция «угрозы информационной безопасности» определяется в п. 2 б) гл. I доктрины Информационной безопасности: «Угроза Информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»[2].

С расширением применений новых технологий в информационной сфере, являющихся непосредственным фактором развития экономики, а также совершенствования функционирования институтов общества и государства одновременно возникают новые информационные угрозы. При этом отсутствие увязки информационной безопасности с обеспечением информационных технологий вызывает значительный риск в проявлении новых информационных угроз:

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, групповому и общественному сознанию, духовному возрождению России[3].

[1] https://мвд.рф/reports/item/13357360/ (Приложение 1).

[2] Доктрина Информационной безопасности Российской Федерации от 05.12.2016 № 646 п. 2 б). Гл. I.

[3] Конституция Российской Федерации. Ст. 24 гл. 2.

2. Угроза информационному обеспечению государственной политики Российской Федерации.

3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникаций и связи, обеспечению потребностей внутреннего рынка ее продукцией и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

4. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Все большее развитие получает и такая угроза информационной безопасности, как киберпреступления. Данная угроза является достаточно опасной, поскольку действует не только на личностном (общественном) уровне, но и на международном как источник межгосударственных противоречий. Именно поэтому многие мировые эксперты считают ее наиболее опасной угрозой информационной безопасности.

Данный вид преступности растет не только в пределах нашего государства, интернет-преступность охватывает и международные масштабы, о чем свидетельствуют данные многих известных международных компаний, а также выводы экспертов и аналитиков. По данным компании Allianz Global Corporate & Specialty на 2016 год, ущерб от данного вида преступности для мировой экономики превысил 575 млрд долларов, что составляет около 1% мирового ВВП. В 2017 году ущерб мировой экономики от участившихся кибератак, по прогнозам Сбербанка России, может превысить 1 трлн долларов, а через 3 года – вырасти до 2 трлн долларов. По расчетам Allianz Global Corporate & Specialty, действия хакеров приносят наибольший вред.

«Важно противодействовать угрозам превращения интернета в театр военных действий или идеологических сражений и обеспечить информационную безопасность каждого государства мира», – подчеркнул Шерстюк[1].

Киберпреступность – один из видов правонарушений, осуществляемый путем применения компьютерных технологий, включающий в себя распространение вирусов, нелегальную загрузку файлов, а также персональной информации: информации по банковским счетам.

Необходимо отличать киберпреступления как правовую категорию от киберпреступлений как социальное явление. Обмен электронной почтой между лицами, готовящими преступление, размещение криминально ориентированной информации на веб-сайтах относятся к киберпреступности как социальному явлению.

Европейская Конвенция Совета Европы по киберпреступлениям (преступлениям в киберпространстве) от 23.11.2001 подразделяет киберпреступления на четыре типа:

1. Незаконный доступ – ст. 2 (умышленный противоправный доступ к компьютерной системе либо ее части).

[1] Директор Института проблем информационной безопасности МГУ имени М.В. Ломоносова Владислав Шерстюк.

2. Незаконный перехват – ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах).

3. Вмешательство в данные – ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных).

4. Вмешательство в систему – ст. 5 (противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных)».

Данные виды преступлений являются «компьютерными», в отличие от остальных – связанных с компьютером либо совершаемых посредствам компьютера, например:

– преступления, где компьютер используется как интеллектуальное средство (размещение в сети Интернет детской порнографии, информации, разжигающей религиозную, национальную, расовую вражду);

– преступления, связанные с нарушением авторских прав;

– преступления, в которых компьютер выступает орудием их совершения (мошенничество, электронные хищения).

Составы таких преступлений как: компьютерные кражи, мошенничества и иные преступления подобного рода включены в национальное уголовное законодательство. Сложность борьбы с данными видами преступлений заключается в их «виртуальном» характере, которой позволяет мгновенно удалять следы преступления, что значительно затрудняет поиск преступника.

Именно поэтому необходимо искать эффективные способы борьбы с киберпреступлениями. На сегодняшний день уже существует большое количество способов борьбы с компьютерными преступлениями, основополагающим из которых является создание и совершенствование нормативно-правовой базы. В Уголовном Кодексе Российской Федерации имеются статьи о преступлениях, связанных с применением компьютера и иных электронных средств, например, ст. 159.6 «Мошенничество в сфере компьютерной информации», ст. 186 «Неправомерный оборот средств платежей», в которой говорится о различных способах неправомерного осуществления приема, выдачи, перевода денежных средств, в том числе с помощью технических средств и компьютерных программ. Помимо вышеперечисленных статей, УК РФ содержит главу 28 «Преступления в сфере компьютерной информации», которая полностью посвящена киберпреступности:

– ст. 272 «Неправомерный доступ к компьютерной информации»;

– ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»;

– ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;

– ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Регулярно для наиболее эффективной борьбы с кибератаками совершенствуется законодательная база путем внесения в нее изменений. Не является исключением и УК РФ. Подготовлен Проект Федерального закона № 186266-7 «О внесении изменений в Уголовный кодекс Российской Федерации», который направлен на усиление уголовной ответственности за хищение денежных средств с банковского счета, а равно электронных денежных средств.

Комитет концептуально поддерживает усиление ответственности в сфере киберпреступлений, в особенности учитывая динамичное развитие как банковских технологий, так и различных форм хакерских атак.

Существуют и иные виды законов, например, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации». В данном законе содержатся способы борьбы с компьютерными атаками на информационные ресурсы Российской Федерации (ст. 5), утверждены силы и средства предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, к которым относят: подразделения, должностные лица федерального органа исполнительной власти; к средствам обнаружения, предупреждения, ликвидации последствий компьютерных атак относят технические программные, программно-аппаратные, криптографические средства защиты информации. Организует и проводит исследования в области защиты информации, экспертные криптографические, инженерно-криптографические и специальные исследования шифровальных средств, а также осуществляют подготовку экспертных заключений по их созданию ФСБ РФ, о чем свидетельствует указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Данным Указом на ФСБ РФ возлагаются функции федерального органа исполнительной власти уполномоченного в области обеспечения функционирования государственной системы обнаружения по предупреждению, ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Помимо ФСБ РФ в России существует Войска информационных операций, созданные Указом Президента России в феврале 2014 год. Данная структура занимается управлением и защитой военных систем управления и связи от кибертерроризма. 14 января 2014 года Приказом министра обороны России С.К. Шойгу было создано кибернетическое командование Генштаба Вооруженных сил России. Оценки аналитиков России показывают, что Россия может входить в топ-5 государств мира по уровню развития кибервойск после таких государств, как США, Китай, Великобритания, Южная Корея.

Активную борьбу с киберпреступностью ведет одно из специализированных подразделений МВД России.

Управления «К» МВД России:

1. Ведет борьбу с преступлениями в сфере компьютерной информации, в процессе которой:

– выявляет и пресекает факты неправомерного доступа к компьютерной информации;

– ведет борьбу с изготовлением, распространением и использованием вредоносных программ для ЭВМ;

– противодействует мошенническим действиям с использованием возможностей электронных платежных систем;

– ведет борьбу с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресекает противоправные действия в информационно-телекоммуникационных сетях, включая сеть Интернет:

– выявляет и пресекает преступления, связанные с незаконным использованием ресурсов сетей сотовой и проводной связи;

– противодействует мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;

– противодействует и пресекает попытки неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Ведет борьбу с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявляет и пресекает факты нарушения авторских и смежных прав в сфере информационных технологий.

5. Ведет борьбу с международными преступлениями в сфере информационных технологий:

– оказывает противодействие преступлениям в сфере информационных технологий, носящим международный характер;

– взаимодействие с национальными контактными пунктами зарубежных государств.

6. Осуществляет международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Международное сотрудничество играет огромную роль в борьбе с киберпреступностью, поскольку с развитием новых информационных технологий существенно увеличился риск их применения значительной частью государств в каких-либо возникающих международных противоречиях, для распространения преступлений экстремистской направленности и иных преступлений, связанных с посягательством на права и свободы, а также законные интересы человека. Ежегодно на государственные интернет-ресурсы Российской Федерации, США, КНР в среднем совершается 70 млн кибератак (см. приложение 2). Наиболее серьезной проблемой является поединок информационных технологий между несколькими сильными государствами, ведь принимая свои технические новшества для защиты собственных интересов в процессе противоборства, они могут нанести вред не только друг другу, но и всем окружающим, находящимся на данной территории. Именно поэтому подписывается немало международных соглашений, создаются международные организации, являющиеся противоборствующей силой для киберпреступности.

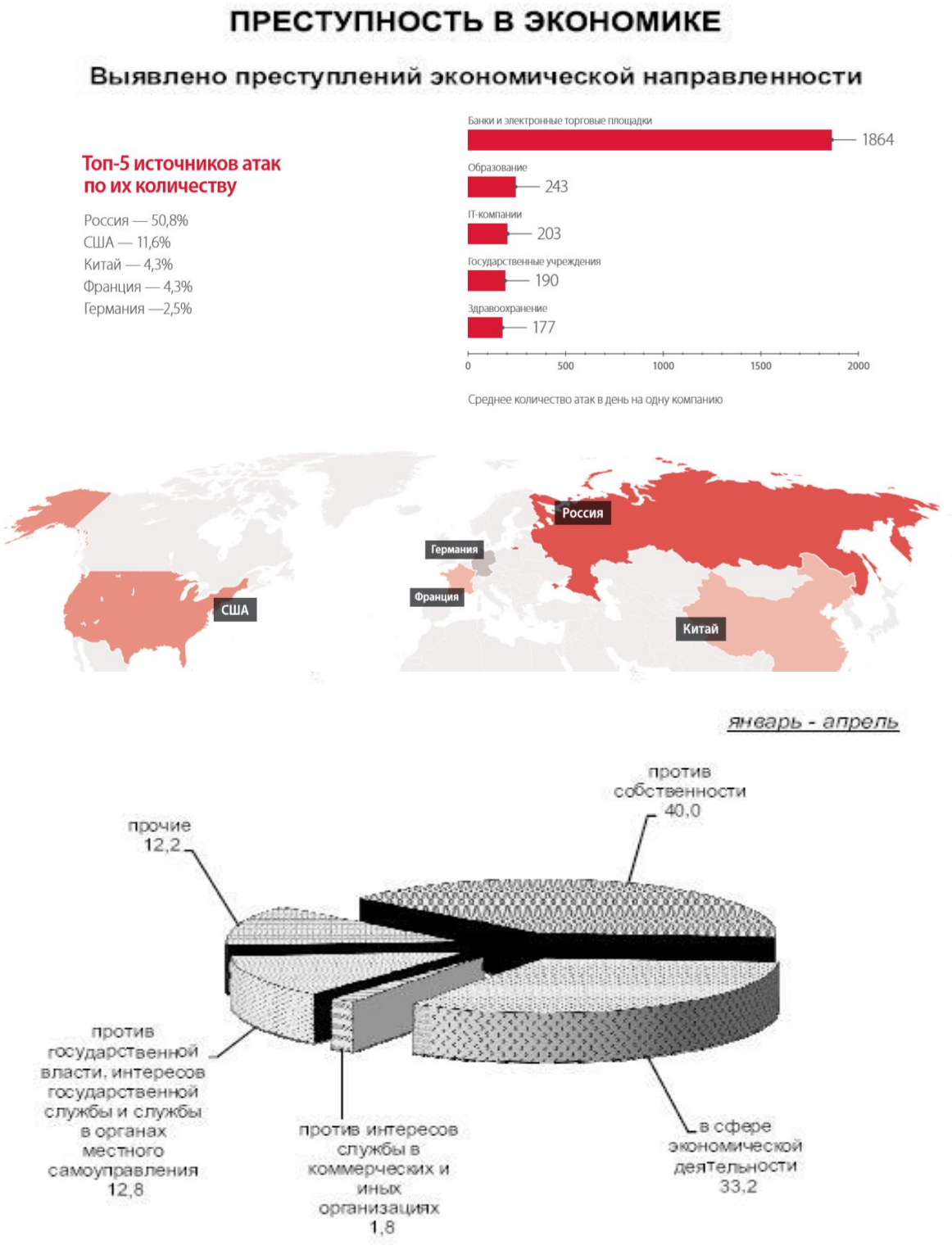
Так, свыше 150 лет назад, в 1865 г., создан такой международный орган, как МСЭ (международный союз электросвязи), который является ведущим учреждением Организации Объединенных Наций в области информационно-коммуникационных технологий, в частности – в укреплении доверия и безопасности при их использовании. Эта организация задает направление инновациям в сфере ИКТ вместе со своими 193 государствами-членами, а также членами, представляющими около 800 объединений частного сектора, академические учреждения. МСЭ – межправительственный орган, отвечающий за координацию на глобальной основе совместного использования радиочастотного спектра, содействие международному сотрудничеству при присвоении спутниковых орбит, совершенствование инфраструктуры связи в развивающихся странах и создание всемирных стандартов, обеспечивающих беспрепятственное взаимодействие широкого диапазона систем связи.

Таким образом, информация в XXI веке является неотъемлемой частью нашей жизни. Она может служить и объектом посягательства в сфере информационных технологий, а также выступать в качестве объекта и средства воздействия на общество, а также права, свободы, законные интересы, психику (путем распространения нелегальной информации, экстремистской направленности в сети Интернет, различных социальных сетях и иных СМИ) и материальное положение (преступления, совершенные в банковской сфере – мошенничество, кража, нелегальное использование личной информации граждан и др.). Информационные технологии не стоят на месте. Именно поэтому необходимо искать новые способы борьбы с киберпреступностью. Причем важно ее обеспечивать на всех уровнях, начиная с личностного.

На сегодняшний день существует достаточно большое количество мероприятий, акций, направленных на привлечение детей к соблюдению кибербезопасности при использовании сети Интернет. Так, сотрудники МВД России по делам несовершеннолетних из различных точек нашей страны принимают активное участие в акции «Безопасный Интернет – детям». Сотрудники МВД по Республике Бурятия, Самарской области, Краснодарскому краю, Московской, Ивановской областям провели занятия с учащимися различных образовательных учреждений о необходимости защиты компьютеров, гаджетов от кибермошенничества, о нарушениях морали и этики при онлайн-общении, правилах хранения, использования, распространения личной информации, а также о работе с персональной компьютерной техникой.

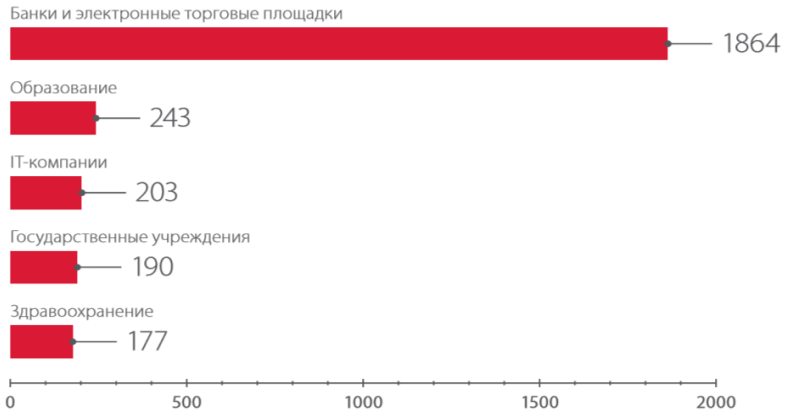
Помимо всего необходимо международное сотрудничество, эффективная работа государственных органов и организаций абсолютно на всех уровнях обеспечения информационной безопасности. Только тогда новая угроза третьего тысячелетия потеряет свою актуальность и силу.

Приложение 1.



Приложение 2.

Статистика атак в веб-приложениях за IV квартал 2017 года (Среднее число атак в день по отраслям)



СИСТЕМА ОБРАБОТКИ ИНЦИДЕНТОВ В УПРАВЛЕНИИ IT-ИНФРАСТРУКТУРОЙ БЕЛГОРОДСКОГО ЮРИДИЧЕСКОГО ИНСТИТУТА МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА

УДК 004

Колтунов Н.Л.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассмотрены вопросы создания и работы системы управления IT-инфраструктурой вуза, в частности автоматизации обработки процессов, связанных с инцидентами пользователей в IT-инфраструктуре образовательной организации.

Ключевые слова: IT-инфраструктура, инцидент, заявка, система управления.

SYSTEM INCIDENT HANDLING IN THE MANAGEMENT OF IT-INFRASTRUCTURE OF THE BELGOROD LAW INSTITUTE THE INTERIOR MINISTRY OF RUSSIA NAMED AFTER I.D. PUTILIN

Koltunov N.L.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article deals with the creation and operation of a system for managing the IT-infrastructure of a university, in particular, automating the pro-

cessing of processes related to user incidents in the IT-infrastructure of an educational organization.

Key words: IT-infrastructure, incident, application, management system.

В современном мире четко отлаженную систему управления вузом невозможно построить без автоматизации всех ее процессов. Это, в свою очередь, предполагает организацию единого информационного пространства и современной IT-инфраструктуры.

Необходимым условием успешной деятельности организации высшего образования является обеспечение быстрого доступа, качественной и своевременной обработки, а также хранения информации при обеспечении соответствующего уровня безопасности. Помимо этого, требуется организация процесса стратегического планирования, при котором работа организации будет, как минимум, экономически оправданной.

Специфика образовательной организации требует внесения определенных корректив в процесс организации и управления IT-инфраструктурой.

Грамотное использование новых информационных технологий является залогом успеха будущего специалиста. В соответствии с этим, одним из главных при подготовке квалифицированных специалистов является такое направление деятельности, как информатизация образования.

В Педагогическом терминологическом словаре дается следующее определение:

информатизация образования – это процесс:

– обеспечения системы образования информационными средствами, продукцией и технологиями с целью совершенствования механизмов управления системой образования на основе использования автоматизированных банков данных;

– совершенствования методологии отбора содержания, методов и организационных форм обучения и воспитания; создания методик, ориентированных на развитие интеллекта учащихся, на формирование у них способности самостоятельно осуществлять информационно-поисковую и экспериментально-исследовательскую деятельность;

– разработки компьютерных тестирующих и диагностирующих методик, обеспечивающих объективный, систематический и оперативный контроль и оценку уровня знаний учащихся[1].

Исходя из вышесказанного можно уверенно заявить, что технологической основой информатизации образования является IT-инфраструктура.

IT-инфраструктура – это комплексная структура, объединяющая все информационные технологии и ресурсы, используемые конкретной организацией. Информационно-технологическая инфраструктура включает все компьютеры, установленное программное обеспечение, системы связи, информационные центры, сети и базы данных [1].

Основной задачей IT-инфраструктуры организации высшего образования является обеспечение постоянного доступа к образовательным и обеспе-

[1] *Бим-Бад Б.М.* Педагогический энциклопедический словарь. – Москва, 2002. С. 109-110.

чивающим ресурсам для различных категорий пользователей (обучающиеся, научно-педагогические работники, учебно-вспомогательный и обеспечивающий персонал (отдел кадров, бухгалтерия и т.п.)).

Правильно построенная IT-инфраструктура и четко отлаженная ее работа является залогом улучшения работы информационных сервисов, систем электронного документооборота, повышения качества образовательных услуг и обеспечения подготовки высококвалифицированных современных специалистов, а также успешной и эффективной деятельности всей образовательной организации.

Существует несколько проблем эксплуатации и совершенствования IT-инфраструктуры. Основной из них является работа с инцидентами пользователей. Данный вид деятельности обычно занимает большую часть рабочего времени IT-подразделения, однако, наименее результативен по соотношению время/задачи и вносит критические изменения в любое планирование. Существенную помощь в преодолении проблем с инцидентами и сроками их решения может оказать разработка Системы управления инцидентами, а анализ инцидентов создаст возможность выявления «узких» мест, требующих модернизации.

Инцидент – незапланированное прерывание (сбой) IT-услуги и/или снижение качества IT-услуги. В большинстве случаев – это прерывание (или частичное прерывание) IT-услуги, которая ранее предоставлялась пользователю в утвержденном режиме (например: Электронная информационно-образовательная среда, согласно ФГОС, должна быть доступна обучающемуся в режиме 24/7).

Необходимо также отметить важность первичной классификации инцидентов. Она определяет весь последующий цикл обращения, в том числе и сроки исполнения. Даже стандартные проблемы должны анализироваться.

Инциденты происходят ежедневно – выходят из строя компьютерная техника, принтеры, заканчиваются расходные материалы, возникают сбои в сетевом подключении и т.п. Поток инцидентов и мероприятий по их устранению смешивается, и, как следствие, картина о проделанной работе представляется только в общих чертах. Безусловно, такая модель работы для IT-подразделений неприемлема.

Отметим, что имеется многообразие частных случаев, которые достаточно сложно поддаются какой-либо классификации. Минимизировать количество неправильно классифицированных обращений, а также уменьшить общее время реакции IT-сотрудников на решение проблемы может внедрение системы управления IT-инфраструктурой, моделей поведения данной системы, алгоритмов действий при возникновении инцидентов или системных проблем.

Понимание системности инцидентов и проблем, критичность узлов IT-инфраструктуры, их своевременный анализ и правильная оценка помогут оптимизировать инфраструктуру, найти и устранить ошибки и, как следствие, четко и правильно организовать систему поддержки деятельности и развития IT-инфраструктуры образовательной организации.

В единой автоматизированной среде IT-менеджмента должен осуществляться прозрачный контроль соблюдения параметров предоставления IT-услуг

(включая время реакции на поступивший запрос и время его исполнения). Это позволит соблюдать установленные регламентом сроки и оперативно производить решение запросов.

В настоящее время подача заявок на устранение различных инцидентов и проблем в области IT-услуг в Бел ЮИ МВД России имени И.Д. Путилина осуществляется в еще традиционном для многих вузов России печатном (бумажном) виде. Такая система организации деятельности (в т.ч. для IT-подразделений) является крайне неудобной. Это влечет за собой значительные затраты времени и трудовых ресурсов на обработку заявок, определение и устранение ошибок, а также на правильное и оптимальное планирование деятельности подразделений.

Для объективного планирования, контроля и подготовки отчетности возникла необходимость внедрения системы управления инцидентами. В Бел ЮИ МВД России имени И.Д. Путилина для этих целей разработана система управления инцидентами в IT-инфраструктуре «Электронная заявка» (см. рис. 1).

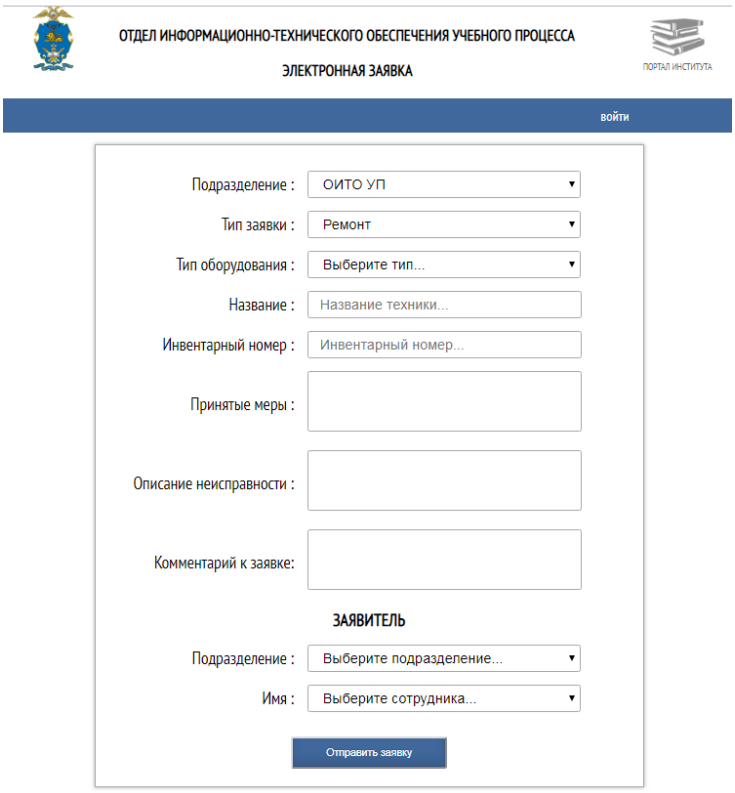


Рисунок 1.
Главная страница веб-интерфейса системы управления инцидентами в IT-инфраструктуре «Электронная заявка»

Система позволяет принимать и обрабатывать заявки на устранение инцидентов (техобслуживание, устранение проблем, сглаживание проблем и т.п.), предоставляет механизм контроля и учета трудозатрат IT-специалистов, необходимых ресурсов, материалов и оборудования, позволяет анализировать и корректировать алгоритмы решения инцидентов, находящихся в зоне ответственности IT-подразделений.

Внедрение Системы управления инцидентами, как одной из подсистем Системы управления IT-инфраструктурой, позволяет планировать изменения как технической составляющей IT-инфраструктурой, так и ее конфигурациями, своевременно и оперативно устранять инциденты и проблемы пользователей, возникающие в процессе их трудовой деятельности, а также осуществлять рациональное и эффективное управление IT-подразделениями и организацией в целом.

Накопленная информация об инцидентах пользователей в IT-подразделении позволит создать систему интеллектуальной поддержки принятия решений управления IT-инфраструктурой организации. В дальнейшем обработка таких данных позволит формировать базы знаний, и, при проведении соответствующего анализа, планировать ремонт или модернизацию отдельных (проблемных) узлов.

Подводя итог, можно отметить, что IT-инфраструктура организации высшего образования включает в себя существенное многообразие аппаратных (технических) и программных составляющих, число которых неуклонно растет из года в год. Это создает необходимость перехода управления IT-инфраструктурой с технического уровня на стратегический. Разработка и внедрение систем управления дает возможность IT-специалистам управлять IT-инфраструктурой из единого центра. Внедрение таких систем, на сегодняшний день, является стратегически правильным решением, т.к. позволяет значительно снизить трудозатраты, своевременно выявлять проблемы, анализировать причины возникновения и оперативно их устранять. Немаловажным аспектом внедрения таких систем является возможность формирования статистики проблем, которая оказывает существенное влияние при принятии решения о модернизации или внедрении новых составляющих IT-инфраструктуры образовательной организации.

Библиографический список

1. https://www.stekspb.ru/autsorsing-it-infrastruktury/it-glossary/it-infrastructure/ (ссылка от 10.09.2018).

ФАКТОРЫ И ПУТИ ПОВЫШЕНИЯ КАЧЕСТВА ОБУЧЕНИЯ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ КРАСНОДАРСКОГО УНИВЕРСИТЕТА МВД РОССИИ

УДК 378.1

Иванов И.П.,
кандидат педагогических наук, доцент
(Краснодарский университет МВД России)

Аннотация: объектом исследования является организация образовательного процесса в условиях современного информационного общества.

Предметом исследования является роль информационных технологий в повышении качества обучения. На основе системного анализа результатов работ других авторов и собственных исследований сделаны выводы о необходимости преобразования педагогической деятельности, направленной на развитие и становление гармоничной личности обучающегося.

Ключевые слова: педагогическая деятельность, эффективность обучения, информационные технологии, уровень образования, образованность.

FACTORS AND WAYS OF ADVANCING THE QUALITY OF EDUCATION AT RUSSIAN UNIVERSITIES OF INTERNAL AFFAIRES: WAYS TO SOLVE IT

Ivanov I.P.,
Candidate of Pedagogical Sciences, Associate Professor
(Russian Krasnodar University of Internal Affaires)

Abstract: the subject of investigation is organization of education process in conditions of modern informational society. The object of education is the role of information technologies in enhancing the education level. Conclusions were based on systematical analyze of other authors 'works and personal investigations. Conclusions were made about necessity of changes in pedagogical actions. The aim is to develop and form a harmonic personality of a student.

Key words: pedagogical activity, learning efficiency, information technologies, education level, education.

В современном мире, несомненно, возрастает роль информационных технологий в преобразовании человеческого сознания, как индивидуального, так и коллективного. Соответственно отдельный человек и целые государства становятся объектами информационного воздействия. Интересы преобразования России требуют существенно поднять уровень подготовки государственных служащих, способных самостоятельно и творчески организовывать свою профессиональную деятельность и управлять социальными процессами. В таких условиях к профессиональной подготовке сотрудников ОВД предъявляются повышенные требования по укреплению правовой, нравственной и, как следствие, экономической основы нашего общества.

Д.А. Медведев в одном из своих выступлений, характеризующих потенциал обучающихся, сказал: «России необходимы квалифицированные кадры, настоящие профессионалы своего дела».

Образование – это совокупность знаний, получаемых человеком. Чем больше их объем – тем выше уровень образования. Значение имеет также разнообразие и качество знаний, а еще очень важно наличие навыков, связанных с их применением в профессиональной деятельности. Образованность – это конкретный результат получения человеком образования.

Поэтому педагогическая деятельность направлена на развитие и становление личности обучающегося (ее обучение, воспитание), но это не различные процессы, а лишь две стороны единого процесса. Деятельность, один из аспектов динамики человека, который является формой его реального существования.

Однако не всякая деятельность обеспечивает достижение желаемых результатов в воспитании и развитии. Поэтому столь же важно и другое положение психологии – положение о ведущем виде деятельности, обеспечивающем необходимые условия для успешного формирования и развития личности.

Вот уже на протяжении последних 60-65 лет развитие когнитивных процессов у обучающихся (включающих знания, умения и навыки) считается основой педагогической деятельности. А выработкой новых подходов к формированию образовательной деятельности и улучшением образованности населения занимается, в основном, преподаватель. Как бы всесторонне ни использовались современные информационные технологии в образовании, а одним из основных трансляторов знаний сегодня остаются межличностные отношения преподавателя и обучающегося. Поэтому в процессе обучения педагог считается основным источником информации.

«Педагог» в словаре Ушакова – это человек, профессионально занимающийся преподавательской и воспитательной работой.

В учебном процессе заложены основные воспитательные и развивающие возможности, но для того чтобы получить максимальную эффективность обучения с целью формирования и развития профессиональных личностных качеств обучающихся, необходимо специальное построение обучения. Эту мысль хорошо выразил Леонид Владимирович Занков, применительно к развитию обучающихся: «Дидактика уже не может ограничиваться областью знаний и навыков, как бы ни важна была эта область. Необходима разработка научно-педагогических основ такого построения учебного процесса, которое давало бы оптимальные результаты в развитии обучающихся. Следовательно, нужно изыскивать новые принципы, правила, требования, которые будут соответствовать современным этапам развития общества и сформулированной задаче. Однако задача заключается не в том, чтобы получить какой-то результат, а в том, чтобы добиться максимальной эффективности обучения, а выполнение этой задачи... требует специального обдумывания и построения учебного процесса» [3].

Поэтому сегодня я хочу поговорить не столько об обучающихся, которым и так уделяется максимальное внимание, а о второй половине составляющей учебного процесса – преподавателях.

Основными целями и задачами, которые ставит перед собой педагог, считается определение выбора средств, форм, методов, приемов, которые он применяет в процессе воспитания и обучения. Эти цели должны в первую очередь определять: кого, чему и как учить.

В процессе воспитания и обучения должен быть достигнут некий результат. Ожидаемый результат определяется качественной составляющей педагогического процесса, включая программы, учебники, методические и на-

глядные пособия, электронные и мультимедийные материалы, а также профессиональные знания и умения преподавателя.

В 2003 году мною было выпущено учебно-методическое пособие «Основы самостоятельной работы курсанта вуза МВД России», в котором нашли свое отражение формы и методы организации самостоятельной подготовки курсантов. В то время сеть Интернет была еще только в процессе развития и планах на будущее, поэтому одним из актуальных направлений считалось овладение методами и средствами поиска, первоначальной обработки и изучения информации, что включало в себя:

– самостоятельный поиск с помощью каталогов или картотеки библиотеки;

– поиск с помощью библиотекаря или сотрудника методического кабинета;

– самостоятельный поиск с помощью справочно-информационных изданий и библиографических пособий.

Все эти методы остались актуальными и сегодня, только данные действия можно осуществлять с помощью компьютера. Но у компьютера есть и отрицательные моменты, которым необходимо научить обучающихся. Например, при поиске информации в поисковых системах для качественной формулировки поискового запроса необходимо знать половину правильного ответа. После отражения списка найденной информации, чтобы из вороха мусора выбрать качественную информацию на поставленный вопрос, снова потребуется знание второй половины ответа. Вот и делайте выводы. Это конечно шутка, но с определенной долей правды. Поэтому одной из целей образования можно считать не только закладку фундаментальных возможностей поиска, но и развитие умения качественного осмысления информации. С этого года в Британии на экзаменах разрешили обучающимся пользоваться Интернетом. Хорошо это или плохо. С одной стороны – плохо, так как предлагается использовать на первых отображаемых страницах заведомо неверные варианты ответов. С другой стороны, это позволит развивать память обучающихся, для дальнейшего сравнения правильности запоминаемой информации. Например, можно привести следующий вариант деятельности обучающихся. Как действуют обучающиеся во время тестирования? Первое – читают внимательно вопрос теста. Второе – читают предложенные варианты ответов и выбирают среди них правильный. А надо было сначала ответить на предложенный вопрос, а затем искать вариант совпадения.

Электронные обучающие ресурсы. Образовательный процесс, в котором есть постоянный доступ к электронным ресурсам образовательной организации, способствует конкретному целенаправленному способу изучения качественной и минимального объема информации. Куранты старших курсов регулярно пользуются рабочими программами на экзаменах. А курсанты начальных курсов утрачивают эту возможность, в связи с отсутствием печатных изданий. Электронные ресурсы, хранимые на портале университета, в оболочке «Битрикс» не всегда оправдывают себя. Для обращения к учебно-методи-

ческим комплексам необходимо извлечь информацию из архива на свой компьютер. При этом могут возникать определенные трудности:

1. Надо установить дополнительно программу для работы с файлами на локальном диске.

2. При этом для сохранности информации и дальнейшего ее использования курсанты пользуются своими индивидуальными папками. Посчитайте, если 100 курсантов скопируют весь файл в свои каталоги – это будет очень большой объем информации.

3. Большинство курсантов не имеют навыков пользования программой «Битрикс», а некоторым курсантам в течение года так и не был выдан индивидуальный пароль.

Чтобы избежать данных противоречий, необходимо разработать место для хранения информационных электронных ресурсов, которое курсантам будет доступно при обращении с любого компьютера, подключенного к внутренней сети университета. После этого можно переходить к форматам открытого образования и модернизировать их деятельность.

Утеря связи с другими учебными порталами образовательных учреждений возникла при переходе от сети ЕИТКС (единой информационной телекоммуникационной сети) к ИСОД (Единой системе информационно-аналитического обеспечения деятельности МВД России).

Главная задача преподавателя не просто рассказать о проблеме, а уметь изложить ее таким образом, чтобы обучающийся дальше сам смог развиваться. Мой научный руководитель диплома в университете в процессе обучения студентов всегда старался поднять наш уровень самостоятельности и значимости обучения. Его основная фраза, которую он говорил, звучала следующим образом: «Вы студенты Университета. И после окончания вуза Вам будет без разницы, какой предмет преподавать, самое главное вы должны вовремя и качественно успеть подготовиться к нему». Данное правило послужило выбором моей дальнейшей трудовой деятельности. Вот и наша основная задача должна заключаться в повышении образованности выпускников университета по сравнению с другими образовательными учреждениями.

Для достижения необходимого уровня качества обучения преподавателю следует формировать комплексный подход к организации педагогической деятельности, но всегда надо помнить об основных требованиях к себе:

1. Занятие надо проводить не из-за необходимости изучения вопросов программы, а для возможности воздействия на личность обучающегося с потенциалом формирования определенных интеллектуальных и психических качеств личности.

2. Все изменения в развитии личности будут носить качественный показатель при наличии внутреннего побуждения обучающегося. Поэтому положительные или отрицательные результаты занятия не должны вызывать негативное отношение к изучаемому предмету. Не получилось сегодня, повторю завтра, но обязательно достигну поставленной цели.

3. Каждое занятие должно иметь познавательные составляющие: воспроизводящую, интерпретирующую и творческую.

4. Не забывать, что успех обучения зависит не только от содержания материала, методики проведения занятий и мастерства педагога, но и от внутренних психологических особенностей обучающихся.

Профессионализм преподавателя считается качественным неотъемлемым атрибутом его деятельности. Он позволяет достичь разных высот и добиться своей значимости. Быть профессионалом – это особый талант. Организация процесса обучения занимает основное внимание педагога, направленное на целостное развитие личности обучающегося, который в свою очередь желает получить необходимые навыки своих возможностей для дальнейшего их развития. Поэтому современный учебный процесс должен постоянно совершенствоваться и реорганизовываться в зависимости от условий развития общества.

Библиографический список

1. *Иванов И.П., Федулов Б.А.* Рейтинговая оценка успеваемости и общественной активности курсантов и студентов // Вестник учебного отдела Барнаульского юридического института МВД России. 2005. № 4. С. 21-25.

2. *Иванов И.П.* Основы самостоятельной работы курсанта вуза МВД России: учебно-методическое пособие. – Барнаул: БЮИ МВД России, 2003. – 71 с.

3. *Занков Л.В.* Избранные педагогические труды. – Москва: Педагогика, 1990. – 424 с.

ТИПОЛОГИЧЕСКИЕ ОСОБЕННОСТИ КИБЕРПРЕСТУПЛЕНИЙ

УДК 343

Страхов А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: проведен анализ и типологическая классификация киберпреступлений. Отмечены факторы, способствующие росту тенденции использования киберпространства для совершения традиционных противоправных деяний. Предложены первоочередные меры повышения эффективности подготовки профессиональных кадров для правоохранительных органов.

Ключевые слова: информационное общество, киберпространство, киберпреступность, информационная безопасность, информационное воздействие, социальная инженерия.

TYPOLOGICAL FEATURES OF CYBERCRIME

Strahov A.A.
(Kikot Moscow University of the Ministry of the Interior of Russia)

Abstract: the analysis and typological classification of cybercrime. The factors contributing to the growth of the trend of using cyberspace for the Commission of traditional illegal acts are noted. The priority measures to improve the efficiency of training of professional personnel for law enforcement agencies are proposed.

Key words: information society, cyberspace, cybercrime, information security, information impact, social engineering.

Стремительное развитие информационной индустрии и повсеместное внедрение информационных технологий позволили значительную часть общественных отношений сместить в информационное пространство (киберпространство), представляющее собой «совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры» [1].

При этом, в отличие от материального мира, киберпространство является более благоприятной средой для совершения преступлений. Этому способствует трансграничность, высокая скорость информационного обмена, анонимность и т.п. Круг преступлений, так или иначе связанных с киберпространством, постоянно расширяется, и они уже получили наименование – киберпреступления.

Вместе с тем, довольно часто к киберпреступлениям относят противоправные деяния только в отношении компьютерных систем, что на взгляд автора значительно суживает объем этого понятия. Не менее опасным может быть противоправное использование киберпространства для информационного воздействия на сознание личности и общества.

Основной целью данной статьи является типологическая характеристика киберпреступлений во всем их многообразии. За основу классификации принята структура, рекомендованная Будапештской конвенцией о преступности в сфере компьютерной информации 2001 г. [2].

Преступления против информационной безопасности компьютерных систем и данных – наиболее типичный вид киберпреступлений, к которому относятся:

– преднамеренный противозаконный доступ к компьютерной системе в целом или любой ее части с нарушением мер безопасности (несанкционированный доступ);

– неправомерный перехват данных или преднамеренное создание каналов утечки информации с помощью технических средств;

– умышленное повреждение, удаление, ухудшение качества, изменение или блокирование данных, повлекшее за собой серьезный ущерб;

– умышленное воздействие на компьютерную систему, путем неправомерного ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных;

– изготовление, продажа, приобретение, использование аппаратно-программных средств, разработанных или адаптированных для преступных целей в отношении компьютерных систем, а также компьютерных паролей, ключей, кодов доступа к компьютерной системе в целом или любой ее части.

Среди преступлений данного вида лидирует хакерство – получение несанкционированного доступа к компьютерной системе или данным в обход системы компьютерной безопасности, чаще всего путем целенаправленных кибератак. Причем мотивация у хакеров различна, одним достаточно доказать свою гениальность, другие взламывают компьютерные системы ради политической или экономической выгоды, третьи делают это в государственных интересах и т.п. Для автоматизации хакерских атак разрабатываются универсальные программы, которые можно скачать из интернета. Доступность подобного инструментария порождает хакеров, готовых «на заказ» ломать все подряд.

Перехват данных при передаче в каналах связи или при обработке в компьютерной системе или организация утечки информации осуществляются с помощью специализированных технических средств – «шпионских штучек», таких как аппаратные закладки, программные трояны, бэкдоры, клавиатурные шпионы, устанавливаемые непосредственно в компьютерные системы. Традиционными каналами утечки информации являются побочные электромагнитные излучения и наводки компьютерного оборудования. Повсеместное использование беспроводных точек доступа способствует росту преступлений, связанных с перехватом персональных данных.

По-прежнему достаточно распространенным средством несанкционированного воздействия на компьютерную систему и данные в ней являются компьютерные вирусы. Заражение может осуществляться по сети или через зараженные программы на отторгаемых носителях. В кибервойнах вирусы рассматриваются как эффективное средство нанесения ущерба противнику при минимальных затратах, и их разработка осуществляется при государственной поддержке. В качестве примера можно привести «боевые» вирусы Stuxnet, Duqu, Flame, Regin или вирусы-вымогатели типа WannaCry или Petya.

Преступления, связанные с нарушением конфиденциальности, целостности и доступности информации в компьютерных системах являются традиционными в киберпространстве, и их квалифицирующие признаки наиболее проработаны в уголовном законодательстве развитых стран. Вместе с тем, в информационном обществе, где информационные технологии «кардинальным образом влияют на экономические и социокультурные условия жизни граждан» [1], данный вид противоправных деяний все чаще становится подготовительным шагом к дальнейшим противоправным действиям с компьютерными системами.

Следующий вид киберпреступлений – *традиционные преступления с использованием киберпространства для получения экономической выгоды*:

– подлог или подделка данных;

–хищения и мошенничество;

– присвоение активов и интеллектуальной собственности;

– незаконный товарооборот или оказание услуг.

Цифровая экономика – это хозяйственная деятельность в киберпространстве. Довольно часто мошенничество, хищение денежных средств, незаконное получение кредита, уклонение от уплаты налогов и т.п. сопровождаются нарушением аутентичности компьютерных данных. При этом в случае подлога используются подлинные данные, но авторизованные на другое лицо. Предметом преступления, например, могут быть электронные документы, удостоверенные электронной подписью, или персональные идентификаторы, позволяющие получить удаленный доступ к конфиденциальной информации. В этой связи возник отдельный вид угроз информационной безопасности – кража личности (identity theft). Использование чужой личности в киберпространстве становится настолько популярным, что появились специальные методы и средства для сбора сведений об аккаунтах в социальных сетях, о банковских или кредитных картах, о почтовых клиентах и т.д. Параллельно с техническими методами и средствами активно применяются психотехники социальной инженерии – «взлома» человеческого сознания за счет информационного воздействия. Персональные данные пользователей компьютерных систем сами стали товаром, в том числе в среде кибермошенников.

Предметом кибермошенничества являются данные, которыми можно манипулировать путем ввода, удаления, изменения или блокирования, включая вмешательство в функционирование компьютерной системы.

На официальном сайте МВД России перечисляются наиболее распространенные мошеннические схемы в Рунете [3]:

«Брачные мошенничества» – вступая в переписку, преступники под различными предлогами выманивают у жертвы деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.);

«Приобретение товаров и услуг посредством сети Интернет» – создается аккаунт на торговых интернет-площадках или «одноразовых» сайтах, выставляются интересные предложения о продаже товаров, как правило, со 100% трансграничной предоплатой, например, через «Western Union»;

«Крик о помощи» – выкладывая в Интернет душераздирающую историю о больном ребенке, собачьем питомнике, несчастном ветеране, мошенники организуют сбор денежных средств на электронные счета;

«Фишинг» – с помощью спам-рассылок отправляются подложные письма от имени известных организаций с интересными предложениями (работа за границей, выигрыш в лотерею, просрочка платежей и т.д.), в ответ на которые требуется зайти на сайт-двойник и ввести пароли, пин-коды, CVV-коды и другую персональную информацию;

«Нигерийские письма» – мошенники уведомляют жертву о возможности поучаствовать в получении многомиллионной денежной суммы (например, наследство неизвестного родственника) при незначительных накладных расходах (на оплату налогов и сборов, оформление документации, взяток);

«Брокерские конторы» – все чаще граждане жалуются на недобросовестные действия брокерских контор («MXTrade» и «MMCIS»).

К списку мошеннических схем можно добавить использование онлайн-аукционов, электронных торговых площадок и досок объявлений (eBay, AliExpress, Avito) с целью реализации контрафактных товаров, а также мошенничество с использованием платежных карт.

В качестве примеров кибератак на банковские активы можно рассмотреть международные расследования компании Group-IB [4]. Хакеры из северокорейской группы Lazarus долгие годы шпионили за идеологическими врагами режима – госучреждениями и частными корпорациями США и Южной Кореи. Теперь Lazarus атакует банки и финансовые учреждения по всему миру. В июне 2016 года в России была зарегистрирована первая атака группы Cobalt, которая сначала организовывала кражи денег через банкоматы, а затем стала атаковать любые системы финансовых организаций, в которых имелись деньги (карточный процессинг, платежные системы, SWIFT и пр.). Хакеры Buhtrap с августа 2015 по февраль 2016 года осуществили 13 успешных атак на банки России, сняв со счетов 1,8 млрд рублей. Средняя сумма хищения составила 62% от уставного капитала банка. Организованная преступная группа Anunak с 2013 г. осуществила хищения денежных средств непосредственно из 50 российских банков и 5 платежных систем. Среднее время с момента проникновения во внутреннюю сеть финансовой организации до момента хищения составляло 42 дня.

Компании, распространяющие продукцию напрямую через Интернет, могут столкнуться с правовыми проблемами, связанными с нарушениями авторских или смежных прав. Торговая марка, логотип, фирменный дизайн продуктов известной компании могут использоваться при изготовлении и сбыте контрафакта или при создании поддельных информационных ресурсов в сети Интернет.

Киберпреступления, связанные с нарушением прав интеллектуальной собственности, в основной своей массе используют механизмы противозаконного копирования и распространения цифровых данных. Если в доинформационном обществе копирование аудио- и видеозаписей всегда приводило к некоторому снижению качества, то сейчас цифровые версии авторских произведений можно копировать без потери качества неограниченное число раз и выкладывать для общего доступа на файлообменники, в социальные и пиринговые сети и т.п. Коммерческая выгода от интернет-пиратства настолько велика, что взлом любых технологий защиты быстро окупается.

Возможность анонимного взаимодействия поставщика товаров (услуг) и потребителя, а также электронные платежи позволили использовать киберпространство для совершения большинства традиционных преступлений, связан-

ных с незаконным товарооборотом или оказанием услуг. Помимо незаконной коммерческой деятельности к данному виду преступлений можно отнести торговлю запрещенными препаратами, оружием, алкоголем, контрафактом и т.п.

МВД России в первом полугодии 2017 г. выявлено 3775 преступлений, связанных с незаконным оборотом наркотиков, совершенных с использованием интернет-технологий. К уголовной ответственности привлечено 1583 лица, из незаконного оборота изъято свыше 760 кг наркотиков. Пресечена деятельность 1345 интернет-ресурсов, посредством которых осуществлялась торговля наркотиками, на территории РФ решением Роскомнадзора доступ к ним запрещен. Ликвидирован крупнейший интернет-магазин наркотиков RAMP (Russian anonymous marketplace), действовавший в русскоязычном сегменте анонимной сети TOR [5]. В конце июня 2018 г. в УК РФ внесены изменения, устанавливающие уголовное наказание за «незаконное приобретение или продажу особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в красную книгу Российской Федерации и/или охраняемым международными договорами Российской Федерации, их частей и дериватов (производных) с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет» (статья 258.1).

Среди множества киберпреступлений следует выделить *преступления, связанные с противозаконным контентом*:

– педофилия и распространение детской порнографии;

– экстремизм и терроризм;

– преступления против личности.

Учитывая низкую затратность практически мгновенной доставки контента неограниченному кругу заинтересованных потребителей, детская (и взрослая) порнография в сети Интернет считается высокодоходным бизнесом при минимальном риске. Большая часть материалов хранится и распространяется в зашифрованном виде на форумах с ограниченным доступом, и оплата осуществляется через анонимные платежи.

Те же причины, а также возможность информационного воздействия на личность и общество с территории другой страны способствуют расширению антигосударственной пропаганды, экстремистской и террористической деятельности в киберпространстве. Причем в ряде случаев эта деятельность осуществляется под эгидой иностранных спецслужб. Ярким примером этому могут служить цветные революции и иные протестные выступления, организуемые через социальные сети.

Основная проблема данного вида преступлений не в квалификации деяния, а в его профилактике, обнаружении и раскрытии. Значительный процент подобных преступлений раскрывается в ходе агентурных оперативных мероприятий. Дополнительной проблемой является незнание интернет-пользователями уголовного законодательства, которые часто не подозревают, что в российском уголовном законодательстве предусматривается ответственность как за оригинальную противозаконную публикацию, так и за ее репост. Если на

своей странице разместить ссылку на чужие персональные данные, карикатуры, клевету, приглашение на несанкционированный митинг и т.п., то можно получить наказание от штрафа в несколько тысяч рублей до лишения свободы. Или, например, развратными могут признаваться действия в отношении лиц, не достигших шестнадцатилетнего возраста, совершенные с использованием сети Интернет без непосредственного физического контакта с телом потерпевшего лица.

Кроме неправомерного физического воздействия на критическую информационную инфраструктуру Российской Федерации существует еще информационное воздействие на индивидуальное и общественное сознание.

К экстремистским киберпреступлениям могут быть отнесены:

– публичные призывы к осуществлению террористической деятельности, экстремизму и массовым беспорядкам;

– распространение или обеспечение свободного доступа к ксенофобским материалам экстремистской направленности;

– распространение или обеспечение свободного доступа к материалам, отрицающим негативные последствия, одобряющим или оправдывающим геноцид и другие общепризнанные преступления против человечества;

– публичные оскорбления или угрозы жизни и здоровью лицам, выделяемым по расовым признакам, национальному или этническому происхождению, а также вероисповеданию.

Борьба с подобными преступлениями затрудняется неоднозначностью понимания свободы слова в разных странах. Достаточно вспомнить случаи с публикациями во французском сатирическом еженедельнике «Шарли Эбдо».

В последнее время все более резонансными становится преступления, связанные с информационным воздействием на личность, путем публикации соответствующего контента в сети Интернет. В большей степени подобному воздействию подвержена молодежь.

Печальную известность получили квесты в социальных сетях, финальной целью которой является самоубийство игрока («Синий кит», «Тихий дом», «Разбуди меня в 4:20», «Море китов», «Млечный путь», «F57», «Красная сова» и т.п.). Опасность суицида от деструктивного воздействия на детское сознание подобных игр, а также клеветы, троллинга, буллинга и других форм агрессивного преследования в социальных сетях настолько возросла, что потребовались существенные изменения уголовного законодательства в части касающейся.

В заключение хочется подчеркнуть, что научно-технический прогресс не стоит на месте, а киберпреступность в своей изобретательности не имеет границ и зачастую опережает правоохранительные органы на несколько шагов вперед. Смещение жизнедеятельности в киберпространство способствует тому, что оно все чаще становится местом совершения преступлений. Проведенный экспресс-анализ позволяет сделать вывод, что киберпреступность – понятие многогранное и борьба с ней – это комплексная проблема информационного общества.

Учитывая вышеизложенное, по убеждению автора, первоочередными мерами повышения эффективности подготовки профессиональных кадров для правоохранительных органов должны стать:

– усиление киберсоставляющей в учебных программах профильных дисциплин;

– активизация творческой деятельности и привлечение к научным исследованиям по изучению передового опыта профилактики, выявления, пресечения и расследования киберпреступлений;

– организация взаимодействия обучающихся с IT-специалистами соответствующего профиля из подразделений МВД России и сторонних заинтересованных организаций.

Библиографический список

1. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // СПС «КонсультантПлюс».

2. Конвенция о преступности в сфере компьютерной информации» (ETS № 185) [рус., англ.] (Принята в г. Будапеште 23.11.2001, с изм. от 28.01.2003) // СПС «КонсультантПлюс».

3. МВД России. – URL: https://мвд.рф/document/11700239.

4. Расследования высокотехнологичных преступлений. – URL: https://www.group-ib.ru/investigation.html.

5. Информационное агентство России ТАСС. – URL: http://tass.ru/proisshestviya/4572560».

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННЫХ РЕСУРСОВ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «СПЕЦИАЛЬНАЯ ТЕХНИКА ОРГАНОВ ВНУТРЕННИХ ДЕЛ»

УДК 378.1:004

Баумтрог В.Э.,
кандидат физико-математических наук, доцент
(Барнаульский юридический институт МВД России)

Аннотация: статья посвящена специфике реализации дистанционного обучения по дисциплине «Специальная техника органов внутренних дел». В статье обсуждаются проблемы формирования электронных материалов по вышеуказанной дисциплине, приводятся ссылки на электронные ресурсы, применяемые в образовательном процессе.

Ключевые слова: специальная техника органов внутренних дел, дистанционное обучение, специальные технические средства, электронный учебный курс, современные информационные технологии.

TO QUESTION ABOUT THE USE OF ELECTRONIC RESOURCES AT STUDY OF DISCIPLINE «THE SPECIAL TECHNIQUE OF ORGANS OF INTERNAL AFFAIRS»

Baumtrog V.E.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Barnaul Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the Article is devoted to the specifics of the implementation of distance learning in the discipline «Special technique of internal Affairs». The article discusses the problems of formation of electronic materials on the above discipline, provides links to electronic resources used in the educational process.

Key words: special equipment of internal Affairs bodies, distance learning, special technical means, electronic training course, modern information technologies.

Для выполнения требований, установленных современными Федеральными государственными образовательными стандартами, образовательные организации обязаны сформировать электронную информационно-образовательную среду, одним из элементов которой являются электронные курсы для информационного обеспечения соответствующих дисциплин.

В Барнаульском юридическом институте МВД России ведется значительная работа по формированию электронных курсов, наполнению их актуальным содержанием. Определенная специфика есть при формировании электронных курсов для обеспечения дисциплины «Специальная техника органов внутренних дел» (далее – дисциплины). Некоторые проблемы и пути их решения предполагается обсудить в рамках настоящей статьи.

Первой особенностью является то, что в рамках дисциплины изучается достаточно большое количество образцов, комплексов систем специальной техники. Так, согласно Перечню образцов (комплексов, систем) специальной техники, принятых на снабжение органов внутренних дел Российской Федерации (с учетом внесенных в него 19-ти изменений на сентябрь 2018 г.), на снабжении МВД России имеется порядка 500 изделий.

Еще большее количество образцов специальной техники является предметом рассмотрения в рамках отдельных тем. Например, при изучении темы «Технические средства защиты информации» обучающиеся знакомятся с Государственным реестром сертифицированных средств защиты информации, в котором содержится около 1800 изделий или технических средств [1]. При рассмотрении темы, посвященной техническим средствам охраны, обучающиеся знакомятся со «Списком технических средств безопасности, удовлетворяющих единым требованиям…» [2], который на текущий момент (сентябрь 2018 г.) содержит 134 изделия. Такое многообразие, с одной стороны, дает широкую возможность преподавателю для вычерчивания индивидуальной образовательной траектории обучающемуся, с другой стороны, требует помещения в образовательный контент информации обзорного характера. Это могут

быть презентации, содержащие в себе как классификацию техники в рамках отдельной темы, так и изображения конкретных ее образцов. Хорошим решением проблемы усвоения многообразия форм является учебный фильм, позволяющий продемонстрировать приемы использования приборов.

Вторая особенность заключается в том, что отдельные темы предполагают знакомство со специальными техническими средствами для негласного получения информации. Образцы таких изделий не содержатся в открытых информационных ресурсах. Перечень такой техники и ее признаки есть в открытых Постановлениях правительства Российской Федерации от 01.07.1996 № 770 и от 10.03.2014 № 214. Как вариант, при формировании обучающего контента возможно размещать ссылки на электронные сведения о подобных изделиях иностранного происхождения. Примеры таких обзоров приведены в хрестоматии по специальной технике органов внутренних дел [3].

Третья особенность изучения дисциплины заключается в ее практической направленности, что требует рассмотрения технических характеристик конкретных образцов. В этой связи стоит привести весьма содержательные сайты отдельных производителей специальной техники, специальных средств. Это официальные сайты компаний: «НПО Специальных материалов» (http://www.npo-sm.ru); «НИИ СТАЛИ» (http://www.niistali.ru); «Армоком» (http://armocom.ru), ООО НПП «Термотекс» (http://www.npptermotex.ru), ЗАО «Техкрим» (http:/techcrim.ru); ЗАО НПЦ Фирма «НЕЛК» (http://www.nelk.ru); «Найстек» (http://nicetec.ru); «Март» (http://marchgroup.ru); «НОВО» (http://www.novocom.ru). Обширная информация содержится на сайте Бюро научно-технической информации (http://www.bnti.ru). Эта компания предоставляет информационные ресурсы базы данных: о технических средствах; аналитический материал (статьи, сообщения, публикации, заключения, аналитические обзоры, результаты испытаний, экспертиз, проблемные статьи, методики, нормативные акты, перечни и т.п.); техническую документацию на изделия; информацию о поставщиках и разработчиках оборудования.

В заключение следует отметить, что весьма важным при формировании электронного контента является опора на ресурс, обеспечивающий круглосуточный доступ к актуальным нормативно-правовым актам технического характера: государственным стандартам, рекомендациям и пр. К таким, по мнению автора, следует отнести «Электронный фонд правовой и нормативно-технической информации» [4]. Опыт эксплуатации настоящего портала показал его безотказную работоспособность. Важной особенностью указанного сайта является наличие небольших по длине электронных адресов источников, что играет свою положительную роль в их описании в литературе.

В частности, для реализации образовательного процесса по дисциплине автором используются следующие основные ГОСТы (в скобках приведен URL), размещенные на вышеуказанном портале: Системы охраны и безопасности. Термины и определения: ГОСТ Р 52551-2016 (http://docs.cntd.ru/document-/1200113776); Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний: ГОСТ Р 52435-2015

(http://docs.cntd.ru/document/1200125960); Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний: ГОСТ Р 52436-2005 (http://docs.cntd.ru-/document/1200043047); Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний: ГОСТ Р 51558-2014 (http://docs.cntd.ru/document/1200113776); Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний: ГОСТ Р 51241-2008 (http://docs.cntd.ru/document/1200071688); Бронеодежда. Классификация и общие технические требования: ГОСТ Р 50744-95 (http://docs.cntd.ru/document/ 1200026028).

Итак, в настоящей статье приведен обзор современных ресурсов, позволяющих наполнить вновь создаваемые курсы по дисциплине «Специальная техника органов внутренних дел», откорректировать имеющиеся материалы, опираясь на современные источники. Приведенные ресурсы также могут использоваться обучающимися для углубления своих знаний в рамках самоподготовки.

Библиографический список

1. ФСТЭК России: технические средства защиты информации [Электронный ресурс]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii-/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00.

2. НИЦ «Охрана»: нормативно-техническая документация: [Электронный ресурс]. – URL: http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html.

3. *Баумтрог В.Э.* Специальная техника органов внутренних дел: хрестоматия / сост. В.Э. Баумтрог. – Барнаул: Барнаульский юридический институт МВД России, 2014. – 142 с.

4. Электронный фонд правовой и нормативно-технической документации [Электронный ресурс]. – URL: http://docs.cntd.ru.

ВОПРОСЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 004.056.53

Земляченко В.В.,
кандидат технических наук, доцент
(Белгородский университет кооперации, экономики и права)

Аннотация: в статье представлены вопросы возможности применения PGP-технологий в государственных информационных системах для обеспечения конфиденциальности, аутентичности и целостности информационных ресурсов (персональных данных).

Ключевые слова: PGP-технологии, информационная безопасность, криптография, открытый ключ, закрытый ключ.

ISSUES OF CRYPTOGRAPHIC PROTECTION OF PERSONAL DATA IN INFORMATION SYSTEMS

Zemlyachenko V.V.,
Candidate of Technical Sciences, Associate Professor
(Belgorod University of Cooperation, Economics and Law)

Abstract: the article presents the questions the possibility of using the PGP-technologies in state information systems to ensure the confidentiality, authenticity and integrity of information re-resources.

Key words: PGP-technology, information security, cryptography, public key, private key.

При использовании средств криптографической защиты информации оператор информационной системы (ИС), гражданин или юридическое лицо, осуществляющее эксплуатацию аппаратно-программных средств ИС, обязан применять сертифицированные средства и строго регламентированные технологии.

Широкое применение в информационном обороте обработки персональных данных выдвинуло целый ряд проблем перед разработчиками и пользователями этих систем. Одна из наиболее важных проблем – это проблема информационной безопасности. Тенденция роста угроз информационным ресурсам (как государственным, так и иной формы собственности объектов информатизации) обуславливает необходимость создания условий функционирования (ИС), гарантирующих защиту законных интересов пользователей сертифицированной информационной системы от противоправных посягательств, недопущения хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения конфиденциальной, в том числе служебной и персональной (личной) информации.

Среди мер по защите информации важное значение отводится криптографической защите информации, основанной на использовании математических приемов и методов, что позволяет использовать открытые каналы связи. При этом лицо, замышляющее неправомерный доступ к конфиденциальной информации, зная о факте передачи интересующей его информации и имея физический доступ к ней, не может понять ее смысла, если не владеет секретным ключом.

Методология организации и обеспечения функционирования криптографических средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, например, в системах персональных данных, определяется «Типовыми требованиями» от 21.02.2008

№ 149/6/6-622, утвержденными ФСБ России [1]. Этот документ указывает, что при передаче персональных данных по каналам связи оператор информационной системы должен применять сертифицированные ФСБ России и ФСТЭК России средства криптографической защиты информации.

Среди криптографических программных продуктов широко известны программы, основанные на технологии PGP Files, относящиеся к «программному обеспечению неприкосновенности частной жизни», написанного на языке Multi-Language и появившегося официально на рынке в 1991 году. Криптографические программные продукты разряда PGP Files используются в таких операционных системах, как Linux, Mac OS X, Windows.

PGP (Pretty Good Privacy) технологии – криптографические приложения для обеспечения защиты и аутентификации данных. Это компьютерная программа, а также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жестком диске.

Аутентификация гарантирует, что если некоторая информация была создана пользователем и выложена для публичного доступа, то она действительно поступила от самого пользователя и не была никем фальсифицирована или изменена в процессе распространения по каналу связи.

Криптографическая стойкость PGP основана на предположении, что используемые алгоритмы устойчивы к криптоанализу на современном оборудовании. Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причем каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из симметричных алгоритмов: AES, CAST5, 3DES, IDEA, Twofish и др.

PGP изначально разрабатывалась для шифрования электронной почты на стороне клиента, но с 2002 года включает также шифрование жестких дисков переносных компьютеров, файлов и директорий, сессий программ мгновенного обмена сообщениям, пакетной передачи файлов, защиту файлов и директорий в сетевых хранилищах, а в современных версиях – еще и шифрование HTTP-запросов и ответов на стороне сервера (mod openpgp) и клиента (Enigform).

Пользователи данного программного продукта криптографической защиты информации отмечают его достоинства и недостатки [2].

В Российской Федерации основными специальными нормативно-правовыми документами, регулирующими разработку и применение криптографических методов и средств защиты информации в государственных информационных системах, являются [3]:

1. Приказ ФСБ РФ от 09.02.2005 № 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (Зарегистрировано в Минюсте РФ 03.03.2005 № 6382).

ПОЛОЖЕНИЕ о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПОЛОЖЕНИЕ ПКЗ-2005).

2. Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств».

ПОЛОЖЕНИЕ о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств.

3. Приказ ФСБ России от 30.08.2012 № 440 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифрования...».

ПРИЛОЖЕНИЕ. Административный регламент Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

4. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Зарегистрировано в Минюсте РФ 06.08.2001 № 2848).

ПРИЛОЖЕНИЕ. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Анализ этих документов показывает, что на сегодняшний день в целом прямых законодательных запретов на использование PGP технологий по криптографической защите информации в России нет. Законодательно ограничивается использование криптографии только в государственных и муниципальных учреждениях. ФСБ предписывает всем государственным структурам использовать только сертифицированные средства криптографии. Физические лица и компании сами устанавливают, какая информация является для них

коммерческой тайной, методы хранения и передачи такой информации. Закон «Об информации, информационных технологиях и защите информации» также указывает, что способ защиты информации, представляющей собой тайну, для негосударственных структур определяется оператором [4].

Информационный ресурс Helpdesk24 [5] в статье «Правомерность использования криптографических средств защиты информации» приводит выдержки из федеральных законов, поясняющие данный вопрос.

Также авторы проекта «OpenPGP в России» утверждают, что не существует законов, запрещающих использование PGP [6].

Электронная подпись, генерируемая с помощью PGP и ее несертифицированных аналогов, имеет юридическую силу в Российской Федерации, т.к. согласно пункту 3 статьи 5 Федерального закона № 63-ФЗ «Об электронной подписи» [7] попадает под определение усиленной неквалифицированной электронной подписи. Согласно пункту 2 статьи 6 этого Федерального закона для признания такой ЭП необходимо соглашение между участниками электронного взаимодействия.

Таким образом, в своей практической деятельности сотрудники служб информационной безопасности должны придерживаться правила, согласно которому использование PGP-технологий в информационных системах для обеспечения конфиденциальности, аутентичности и целостности информационных ресурсов в прямой постановке возможно при соблюдении требований сертификации применяемых средств криптографии. Во всех остальных случаях информационного обмена применение PGP-технологий криптографической защиты информации возможно при взаимном согласии участников электронного взаимодействия.

Библиографический список

1. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ РФ 21.02.2008 № 149/6/6-622) [Электронный ресурс]. – URL: http://www.consultant.ru

2. PGP. [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/PGP

3. Нормативные документы по защите информации [Электронный ресурс]. – URL: https://fstec.ru/

4. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.07.2016) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3448.

5. Правомерность использования криптографических средств защиты информации [Электронный ресурс]. – URL: helpdesk24.ru

6. Проект «OpenPGP в России» [Электронный ресурс]. – URL: https:// www.pgpru.com/.

7. Федеральный закон от 01.07.2011 № 169-ФЗ (ред. от 28.06.2014) «Об электронной подписи» // Собрание законодательства Российской Федерации. 2011. № 15. Ст. 2036.

ПРИМЕНЕНИЕ ЭЛЕМЕНТОВ ДИСТАНЦИОННОГО ОБУЧЕНИЯ НА КАФЕДРЕ ИНФОРМАТИКИ И СПЕЦИАЛЬНОЙ ТЕХНИКИ БЮИ МВД РОССИИ

УДК 378.1

Рычкова Н.В.,
кандидат физико-математических наук, доцент
(Барнаульский юридический институт МВД России)

Аннотация: статья посвящена вопросам использования дистанционного обучения в БЮИ МВД России на примере изучения дисциплины «Правовая статистика». В статье рассматривается применение системы дистанционного обучения «Moodle» в образовательном процессе. Приводится структура учебного электронного курса и его методическое наполнение.

Ключевые слова: дистанционное обучение, система «Moodle», электронный учебный курс, современные информационные технологии, учебный материал.

APPLICATION OF ELEMENTS OF THE CONTROLLED FROM DISTANCE EDUCATING ON DEPARTMENT OF INFORMATICS AND SPECIAL TECHNIQUE OF БЮИ OF МВД OF RUSSIA

Rychkova N.V.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Barnaul Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article is devoted to the issues of using distance learning in the BYuI of the Ministry of Internal Affairs of Russia on the example of studying the discipline «Legal statistics». The article deals with the application of the Moodle distance education system in the educational process. The structure of the e-learning course and its methodological content is given.

Key words: distance learning, «Moodle» system, electronic training course, modern information technologies, educational material.

В настоящее время в мире электронное образование используется повсеместно. Развитие рынка электронного обучения в России, по оценкам специалистов, по сравнению с ситуацией в мире, отстает на 5-7 лет [1].

Система дистанционного обучения «Moodle» (модульная объектно-ориентированная среда) ориентирована в большей степени, по нашему мнению, для организации дистанционного самостоятельного обучения как по очной, так и по заочной формам обучения, в часы самостоятельной работы обучающихся.

Для функционирования системы «Moodle» необходимо программное обеспечение, роль которого выполняет LMS (Learning management system – система управления обучением). LMS представляет собой платформу для развертывания электронного обучения [2].

Применение системы дистанционного образования дает возможность обучающимся самостоятельно изучать учебный материал, а также углублять и закреплять полученные знания и навыки в часы аудиторных занятий, выполняя практические задания, консультироваться с преподавателем и видеть результаты своего обучения.

Использование системы «Moodle» позволяет объективно оценивать степень усвоения учебного материала обучающимися по заочной форме обучения при условии выполнения ими самостоятельно всех заданий, материал которых предусмотрен рабочей программой данной учебной дисциплины. Исходя только из малого количества аудиторных занятий, представляется затруднительным оценивание качества освоения компетенций по учебной дисциплине.

В связи с этим при изучении дисциплины «Правовая статистика» активно используется система дистанционного обучения «Moodle».

Дистанционный курс по дисциплине «Правовая статистика» состоит из следующих блоков:

– **новостной**, где находится форум и оперативная информация для обучающихся;

– **организационный**, где размещены методические материалы для изучения дисциплины, планы занятий, даны ссылки на учебники, находящиеся в электронной библиотечной системе «IPR BOOKS»;

– **учебный,** где по каждой теме дается: теоретический материал, который обучающийся может изучить либо с экрана монитора, либо распечатав его, либо прослушав видеолекцию (по отдельным темам); презентационный материал; примеры выполнения заданий и решения практических задач; вопросы для текущего контроля и самоконтроля знаний, практические задания для закрепления полученных навыков и тестовые задания. В тестовые задания включены вопросы как теоретического характера, так и практического;

– **справочный,** где размещены справочные материалы для более качественного усвоения учебного материала такие, как словарь терминов, наиболее часто используемые формулы и т.п.;

– **контрольный,** где находятся задания для промежуточного контроля знаний и контроля остаточных знаний.

Организационная часть

- Цели и задачи ЭУМП
- Цели и задачи курса
- Обращение к обучающимся
- Рабочая программа дисциплины
- Рабочий тематический план
- Планы занятий для ФПСПиС (40.05.02) Загружено 4/10/17, 13:21
- Электронная библиотека IPRBOOKS
- Правовая статистика / В.Н. Демидов [и др.].
- Портал правовой статистики
- Федеральная служба государственной статистики
- Управление Федеральной службы государственной статистики по АК и Республике Алтай

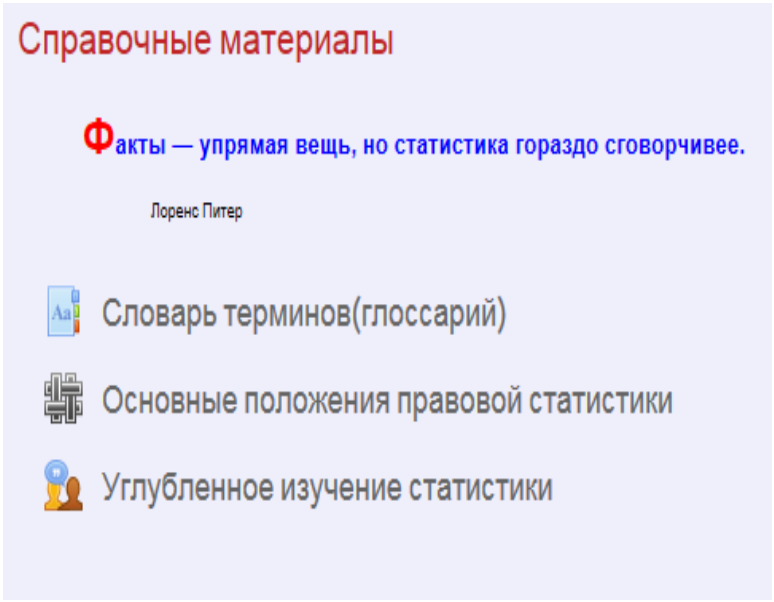
Анализ, обобщение, интерпретация статистических данных

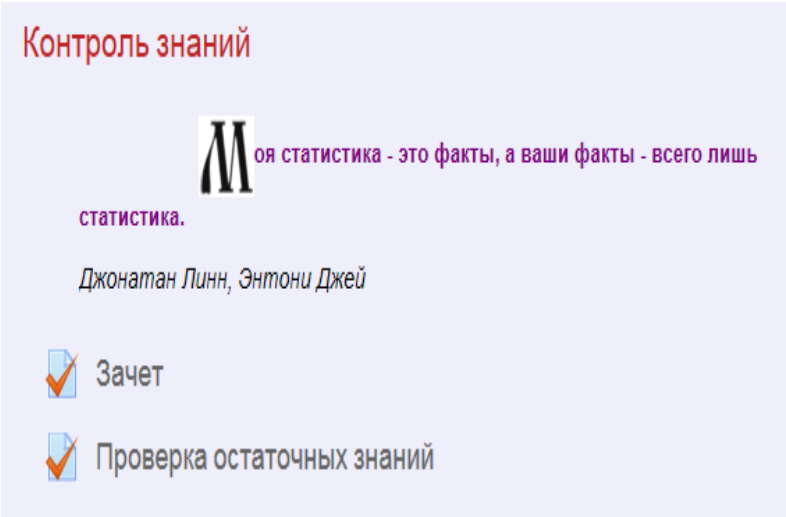
Статистика, возможно, знает все. Но ее знают не все. (Из статистических данных).

Александр Самойленко

- Тема 5. Статистический анализ и прогнозирование
- Статистический анализ, обобщение и интерпретация статистических данных
- Регрессионный анализ Загружено 4/10/17, 13:09
- Сглаживание данных Загружено 4/10/17, 13:08
- Исходные файлы для выполнения заданий
- Анализ и прогноз (Задание для ФПСПиС)
- Анализ и обобщение статистических данных

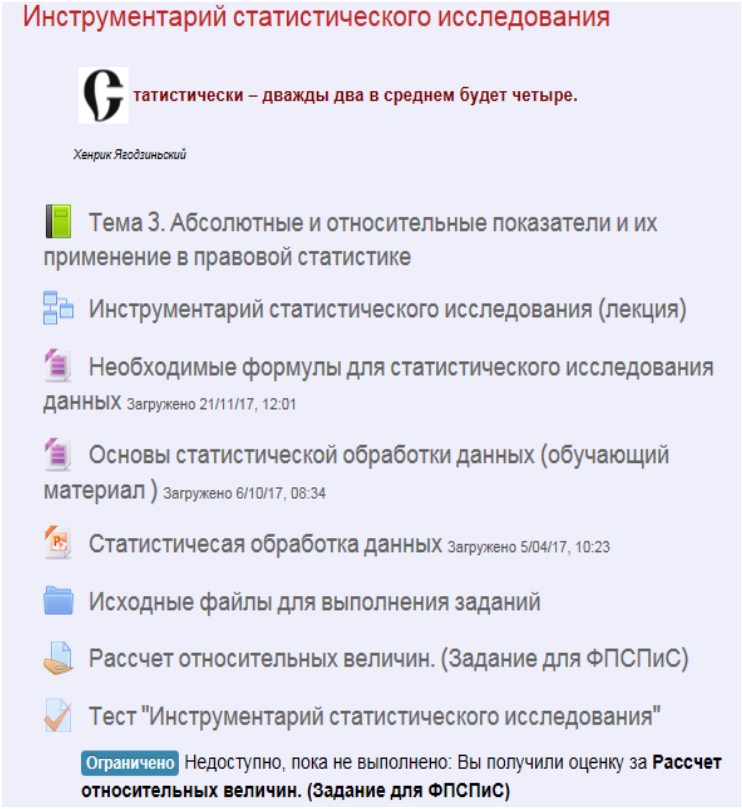
Ограничено Недоступно, пока не выполнено: Вы получили необходимую оценку за **Анализ и прогноз (Задание для ФПСПиС)**





Данный учебный курс настроен таким образом, что выполнение тестовых и практических заданий возможно только после изучения теоретического материала.

Выполненные обучающимися практические задания проверяются преподавателем у каждого обучающегося с возможностью выставления оценки и пояснения или замечания в комментариях, которые доступны обучающемуся. В настройках каждого элемента курса есть возможность указать количество попыток выполнения задания, что стимулирует обучающегося качественно усваивать учебный материал и не посылать неверно или не полностью выполненное задание.



После того, как обучающийся сдал практическое задание, он может перейти к тесту по данной теме. На вопросы теста он может отвечать в любое удобное для него время, не выходя за рамки установленного. Итоговая оценка за тему учитывает результаты самостоятельного выполнения практических и тестовых заданий. Задания теста для промежуточной аттестации состоят из теоретических и практических вопросов.

Проводится данное тестирование в аудитории в присутствии преподавателя.

По результатам опроса слушателей заочной формы обучения в БЮИ МВД России о необходимости использования СДО «MOODLE» при изучении дисциплины можно констатировать, что используют данные ресурсы для самостоятельного изучения во вне учебное время 63%; довольны имеющимися учебными материалами дистанционного обучения 77%.

Таким образом, современные методы обучения благодаря новым информационным технологиям позволяют повысить качество усвоения учебного материала. Использование в лекциях качественной графики, звука, анимации дает возможность более качественного усвоения обучающимися учебного материала. Преимущество электронного учебного курса также заключается в полноте охвата необходимых областей знаний и их достаточной глубине. При появлении вопросов по изучаемым темам у обучающихся они их могут задать преподавателю, используя глобальную сеть Интернет, электронную почту, либо в чате или на форуме. Говоря о необходимости образования и постоянном самообразовании человека в настоящее время, повышении собственной квалификации, мы подразумеваем обучение, которое может происходить на удаленном расстоянии от образовательной организации без отрыва от выполнения своих должностных обязанностей.

Библиографический список

1. Обзор мирового и российского рынка электронного обучения. [Электронный ресурс]. – URL: https://ra-kurs.spb.ru/info/articles/?id=42

2. MOODLE [Официальный сайт]. – URL: http://www.moodle.org

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ПРЕПОДАВАНИЯ ФОРЕНЗИКИ

УДК 378.1

Горев А.И.,
кандидат юридических наук, доцент;
Горева Е.Г.,
кандидат физико-математических наук
(Омский государственный университет им. Ф.М. Достоевского)

Аннотация: рассматриваются вопросы подготовки специалистов правоохранительных органов для противодействия преступности в сфере информационных технологий.

Ключевые слова: форензика, гаджет, формат информации, электронные носители, доказательство.

SOME FEATURES OF THE TEACHING OF FORENSIC

Gorev A.I.,
Candidate of Jurisprudence Sciences, Associate Professor;
Goreva E.G.,
Candidate of Physical and Mathematical Sciences
(Omsk state University F.M. Dostoevsky)

Abstract: the article deals with the training of law enforcement specialists to counter crime in the field of information technology.

Key words: forensic science, gadget, information format, electronic media, proof.

Всеобщая компьютеризация жизни общества и поставленные ориентиры на «цифровизацию» экономики ставит перед правоохранительными органами все более сложные задачи. Уже никто не оспаривает, что стремительное внедрение цифровых технологий породило новые составы преступлений. В некоторых случаях подобные деяния невозможно квалифицировать по действующему законодательству. Однако компьютерные технологии стремительно меняют и традиционные составы: бухгалтерия и документооборот, как правило, исследуются в электронном виде. Прогресс необратим – в ближайшем будущем электронный документооборот полностью вытеснит бумаготворчество. Раскрытие и расследование других видов преступлений также все чаще затрагивает цифровые технологии: сотовая связь, электронная почта, чаты по интересам и социальные сети – вот неполный перечень того, что еще 20 лет назад было экзотикой. Конечно, далеко не каждый, совершающий высокотехноло-

гичное преступление, является хакером[1]. Однако отличительной особенностью преступлений в данной сфере является то, что разработать его может специалист, а выполнить по инструкции – любой пользователь, поскольку запустить на выполнение установленную программу не составляет труда. Более того, уже зафиксированы случаи, когда хакер является разовым наемным работником для легендированной операции аудита безопасности информационно-вычислительной системы, выполнив которую, он по договору получает фиксированное вознаграждение, а нанявшие его преступники – ключи к прорехам безопасности.

Несомненно, что изменение общества ставит перед правоохранительными органами задачи по совершенствованию их деятельности, движению в ногу со временем. В связи с этим возникает вопрос об изменении подходов к подготовке оперативных работников и следователей для работы в современных условиях. Напрашивается необходимость обучения указанных категорий форензике – компьютерной криминалистике. Ведь по отношению к докомпьютерной эпохе в настоящее время возникают вопросы не только отыскать носитель с информацией, но и правильно его идентифицировать, изъять, найти на нем доказательственную базу и приобщить к делу. Сложность данного процесса определена следующими факторами:

– любой современный гаджет (телефон, плейер, навигатор и пр.) может рассматриваться как цифровой носитель, емкость которого определена только установленной карточкой памяти;

– законодательно запрещен оборот закамуфлированных устройств фиксации информации, но для хранения такого запрета нет, что обуславливает широкий оборот носителей, встроенных в часы, ручки, оправы очков, зажигалки и пр.;

– для операций записи/чтения информации широко используются бескабельные соединения разных форматов;

– информация на компьютерный носитель может быть записана в формате стандартных файлов (в настоящее время существует более ста форматов записи информации в файл), а может – в режиме прямого доступа к носителю в обход файловой системы;

– возможно применение программ стеганографии – маскирование данных в иных файлах. В качестве файлов-контейнеров могут быть использованы файлы любого формата (наиболее часто – мультимедиа и графика). В этом случае наличие данных на носителе неочевидно;

– возможно слияние файлов различных форматов, в результате чего на экран будет выводиться информация того файла, чье расширение указывается в конечном формате. Например, если doc – выводится текстовый файл, если xls – электронная таблица;

[1] В нашем понимании «хакер» – высококлассный специалист и может быть как преступником, так и специалистом в сфере защиты информации.

– для записи данных могут применяться экзотические форматы, вплоть до самодельных. Примером может быть формат Radix-50, широко распространенный в 80 гг. XX века и забытый в настоящее время;

– может быть использовано кодирование информации (например, группа шрифтов Wingdings из MS Office преобразует текст в набор графических символов) или криптографическая защита с паролем.

Указанные факторы существенно усложняют доступ к информации и определяют необходимость наличия у каждого участкового, оперработника, следователя специальных познаний в области вычислительной техники хотя бы для определения уровня своей компетентности в конкретной ситуации. На деле, однако, молодые сотрудники правоохранительных органов с навыками пользователей с низкой квалификацией смело берутся за проведение любых оперативных и следственных действий. Внешняя легкость использования компьютерных информационных технологий порождает ошибочное мнение о том, что умения веб-серфинга и пользования персонального компьютера в качестве пишущей машинки достаточны для самостоятельного проведения любых действий без участия специалиста. А ведь большой объем информации о рабочем месте, где был создан или редактировался файл, времени и дате, первоисточниках данных в файлах любого формата может быть получен при исследовании служебной информации, о которой пользователи даже не догадываются.

Результаты такой необразованности приводят к плачевным последствиям. Например, только во время проведения обыска на одном из крупных предприятий г. Омска выяснилось, что в бухгалтерии предприятия для работы с базой данных используются «облачные» технологии, причем используемое «облако» территориально расположено вне пределов Российской Федерации. В другом случае, на изъятом компьютере «продвинутого» злоумышленника эксперт не смог обнаружить даже следов противоправной информации, поскольку, как выяснилось позже, владелец компьютера разбросал свои файлы по общедоступным ресурсам пиринговой сети. Показательный пример был продемонстрирован в новостях НТВ 6 ноября 2015[1]. Сотрудники спецназа штурмом брали офис организации, который располагался в центре Москвы в подвале исторического здания. За полтора часа штурма бронированного помещения преступники успели уничтожить документы и вывести из строя компьютерную технику. И подобные примеры не единичны.

Понятно, что ситуацию необходимо исправлять, но сделать из полицейских специалистов в сфере вычислительной техники нам представляется невозможным. Данный тезис подтверждается следующими соображениями:

– преподавать в юридическом вузе форензику невозможно, поскольку юристы не обладают знаниями в области особенностей работы файловых систем, сетевых протоколов и пр.;

– знания особенностей работы операционных систем и прикладного программного обеспечения невозможно без фундаментальных знаний по математике;

[1] http://www.ntv.ru/novosti/1562899/?fb#ixzz3rFjgnGVX

– совершенствование средств вычислительной техники, появление новых гаджетов и общедоступного программного обеспечения, создание новых технологий общения (мессенжеров, социальных сетей, твитов и пр.) требует пристального наблюдения за данной сферой и ежедневного (!) отслеживания изменений. Понятно, что сотрудник ОВД не имеет для этого ни времени, ни знаний.

Единственный выход из создавшегося положения нам видится в повторении опыта научных рот в Министерстве обороны: привлечение для работы в ОВД специалистов, окончивших математические факультеты университетов. Организовать подготовку специалистов высокого уровня в рамках учебного заведения МВД невозможно из-за отсутствия кадров данной направленности и неподготовленности обучающихся. Имея опыт преподавания дисциплин «Компьютерная экспертиза» и «Расследование компьютерных инцидентов»[1] на факультете компьютерных наук университета можем констатировать, что даже студенты со специальной подготовкой не всегда справляются с поставленными задачами поиска доказательственной информации. Выбор студентов математического или компьютерного факультетов объясним тем, что при обучении программированию студенты знакомятся с методами защиты программ и данных от неправомерного воздействия. А эти знания являются основой компьютерной контркриминалистики[2].

Форензика как наука, появившаяся на стыке традиционной криминалистики и специальных разделов информационных технологий, включает в себя составляющие исходных отраслей. Однако специфика ИТ-отрасли не позволяет ее изучать без предварительной подготовки. Форензику необходимо изучать, имея базовые знания в области построения операционных систем, функционирования сетевых протоколов, структур файлов разных типов и файловых систем в целом и пр. Наивно полагать, что без этих знаний можно понять технологию совершения современных преступлений в области компьютерной информации. А без понимания механизма совершения преступного деяния невозможно установить лиц, его совершивших.

Библиографический список

1. http://www.ntv.ru/novosti/1562899/?fb#ixzz3rFjgnGVX

1 Аналогичные курсы читаются в учебном центре «Информзащита» http://itsecurity.ru

[2] Компьютерная контркриминалистика – противодействие методам поиска, обнаружения и закрепления доказательств в виде компьютерной информации. иными словами, компьютерная контркриминалистика – дисциплина, направленная на противодействие расследованию компьютерных инцидентов и преступлений, а также на противодействие проведению криминалистических исследований и экспертиз компьютерной информации. *Суханов М.* Компьютерная контркриминалистика: состояние и перспективы. – URL: http://www.securitylab.ru/analytics/397811.php

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ КАК ВЫЗОВ ВРЕМЕНИ

УДК 004

Варданян Е.А.,
кандидат философских наук;
Кокоркин В.М.,
курсант
(Ростовский юридический институт МВД России)

Аннотация: вызовы времени актуализируют фокус исследовательского внимания на внедрении искусственного интеллекта и процесса роботизации в функциональную и профессиональную деятельность правоохранительных органов, оценку потенциала применения искусственного интеллекта в работе полиции.

Ключевые слова: информационные технологии, роботизация, искусственный интеллект, технологические инновации, цифровое будущее правоохранительных органов, киберпространство.

INFORMATION TECHNOLOGIES IN THE ACTIVITIES OF LAW ENFORCEMENT BODIES AS A CHALLENGE OF TIME

Vardanyan E.A.,
Candidate of Philosophy Sciences;
Kokorkin V.M.,
Cadet
(Rostov Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: challenges of time actualize the focus of research attention on the implementation of artificial intelligence and the process of robotization in the functional and professional activities of law enforcement agencies, the assessment of the potential of using artificial intelligence in police work.

Key words: information technologies, robotization, artificial intelligence, technological innovations, digital future of law enforcement agencies, cyberspace.

Технологии и информационное развитие не стоят на месте. Мир стоит на грани революции в понимании политики общества и мира в целом. Под влиянием этого развития изменяется культура и цивилизация, и как бы это ни звучало фантастично, но пройдет еще немного времени, и человек станет делить планету с роботами. Роботизация – одна из областей науки и техники, которая, несомненно, будет определять будущее развитие цивилизации в мире ближайшие четверть века [4].

В России уровень роботизации пока крайне низок. Роботы применяются, в основном, в промышленности, на производстве. И может показаться, что роботы-полицейские – это, по-прежнему, информация из области фантастики. Однако будущее наступает и сегодня реально бросает вызов.

Существует мнение экспертов, что роботы будут одной из важнейших технологий XXI века, а широкое их применение первоначально вызовет всплеск их похищений, а также применение в криминальных целях. Уже сейчас дроны и коптеры широко применяются для переправки через границы контрабанды и наркотиков. Это потребует уникальной маркировки каждого робота, системы регистрации принадлежности робота определенному владельцу, ведение журнала его действий, а для некоторых видов сервисных роботов – медицинских, мобильных, охранных – видеорегистрации действий и окружения.

По оценкам Международной федерации робототехники, В России в настоящий момент работают около 5 тыс. роботов, тогда как в Евросоюзе – 380 тыс., в Японии – 540 тыс., а в Китае, по прогнозу, в ближайший год их станет 400 тыс. [4].

Роботы активно внедряются в вооруженные силы и силовые ведомства, в том числе в деятельность правоохранительных органов. Армия, оснащенная перспективными типами и образцами робототехнических комплексов завтрашнего дня, будет обладать неоспоримым интеллектуально-технологическим преимуществом над противником. Все классы вспомогательных и боевых роботов: воздушные, морские, сухопутные, работы для МЧС. По прогнозам, к 2035 году в России, в целом, роботизация войск достигнет от 30 до 80% [4].

Так, например, Москва стала одним из первых мегаполисов, который внедряет распознавание лиц в городской сети видеонаблюдения, состоящей из 170 тысяч камер, в результате чего 70% правонарушений в Москве, включая правонарушения на дорогах, уже раскрывается с помощью систем видеонаблюдения. Однако столичные камеры не включены в систему интеллектуальной разработки изображения и идентификации лиц, возможность внедрения такой системы вполне вероятна и обсуждается аналитиками.

В сентябре 2017 года Президент России В. Путин, выступая в Ярославле на форуме «Проектория», утвердительно заявил: «Лидер по созданию искусственного интеллекта станет властелином мира …Искусственный интеллект – это будущее не только России, это будущее всего человечества. Здесь колоссальные возможности и трудно прогнозируемые сегодня угрозы».

Возникает необходимость актуализации технологических вызовов современности, их практической и методологической оценки. Необходимо определить их роль в функциональном и профессиональном изменении деятельности правоохранительных органов.

Как будет происходить постепенное внедрение разработок искусственного интеллекта и робототехники и других технологических вызовов в функциональную и профессиональную деятельность сотрудников полиции? Какие риски ожидают сотрудников правоохранительных органов и угрозы, исходящие от роботизации отдельных профессиональных функций? Какие разработ-

ки в сфере искусственного интеллекта наиболее популярны и доступны и могут носить характер массового внедрения? Каковы возможности масштабирования опыта внедрения технологических инноваций в деятельность полиции России?

Назрела необходимость реформы образовательных программ в целях подготовки соответствующих компетенций у сотрудников полиции и создания новой образовательной парадигмы в обучении сотрудников правоохранительных органов в отношении изучения сферы информационных технологий, развития когнитивных навыков работы с большими объемами информации и навыков конструктивного функционирования в среде искусственного интеллекта и технологических изменений.

Эксперты и представители различных правоохранительных органов России, в том числе МВД, ФСО, прокуратуры совместно с Всероссийским научно-исследовательским институтом МВД в марте 2017 года проанализировали наступление «киберфизической реальности», в которой гаджеты и люди существуют как в физическом пространстве, так и в «цифре», которую гораздо труднее держать под контролем.

Среди обязанностей сотрудника полиции, отметили эксперты, есть относительно простые функции, которые вполне по силам искусственному интеллекту даже на текущем этапе развития технологий. Среди них, например, обработка огромного количества обращений и жалоб граждан, анализ криминальной статистики в целях прогнозирования, создание макетов для управленческих решений. Специальные программные продукты для полицейских могут применяться для автоматической регистрации выстрелов, распознавания лиц преступников и выявления аномальной городской активности по геотегам.

Более отдаленная перспектива – роботы-полицейские, которые патрулируют городские улицы или «кабинетные» роботы-следователи.

Внедрение новых алгоритмов обработки данных может принципиально изменить работу ГИБДД: если в будущем все машины будут оснащены «черными ящиками», позволяющими в реальном времени получать информацию о водителе, параметрах езды и правонарушениях.

Это только небольшие акценты на изменениях, которые последуют в связи технологической революцией в реализации правовой и правоохранительной деятельности в России.

Свои предложения по регламентированию внедрения технологий в работу полиции на рассмотрение МВД России уже инициировал в январе 2016 года член Общественной палаты РФ, заместитель председателя комиссии по безопасности и взаимодействию с ОНК Дмитрий Чугунов [7]. По мнению Дмитрия Чугунова, оснащение полицейских гаджетами ведет к реальному улучшению показателей их работы и является актуальным в целях повышения мобильности и оперативности работы сотрудников полиции.

Д. Чугунов приводит ряд показательных примеров использования высоких технологий в повседневной работе полиции в странах, где это носит уже массовый характер.

В сравнение, в российских регионах в качестве примеров можно привести пока внедрение отдельных инноваций:

– пилотный проект в ГУ МВД России по г. Санкт-Петербургу и Ленинградской области, где в практику сотрудников полиции внедрен аппаратно-программный комплекс «ПоВАД» для оптимизации процессов создания материалов и сопутствующих им документов в рамках возбуждения административного делопроизводства. За 2014 год с его помощью было составлено более 256 тыс. административных материалов на сумму более 322 млн рублей;

– посты ДПС ГИБДД в столичном регионе (Москва и Московская область) еще с 2006 года оснащены электронной системой «Поток», сопряженной с дорожными видеокамерами. Эта система позволяет в режиме реального времени проверять проходящий автотранспорт на угон и в случае обнаружения автомобиля, числящегося угнанным, немедленно оповещает об этом госавтоинспекторов поста ДПС;

– с 2014 года, начиная с Олимпиады «Сочи-2014», в составе специализированных авиационных отрядов полиции во многих регионах страны наряду с привычной пилотируемой техникой (вертолетами) для контроля дорожной обстановки, воздушной разведки, борьбы с браконьерами и др. активно используются и беспилотники различных типов, мобильные комплексы обеспечения действий которых смонтированы на базе спецавтомобилей «Газель» или «Соболь»;

– в июне 2016 года дроны позволили сотрудникам авиационного отряда МВД по Республике Адыгея за полгода выявить более 150 нарушений ПДД. А в Красногвардейском и Майкопском районах беспилотники позволили обнаружить нарушения в сфере недропользования и незаконные вырубки лесов.

– разработкой и внедрением наиболее перспективных инноваций для полиции и внутренних войск МВД России занимается специализированное подразделение ФКУ «Научно-производственное объединение «Специальная техника и связь» МВД России.

Согласно сообщению пресс-центра МВД, серьезных правовых проблем по использованию беспилотников в рядах силовиков в нашей стране нет. Однако стоит отметить, что даже этот факт не приводит к активному распространению дронов-полицейских в России. Потенциальные возможности использования квадрокоптеров велики – они могут применяться полицейскими в различных ситуациях, вплоть до обезвреживания опасных преступников.

Убеждая в эффективности внедрения современных технологий в оперативную деятельность российской политики, политик уверен, что «повсеместное введение нательных камер для сотрудников нашей полиции положительно скажется на соблюдении законности и правопорядка и гражданами, и самими полицейскими. Даже в нынешней непростой ситуации в стране внедрение в работу МВД достижений высоких технологий, как минимум, высвободит оперативное время для полицейских. Особенно это касается административных правонарушений. Например, если человека задерживают за курение в неположенном месте, то оформление правонарушения и наложение штрафа выстраи-

вается в сложную цепочку действий. Человека сначала задерживают, доставляют в отделение, оформляют протокол, выписывают штраф – все это занимает от двух и более часов.

По утверждению Д. Чугунова, если у сотрудника полиции при себе имеется планшетный компьютер, подключенный к единой информационной системе МВД, портативный банковский терминал, весь процесс оформления штрафа занимает не более 5-10 минут.

В рамках обсуждения практики внедрения высоких технологий спецназначения свое мнение высказал депутат Государственной Думы РФ, первый заместитель председателя комитета по науке и наукоемким технологиям Дмитрий Новиков, подчеркнув, что для этого нужны соответствующие государственные программы и выделение соответствующего бюджета на проведение подобных разработок. Законодатель отметил, что все технологические изменения должны предусматривать соблюдение принципа презумпции невиновности граждан и ограничивать массовый тотальный контроль органов правопорядка над их частной жизнью.

Правоохранителям и законодательным органам различных стран еще предстоит решить юридические вопросы, связанные с возможностями использования искусственного интеллекта и других технологических инноваций.

Что должно измениться для того, чтобы технологическая революция не обошла стороной правоохранительную деятельность как в сравнении с оснащенностью с органами полиции других стран, так и в каждом регионе России? Специалист в области Big Data Иван Бегтин отметил, что прежде всего, необходимо учиться налаживать собственные процессы работы с данными, развивать статистические службы и внедрять новые инструменты прогнозирования. В ином случае, накопление информации с помощью высоких технологий не будет целенаправленно использовано для совершенствования правовой и правоохранительной деятельности. «Работа с данными – это универсальный инструмент, который является базовой подготовкой любого человека в современном мире, – отметил вице-президент Высшей школы экономики Игорь Агамирзян. – Воспользоваться возможностью профессионального и карьерного роста в будущем смогут только те, кто сумеет работать как в физической среде, так и в информационной».

Многие реформы, в том числе правовые, начинаются с образовательных процессов, и технологическое обновление правоохранительных органов – не исключение.

«Цифровое» будущее правоохранительных органов – это и возможности, но и многие риски. Новые технологии приведут к тому, что пресекать преступления или накладывать арест на денежные средства будет значительно сложнее. Привычный юридический язык перестает работать в киберпространстве – трудности при определении потерпевших и квалификации преступлений возникают уже сегодня. Но главная проблема лежит в плоскости кибербезопасности: в будущем для убийства смогут использовать не обычное оружие, а, например, взломанный беспилотный автомобиль. А сеть из ста таких авто-

мобилей сможет вызвать в городе транспортный коллапс и привести к фатальным последствиям.

Под угрозой окажутся элементы «цифровой личности» людей – аккаунты в соцсетях, банковские карточки, сервисы электронной почты. К 2020 году к интернету будет подключено около 50 млрд девайсов, что неизбежно повлечет за собой появление новых способов мошенничества. Экономический ущерб от киберпреступлений к этому времени может вырасти до триллиона долларов в год, а количество «утекших» записей персональных данных из коммерческих компаний и госорганов будет исчисляться в миллиардах единиц.

Для того, чтобы справиться с этими вызовами, полиции будущего нужно будет перейти на новый уровень, где информационные технологии станут обязательной частью повседневной деятельности. Уже сегодня в ст. 11 Федерального закона «О полиции» утверждается, что «…Полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру».

Библиографический список

1. «Беспилотный летательный аппарат БПЛА (дрон)». – URL: http://www.tadviser.ru/index.php

2. В Дубае на службу выйдет робот-полицейский. К 2030 году появится полицейский участок из одних роботов. – URL: https://meduza.io/shapito/2017/05/23/v-dubae-na-sluzhbu-vyydet-robot-politseyskiy-k-2030-godu-poyavitsya-politseyskiy-uchastok-iz-odnih-robotov

3. В мире. Роботы-охранники выходят на патрулирование аэропортов США. – URL: http://guardinfo.online/2017/09/22/v-mire-roboty-oxranniki-vyxodyat-na-patrulirovanie-aeroportov-ssha-video/

4. Вызов 2035. Электронный сборник по инициативе АО «РВК». С. 114.

5. Первый в мире человекоподобный робот София представлен в Москве. – URL: https://www.plusworld.ru/daily/tehnologii/pervyj-v-mire-chelovekopodobnyj-robot-sofiya-predstavlen-v-moskve/

6. Система распознавания лиц помогла полиции Китая поймать 25 преступников на фестивале. – URL: https://news.rambler.ru/other/37835545-sistema-raspoznavaniya-lits-pomogla-politsii-kitaya-poymat-25-prestupnikov-na-festivale-piva/

7. Член Общественной палаты РФ Дмитрий Чугунов просит МВД повсеместно внедрить достижения высоких технологий для повышения эффективности работы полиции. – URL: http://www.interpolitex.ru/media/news/novosti-bezopasnosti/chlen-op-dmitriy-chugunov-prosit-mvd-povsemestno-vnedrit-dostizheniya-vysokikh-tekhnologiy-dlya-povy/

8. Всемирная история полиции. – Москва: Э, 2017. С. 96.

9. *Шваб К.* Четвертая промышленная революция. – Москва: Э, 2017. С. 64.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОРГАНАХ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ В СИСТЕМЕ МВД РОССИИ В ИСТОРИЧЕСКОЙ РЕТРОСПЕКТИВЕ

УДК 347.93:004:94(47)

Познанский Ю.Н.
(Академия управления МВД России)

Аннотация: в статье рассматриваются основные этапы автоматизации отдельных направлений управленческой деятельности руководителей органов предварительного следствия в системе МВД России в исторической ретроспективе.

Ключевые слова: автоматизированная информационная система, информационные технологии, обеспечение деятельности, управление органами предварительного следствия, организация расследования.

USE OF INFORMATION TECHNOLOGIES IN THE BODIES OF PRELIMINARY EFFECTS IN THE RUSSIAN MINISTRY OF FOREIGN AFFAIRS SYSTEM IN THE HISTORICAL RETROSPECTIVE

Poznanskiy Yu.N.
(Management Academy of the Ministry For Internal Affairs)

Abstract: the article discusses the main stages of automation of certain areas of management activities of heads of preliminary investigation bodies in the system of the Ministry of internal Affairs of Russia in a historical retrospective.

Key words: automated information system, information technologies, support of activities, management of preliminary investigation bodies, organization of investigation.

Дискуссия о возможности существенного повышения эффективности процессов управления с применением информационных технологий (далее – ИТ) в научном сообществе ведется достаточно давно. Электронно-вычислительная техника (далее – ЭВТ), с момента ее появления и развития, постепенно внедрялась в производственную и управленческую сферы деятельности человека, помогая ему оптимизировать и ускорять необходимые процессы. Как отмечается в научной литературе, в средине XX века, в результате заметного обострения противоречий, возникшего между потребностями быстрого управления процессами, возросшим объемом информации и психофизиологически-

ми возможностями человека [17, с. 14], было положено начало активному развитию электронного этапа вычислительной техники.

Процесс внедрения ИТ в работу органов предварительного следствия в системе МВД России (далее – ОПС) осуществлялся в ходе общей информатизации общества и практически с момента создания следственных аппаратов в органах внутренних дел (далее – ОВД). Этот факт подтверждается изданным постановлением ЦК КПСС и Совета Министров СССР от 10 декабря 1965 г. «О мерах по улучшению работы следственного аппарата органов прокуратуры и охраны общественного порядка», в котором обращено внимание на необходимость широкого и эффективного применения в следственной практике научно-технических средств…» [15, с. 3]. Однако на начальных этапах, применение ИТ в деятельности руководителей ОПС осуществлялось на основе личной инициативы сотрудников следственных подразделений, имеющих навыки работы с ЭВТ, а затем полученные положительные результаты распространялись среди подразделений МВД СССР.

В период 70-80-х гг. XX в. использование ИТ в основном было ограничено автоматизацией отдельных направлений аналитической работы с информацией по уголовным делам, в частности, путем создания аналитической карточки на разрешенное уголовное дело, приспособленной для обработки в электронно-вычислительной машине (далее – ЭВМ) [4, с. 3], в которых ввод данных осуществлялся с перфокарт или с перфолент [17, с. 14].

Примерно с середины 80-х гг. активное развитие ЭВМ, появление и промышленное производство персональных компьютеров привели к началу использования ЭВМ в деятельности ОПС уже на более качественном уровне. Такой вывод позволил сделать анализ сведений Главного следственного управления МВД СССР за 1988 г., согласно которому, на начало 1988 г. из 111 подразделений МВД, УВД оснащенных вычислительной техникой в 88 были сформированы автоматизированные банки данных [16, с. 133].

Практическое внедрение и использование ИТ в деятельности ОПС сопровождалось и правовым регулированием данного направления деятельности. Одним из основополагающих нормативных правовых актов для системы МВД СССР необходимо назвать программу создания, внедрения и эффективного использования автоматизированных систем и средств вычислительной техники на период до 2000 года. Программа дала толчок использованию средств ЭВМ в деятельности ОВД, в том числе в ОПС, на научной и плановой основе.

Одновременно ЭВМ все чаще стали применять и в образовательном процессе. Так, в середине 90-х гг. в стенах Академии управления МВД России были разработаны программные продукты «Кража – 1» и «Разбой – 1», предназначенные для обучения следователей ОПС в системе МВД России. Программы позволяли имитировать работу следователя по расследованию уголовных дел указанной категории, начиная со стадии рассмотрения заявления, сообщения о преступлении до привлечения лица в качестве обвиняемого [1, с. 122].

В течение 1990-2002 гг. все возрастающая роль персональных компьютеров, появление интернета, массовая обработка и передача информации привели к возникновению новых отношений в обществе, требующих законодательного регулирования. В связи с этим, в период 1991-1996 гг. в стране активно проводилась работа по формированию законодательной базы информатизации. Были приняты ряд федеральных законов и иных нормативных правовых актов на уровне правительства [5]. Аналогичные процессы регулирования информационных отношений происходили и в ОВД РФ. Так, в 1991 г. была утверждена программа компьютеризации ОВД на ближайшую перспективу [14], в которой были определены первоочередные задачи информатизации ОВД, а также изложены основные принципы обеспечения подразделений ОВД средствами ЭВТ. В последствии, в целях реализации идей, заложенных в указанной программе, в 1992 г. было разработано техническое задание на информационно-вычислительную сеть (далее – ИВС) ОВД МВД РФ [8], а в 1996 г. – Концепция развития информационного обеспечения ОВД [10], и Концепция развития ОВД и ВВ [9] (далее – Концепция), в которой перечислены приоритетные направления совершенствования информационного обеспечения системы МВД в целом [2, с. 29].

Одновременно с оптимизацией нормативно-правового регулирования процессов информатизации в этот период осуществлялась разработка и внедрение ИТ в деятельность ОПС. Так, в целях информационной поддержки расследования уголовных дел, на основе интегрированных информационно-вычислительных систем, специализированных банков данных и средств телекоммуникации, создавались аппаратно-программные комплексы и информационные системы (далее – ИС). Вместе с тем, эти ИС имели существенные различия в архитектуре построения, что не позволяло в кратчайшие сроки и при минимальных ресурсных затратах объединить их в единый контур управления [13, с. 5].

Однако указанные различия не стали существенным препятствием на пути информатизации ОПС в системе МВД России и уже в 2000 г. была создана автоматизированная система органов предварительного следствия (далее – АС ОПС) «Гран-УД», в основе которой лежала идея автоматизации отдельных процессов управленческой деятельности руководителя ОПС (в части учета и отчетности) и отдельных процессов, выполняемых следователями. В единую интегрированную систему были объединены две подсистемы: автоматизированное рабочее место руководителя (далее – АРМ «Руководитель») и автоматизированное рабочее место следователя (далее – АРМ «Следователь») [3, с. 106]. Однако использовалась АС ОПС «Гран – УД» редко, т.к. уровень обеспеченности компьютерной техникой ОПС в системе МВД России в это время был довольно низким.

Значительным шагом по автоматизации ОПС в системе МВД России явилось включение подразделений Следственного комитета при МВД России в Программу МВД России «Создание Единой информационно-телекоммуникационной системы органов внутренних дел» [6] в 2004 году, которая содержала

подпрограмму создания «Автоматизированной системы органов предварительного следствия», с целью формирования единого информационного пространства на основе единых технических решений и стандартов. С этого времени началась системная работа по комплексному внедрению ИТ в деятельность ОПС.

Итогом создания АС ОПС должно было стать повседневное внедрение информационных технологий в каждодневную практическую деятельность следователей и руководителей следственных подразделений всех уровней, а также доступ к информационным массивам общего пользования, имеющимся в ОВД [7, с. 198].

В период 2005-2006 гг. в результате проведения опытно-конструкторской работы (далее – ОКР) с активным участием Следственного комитета при МВД России была создана специализированная территориально-распределенная автоматизированная система ОПС (далее – СТРАС ОПС), которая включала в себя следующие основные подсистемы:

– единую автоматизированную систему следственного подразделения (далее – АИС СП), в которую были интегрированы подсистемы АРМ «Руководитель» и АРМ «Следователь»;

– подсистема АРМ «Статистика»;

– программно-аппаратный комплекс банка структурированной информации.

В 2006 году данная работа была окончена. Для ее реализации были изданы ряд приказов МВД России [12].

Подготовленное программное обеспечение АИС СП централизованно было установлено на всех аппаратно-программных комплексах, поставленных в ОПС в рамках Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» (далее – ЕИТКС) в 2006-2008 гг.

Вместе с тем, значительные изменения в уголовном и уголовно-процессуальном законодательстве, произошедшие в 2007-2010 гг., привели к тому, что использование программного средства АИС СП стало практически невозможным, в связи с чем в период с 2011-2012 гг. была осуществлена его модернизация. Однако несмотря на возможности модернизированной версии АИС СП, до настоящего времени она практически не используется по прямому назначению.

Отсутствие специализированного ПО привели к неорганизованной самостоятельной разработке и использованию программных продуктов, позволяющих на минимальном уровне оптимизировать отдельные этапы информационно-аналитической работы начальников ОПС в системе МВД России. При этом использовались различные технические решения, программные платформы, что, в свою очередь, ограничивало круг пользователей, а также возникали проблемы защиты информации.

Ряд задач по организации информационно-методического обеспечения процесса расследования преступлений решается путем использования ресурсов информационного сервера Следственного департамента МВД России, на котором размещаются материалы, предназначенные для оперативного информирования сотрудников следственных подразделений об изменениях в уголовном и уголовно-процессуальном законодательстве, распространения передового опыта, функционируют разделы, содержащие методические рекомендации, аналитические обзоры и указания Следственного департамента, материалы Верховного Суда Российской Федерации.

Несомненно, большим подспорьем для начальников ОПС всех уровней является внедренная в 2015 г. единая система информационно-аналитического обеспечения деятельности МВД России (далее – ИСОД МВД России), которая включает в себя прикладные сервисы обеспечения повседневной деятельности подразделений МВД России (далее – повседневные сервисы ИСОД) и прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России (далее – служебные сервисы ИСОД).

С их помощью возможно оптимизировать решение ряда управленческих процессов начальников ОПС по передаче информации, получения первичной отчётной информации, проведения оперативных совещаний и т.п.

Отдельно необходимо выделить модуль «Уголовное дело», входящий в состав программного обеспечения (сервиса) обеспечения деятельности дежурных частей (далее – СОДЧ), который был разработан в целях оптимизации деятельности сотрудников органов расследования преступлений и управления центров отделов оперативно-разыскной информацией, ставший доступным с 8 июня 2018 года.

Указанный модуль предназначен для накопления информации, собираемой в ходе расследования уголовных дел, в том числе подпадающих под определение преступлений, совершенных дистанционным способом, для последующего анализа данной информации в целях выявления однотипных, серийных и взаимосвязанных преступлений.

В модуле «Уголовное дело» применен принципиально новый подход к представлению и поиску информации, построению взаимосвязей между объектами учета, в том числе с объектом КУСП модуля «Оперативный дежурный» СОДЧ, обеспечивается контроль корректности ввода информации, в том числе для номеров банковских карт, IMEI, банковских счетов, применяются алгоритмы вычисления их контрольных чисел. Разграничение доступа пользователей к ресурсам и функциям модуля «Уголовное дело» СОДЧ регулируется ролевой моделью.

Однако основные функции рассматриваемого модуля не позволяют автоматизировать управленческую деятельность начальников ОПС в части обеспечения оперативного контроля за ходом расследования по каждому уголовному делу, находящемуся в производстве подчиненных сотрудников, выработки единой технологии учета и накопления информации о деятельности ОПС и др.

К сожалению, до настоящего времени ситуация с автоматизацией управленческой деятельности руководителей ОПС в системе МВД России в лучшую сторону не изменилась.

Исследование, проводимое в Академии управления МВД России, позволило сделать ряд выводов относительно состояния автоматизации управленческой деятельности начальников ОПС в системе МВД России:

1) в настоящее время уровень и состояние технического обеспечения ОПС в системе МВД России, особенно на районном уровне, не соответствует реальным потребностям практических органов как в количественном, так и в качественном отношении;

2) констатируется недостаточность обеспечения средствами компьютерной и оргтехникой, которая отражается на возможности начальников ОПС в системе МВД России использовать ИТ и предоставляемые ими возможности в полной мере;

3) фиксируется потребность в специализированном программном обеспечении (далее – СПО), позволяющем автоматизировать отдельные функции управления.

На наш взгляд, повышение эффективности управленческой работы начальников ОПС в системе МВД России возможно путем создания единой автоматизированной информационной системы ОПС в системе МВД России и внедрение ее в качестве служебного сервиса в состав ИСОД МВД России. Сервис может быть создан на основе интеграции возможностей модулей СОДЧ ИСОД МВД России: «Уголовное дело», «Оперативный дежурный» с развитием их функциональных возможностей в части автоматизации управленческой деятельности начальников указанной категории.

Библиографический список

1. Возможности повышения эффективности практического обучения следователей на основе использования средств вычислительной техники // Главное следственное управление МВД СССР. Бюллетень. 1990. № 5.

2. *Кирин В.И.* Регламентация информационных отношений в сфере деятельности органов внутренних дел и внутренних войск / Труды Академии управления. – Москва, 1998.

3. *Литвинцев П.И.* Автоматизация процесса расследования (описание программной системы) // Информационный бюллетень Следственного комитета при МВД России. 2000. № 4 (105).

4. Методические рекомендации по организации и ведению перфокартных систем сбора, накопления, поиска и обработки информации в следственных отделах (управлениях МВД – УВД) // Информационный бюллетень Следственного управления МВД СССР. 1972. № 7.

5. Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации».

6. Приказ МВД России от 14.12.2004 № 896 «Об утверждении программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел».

7. О выполнении программы МВД России «Создание Единой информационно-телекоммуникационной системы органов внутренних дел» и первоочередных задачах органов предварительного следствия по ее реализации // Информационный бюллетень следственного комитета при МВД России 2007. № 3 (133).

8. Приказ МВД России от 26.06.1992 № 207 «О мерах по обеспечению единой технической политики в области создания и внедрения информационных систем ОВД и ВВ МВД России».

9. Приказ МВД России от 20.03.1996 № 145 «О Концепции развития органов внутренних дел и внутренних войск МВД России».

10. Приказ МВД России от 12.05.1993 № 229 «О мерах по реализации концепции развития информационного обеспечения органов внутренних дел».

11. Распоряжение Президента Российской Федерации от 24.09.1992 № 536-рп «О мерах по созданию системы правовой информатизации».

12. Приказ Следственного комитета при МВД России от 03.07.2006 № 29 «О порядке формирования информационных ресурсов автоматизированной системы органов предварительного следствия в системе МВД России».

13. Основные направления комплексной информатизации органов предварительного следствия в системе МВД России на 2002-2006 гг. – Москва, 2002.

14. Приказ МВД РСФСР от 05.07.1991 № 104 «Об утверждении Программы компьютеризации органов внутренних дел РСФСР на 1991 г. и ближайшую перспективу».

15. Проверка работы следственных подразделений органов внутренних дел по применению научно-технических средств и методических рекомендаций в следственной практике // Информационный бюллетень Следственного управления МВД СССР. 1976. № 21.

16. Формирование и активное использование АБД – одна из важнейших задач следствия // Главное следственное управление МВД СССР // Информационный бюллетень. 1988. № 2.

17. *Черников Б.В.* Информационные технологии управления. – Москва: ФОРУМ, 2008. – 352 с.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПРОФИЛАКТИКЕ НАРКОМАНИИ

УДК 004:343.6

Меняйло Д.В.,
кандидат юридических наук, доцент;
Семенюк А.Ф.,
слушатель 254 взвода факультета правоохранительной деятельности
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются технологии использования злоумышленниками информационно-телекоммуникационной сети Интернет в целях распространения наркотиков, Спайса и иных запрещенных к обороту веществ, а также вопросы профилактики наркомании и способы противодействия наркобизнесу с помощью средств информационных технологий.

Ключевые слова: информационные технологии, Интернет, наркотические вещества, наркобизнес, наркодилеры.

USE OF INFORMATION TECHNOLOGIES FOR PREVENTING DRUG ABUSE

Menyaylo D.V.,
Candidate of Jurisprudence Sciences, Associate Professor;
Semenyuk A.F.,
254 students of the law enforcement department platoon
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article discusses the technologies used by cybercriminals of the information and telecommunications network of the Internet in order to spread drugs, Spice and other substances prohibited for trafficking, as well as issues of drug abuse prevention and ways to counter the drug business using means of information technology.

Key words: information technologies, Internet, narcotic substances, drug business, drug dealers.

С появлением в современном мире телевизионной связи, радиостанций и компьютерных технологий, в том числе и сети Интернет, передача и получение информации стала более доступной. Сейчас почти каждый человек умеет обращаться с компьютером, что, несомненно, упрощает процесс информирования и делает информацию для человека более востребованной. Современная молодежь является активным пользователем информационных технологий, полностью погружена в информационный мир, где проводит большую часть

своего времени. Однако, наряду со всеми достоинствами и положительными характеристиками, информационный прогресс имеет свои недостатки. Одним из минусов является то, что в сети Интернет существует большое количество информации, которая носит не достоверный, негативный характер. Так, достаточно часто можно встретить информацию, которая пропагандирует антиобщественный, аморальный образ жизни. Информационные ресурсы оказывают большое влияние на сознание людей, в том числе и на подрастающее поколение, тем самым привязывая негативные привычки, создавая антиобщественную субкультуру и моду. Многие программы, а также сайты и реклама способны кардинальным образом завладеть сознанием людей. Широко известен пример, когда с помощью рекламы пива увеличилось потребление этого пагубного напитка в несколько раз [1]. Напомним, что борьба с чрезмерным употреблением пива в России идет последовательно несколько лет. В июле 2011 года главой государства был подписан законопроект, приравнивающий пиво к остальным алкогольным напиткам и распространяющий на него те же ограничения, в том числе и запрет на рекламу с 1 сентября 2012 года. Согласно проведенному исследованию ВЦИОМ запрет на рекламу алкоголя, в том числе и пива, поддерживает 93% россиян. 1 июля 2014 года Госдума приняла изменения в статью 21 Федерального закона «О рекламе», которые разрешают рекламу пива и алкогольных напитков на основе пива до 31 декабря 2018 года. Поправка вызвана требованием FIFA к чемпионату мира по футболу [2]. На данном примере видно, что с помощью рекламы идет огромное воздействие на сознание человека. Дела с пропагандой наркомании стоят не столь остро, однако проблема информационной профилактики борьбы с наркоманией в настоящее время остается острой. В настоящее время нарастает наркологическая агрессия через сеть Интернет.

Согласно статистике поисковой системы Яндекс количество запросов со словами «травка», «глюк» и т.п. за последние полгода увеличилось на 150% (в среднем от 1,5 до 3 тысяч запросов в день). При этом системы Яндекс, Апорт и Рамблер утверждают, что не поддерживают ни одного наркосайта [1].

Все сайты, которые содержаться в сети Интернет, условно можно разделить на три группы. К первой группе можно отнести такие сайты, которые напрямую рекламируют наркотические вещества. С такой группой сайтов ведут активную борьбу правоохранительные органы в лице Федеральной службы безопасности Российской Федерации, а также сотрудники полиции. В борьбе с такими сайтами сотрудники правоохранительных органов сталкиваются с некоторыми проблемами. Закрыть данный сайт относительно несложно, однако достаточно сложно установить сам факт пропаганды наркотических веществ, так как необходимо определить, что рекламируют именно продукты наркотического содержания. Установление вышесказанного факта уже прерогатива экспертов, филологов, психологов и искусствоведов. Само решение о закрытии сайтов и программ выносит суд. Процедура закрытия сайта достаточно продолжительная. И тут существует еще одна проблема. Сегодня по решению суда сайт закрывают, а завтра он возобновляет работу, но уже под другим

именем, с несколько измененным интерфейсом и содержанием, а иногда даже без изменений. С решением суда о закрытии сайта выносится и решение о штрафе, сумма которого по сравнению с прибылью от деятельности этого сайта незначительна. Поэтому злоумышленники создают сайт заново.

Ко второй группе относятся сайты, которые прямо не рекламируют наркотические продукты, но в них содержится информация о способе приготовления, а также косвенная реклама и различные советы по данному вопросу.

Торговля наркотиками нуждается в регулярной рекламе и пропаганде для привлечения большего числа потребителей, в том числе и молодежи. Так, в Интернете много рекламы различных товаров, таких как футболки, майки, носки и прочих продуктов с изображениями конопли или марихуаны. Все это подсознательно влияет на сознание людей. Также на таких сайтах есть информация по поводу того, как хранить наркотики, как их прятать, алгоритм действий, чтобы избежать ответственности за хранение наркотиков и др.

К третьей группе относятся сайты, в которых также нет прямой рекламы на наркотики, но в них есть различные форумы, где обсуждают и обмениваются информацией по вопросам наркобизнеса. Найти подобный сайт не составляет особого труда для человека, который хоть в малой степени разбирается в сети Интернет. Затем человеку достаточно спросить: «Где найти и купить наркотики?». В течение нескольких минут ему дадут ответ.

Люди, которые занимаются наркобизнесом, создают не одну сотню серверов, с помощью которых происходит, так сказать, «обмен опытом», даются различного рода советы. Основной упор делается на такой вид наркотиков, который якобы не вызывает привыкания. Привлекая человека к такому виду наркотиков, не составляет большого труда в дальнейшем перевести его на потребление более тяжелых видов наркотиков.

Обобщая вышесказанное, можно отметить ряд проблем, которые затрудняют эффективное противодействие членам наркобизнеса. Итак, первая проблема – это невозможность проконтролировать информационный поток в сети Интернет. Человек, который что-то ищет, обязательно это найдет, потратив на это любое количество времени. Вторая проблема – это отсутствие границ в сети Интернет, а также анонимность его пользователей. Так, сам сайт может быть создан за пределами Российской Федерации. В том числе и в странах, где существует легализация наркотиков. Как правило, правоохранительные органы зарубежных стран не отслеживают сайты на русском языке с рекламой наркотиков. Использование зарубежных серверов можно обусловить тем, что российские сервера отслеживают оперативные сотрудники правоохранительных органов на предмет обнаружения нужных кодовых слов. К таким словам обычно относят весь сленг, связанный с наркотическими веществами, который употребляют наркодилеры. При их обнаружении возможно дальнейшее блокирование и проведение соответствующих мероприятий сотрудниками правоохранительных органов. А в иностранных государствах такую выборку делают на иностранном языке, а не на русском, что и оставляет эти сайты незаметными со стороны правоохранительных органов.

Третья и заключительная проблема, с которой можно столкнуться в процессе информационной борьбы с наркоманией, – это невозможность зафиксировать контакт продавца с покупателем при торговле в сети Интернет. Это характеризуется тем, что личные встречи, контакты через курьеров (и так далее) полностью исключены. Получение товара осуществляется в строго определенном месте и определенным бесконтактным способом, а денежные средства переводятся с помощью Интернета.

Все вышесказанные проблемы значительно затрудняют борьбу с наркоманией в наш современный и технологичный век. Для искоренения информационной пропаганды наркотиков, необходимо усовершенствовать и устранить технические проблемы борьбы правоохранительных органов с наркодилерами.

Библиографический список

1. Информационные технологии профилактики наркомании [Электронный ресурс]. – Режим доступа: http://lartdoll.net/osnovnye-tekhnologii-profilaktiki-narkomanii-kurs-lektsij/127-informacionnye-tehnologii-profilaktiki-narkomanii.html (дата обращения: 25.09.2018).

2. Этим летом вы последний раз видите рекламу пива и пьете его так дешево [Электронный ресурс]. – Режим доступа: https://ura.news/articles-/1036271724 (дата обращения: 25.09.2018).

ОСОБЕННОСТИ ПРЕПОДАВАНИЯ МАТЕМАТИКИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ СИСТЕМЫ МВД РОССИИ

УДК 378.1

Ковалева Л.А.,
кандидат физико-математических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Чернова О.В.
(НИУ «БелГУ»)

Аннотация: в статье обсуждается необходимость изучения таких математических дисциплин, как математический анализ, математическая статистика. Новейшие технологии позволяют применять в учебном процессе средства вычислительной техники, разнообразные программные продукты. Отсюда возникает необходимость рассмотреть особенности лекций и практических занятий по математическим дисциплинам в вузах МВД России. Определить совершенно иной подход к проведению занятий, в соответствии с особенностями служебной подготовки будущего офицера полиции.

Ключевые слова: преподавание математики в вузах МВД России, интерактивный метод, дискуссия на занятиях.

FEATURES OF TEACHING MATHEMATICS IN THE EDUCATIONAL ORGANIZATIONS OF A SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION

Kovalyova L.A.,
Candidate of Physical and Mathematical Sciences
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Chernova O.V.
(NIU «BELGU»)

Abstract: in article need of studying of mathematical disciplines, such as mathematical analysis, mathematical statistics and others is discussed when training police officers. The latest technologies allow to apply computer aids, various software products in educational process. From here, there is a need to consider features of teaching lectures and a practical training on mathematical disciplines in higher education institutions of the Ministry of Internal Affairs of the Russian Federation. To define absolutely a different approach to training, according to features of office training of future police officer.

Key words: teaching mathematics in higher education institutions of the Ministry of Internal Affairs of the Russian Federation, an interactive method, a discussion on occupations.

Современный уровень прогресса в обществе и соответственно в структуре МВД, как-то: появление новейших средств наблюдения, технического контроля и программного обеспечения для поддержания функционирования различных технических устройств – выявил необходимость в глубокой математической подготовке сотрудников. Развитие Всемирной сети Интернет и правонарушений, связанных с информационными технологиями, требуют от сотрудников полиции, особенно от офицерского состава, как от руководителя, так и от воспитателя подчиненных, высокого профессионального уровня в данной сфере.

Современный офицер полиции должен уметь критически проверять и логически обосновывать свои действия и точку зрения. В условиях боевой обстановки и в ежедневной службе защитник правопорядка должен уметь моделировать ситуацию, учитывая все мельчайшие детали, рассматривать ее с разных сторон, приводить грамотно выстроенные доказательства, принимать оптимальное решение, учитывая вероятность развития событий.

Важную роль в развитии интеллекта и формирования логического мышления, а также личностных качеств человека играет математическое образование. Благодаря глубоким теоретическим и практическим знаниям сотрудник сможет квалифицированно ориентироваться в научно-, информационно- и технически насыщенном обществе.

Однако на сегодняшний день наблюдается упадок математического образования, начиная со школьной программы. Во многих гражданских вузах и вузах МВД России исчезли такие дисциплины, как математический анализ, теория вероятности и математическая статистика, дискретная математика и другие, а ведь эти дисциплины являются основополагающими для изучения многих юридических дисциплин, например, «Криминологии», «Правовой статистики», «Защиты информации».

Согласно Национальной доктрине образования в Российской Федерации до 2025 года необходимо вести обучение, привлекая информационные образовательные технологии.

В связи с этим необходимо преподавать математику на новом уровне, используя современные компьютерные технологии. Применению в учебном процессе средств вычислительной техники, разнообразных программных продуктов при подготовке специалистов различного профиля посвящены научные работы многих ученых, например, В.П. Дьяконова, А.П. Ершова, А.А. Кузнецова, А.И. Плис, Н.А. Сливиной. Наряду с компьютеризацией учебного процесса нельзя забывать об эффективности обучения математике с использованием информационных технологий. Этот вопрос рассмотрели в своих работах, например, В. П. Беспалько, Е.В. Клименко, Л.Г. Кузнецова, Н.Ф. Талызина [1].

Обучение математике в юридических вузах носит принципиально иной характер. Предлагаемый материал должен быть подобран в соответствии с особенностями служебной подготовки офицера. Необходимо использовать дифференцированный подход, учитывая индивидуальные особенности обучающихся. К наиболее эффективным методам обучения можно отнести применение традиционного и интерактивного подхода [2].

Интерактивный метод может включать в себя, например, дискуссию, как на лекциях, так и на практических занятиях. На лекциях это может быть изучение нового материала посредством диалога с курсантами, в котором преподаватель является собеседником. В ходе такого диалога курсанты сами находят ответы на поставленные вопросы. При этом курсанты учатся мыслить, высказывать свою точку зрения, подбирать весомые аргументы и доказывать свое мнение.

На практических занятиях диалог может состоять в виде групповой игры. Для таких занятий преподаватель подбирает задания, в зависимости от изучаемой темы, и определяет сюжет игры, например, судебное заседание, расследование, викторина. Здесь могут быть задействованы различные видеоматериалы, судебная практика. Однако не стоит забывать, что на занятии будущий полицейский должен научиться принимать решение не только в коллективе. Самостоятельная работа на практическом занятии поможет развить у курсанта чувство ответственности за совершенные действия. Поэтому интерактивный метод должен сочетать в себе коллективное обсуждение и индивидуальную работу. В ходе такого занятия курсанты учатся ставить цель, наблюдать, работать в команде, логически рассуждать, искать взаимосвязи, выделять главные и второстепенные факторы, выстраивать цепочку доказательств и

принимать решение. Контроль знаний обучаемых при интерактивном методе обучения должен осуществляться по ходу занятия.

В результате таких занятий офицер будет знать не только нормативные документы, он научится проводить взаимосвязи между событиями и документами, что является очень важным в работе правозащитника. Знание математических методов даст умение обработать полученную информацию, сделать прогноз на основании статистического материала. Развитое на занятиях логическое мышление позволит правильно оценить любую ситуацию, поставить конечную цель, выделить этапы достижения этой цели, нести ответственность за свое решение.

Библиографический список

1. *Баданов А.А.* Дифференцированное обучение математике курсантов военных вузов МВД России с использованием компьютеров: дис. ... канд. пед. наук. – Новосибирск, 2004. – 192 с.

2. *Зеленина Н.А.* Интерактивные формы и методы обучения математике студентов высших учебных заведений // Концепт. 2014. Т. 16.

РОЛЬ ПРЕПОДАВАТЕЛЯ-ТЬЮТОРА В УСЛОВИЯХ СОВРЕМЕННОЙ СИСТЕМЫ ОБРАЗОВАНИЯ

УДК 159.99

Осинцева Л.М.,
Кирюшин И.И.
(Барнаульский юридический институт МВД России)

Аннотация: в статье рассматриваются проблемы применения информационных технологий и систем обработки информации, так как знания и практические навыки преподавателя по применению и использованию информационных и телекоммуникационных технологий являются основным фактором, который определяет уровень информатизации преподавательской деятельности.

Ключевые слова: преподаватель-тьютор, самообразование, образовательная деятельность, дистанционное обучение, информационные технологии, информационно-образовательная среда.

THE ROLE OF THE TEACHER-TUTOR IN THE MODERN EDUCATION SYSTEM

Osintseva L.M.,
Kiryushin I.I.
(Barnaul Law Institute of the Ministry of Internal Affairs of Russia)

Abstract: the article considers the problems of applying information technologies and information processing systems, since the knowledge and practical skills of the teacher in the use and use of information and telecommunication technologies are the main factor that determines the level of informatization of teaching activities.

Key words: teacher-tutor, self-education, educational activity, distance learning, information technologies, information and educational environment.

Актуальность применения информационных технологий и систем обработки информации в настоящее время приобретает важнейшее значение, так как знания и практические навыки преподавателя по применению и использованию информационных и телекоммуникационных технологий являются основным фактором, который определяет уровень информатизации преподавательской деятельности [4].

Образовательные стандарты третьего поколения предполагают переход к новой информационно-образовательной среде, в которой преподаватель изучает и анализирует возможности, формы, методы и средства обучения, присущие этой среде, а также учебную деятельность обучающихся и результаты этого обучения.

Роль современного преподавателя определяется готовностью к использованию информационно-образовательной среды в профессиональной деятельности. В структуру профессиональной компетенции преподавателя входит формирование готовности к использованию информационно-образовательной среды. Американский ученый-педагог М. Ноулз, занимающийся проблемами обучения взрослых, пришел к выводу: «Подготовка компетентных людей – главная сегодняшняя задача, так как это производство таких людей, которые способны применять свои знания в изменяющихся условиях современного общества и чья основная компетенция заключалась бы в умении включиться в постоянное самообразование на протяжении всей своей жизни» [3]. Можно сделать вывод, что преподаватель-тьютор (консультант) должен использовать все возможности для получения максимального педагогического результата, а именно демонстрировать свое умение по владению и использованию информационно-образовательной среды.

Сравним схематично преподавателя и преподавателя-тьютора (см. рис. 1):

Рисунок. 1. Сравнительная схема преподавателя и тьютора

В непрерывно меняющихся условиях современного общества просто необходимо воспитывать гибкого, динамичного человека, который быстро приспосабливается к новым изменениям. Поэтому очень важно в образовательном процессе выбирать направленность на развитие личности обучающегося как активного субъекта образовательного процесса и всесторонне готовить его к непрерывному процессу образования, саморазвития и самосовершенствования в течение всей жизни [5].

Изменение подготовки преподавателя с точки зрения высшего профессионального образования, прежде всего, зависит от:

- способности овладениями новыми информационно-образовательными технологиями в своей профессиональной деятельности, значительной готовности к самостоятельному принятию решений;
- мобильности и быстрой адаптивности к новым требованиям;
- повышения фундаментальности образования в условиях современного времени, его автоматизации;
- овладения информационными и коммуникационными технологиями вообще и в своей профессиональной деятельности.

Стремительное развитие технологий и возможностей их применения в образовательных целях опережают существующие системы профессиональной переподготовки преподавателей, поэтому в условиях электронного обучения необходимо реализовать подготовку и проведение образовательного процесса с использованием технологий дистанционного обучения, например, в режиме on-line.

На дистанционное обучения в настоящее время возлагаются большие надежды, так как оно включает в себя такие функции как:

- координирование в виртуальной среде познавательного процесса;
- корректировку преподаваемого курса;
- консультирование при составлении индивидуального учебного плана;
- руководство образовательными проектами [1].

Таким образом, методы, с помощью которых происходит управление образовательным процессом, приобретают новое значение. Так как в основе дистанционного обучения стоит бесконтактное взаимодействие между преподавателем и обучающимся, то роль преподавателя значительно усложняется. В связи с этим становятся очевидными противоречия, которые обусловлены тем, что с одной стороны, технологии электронного обучения являются обязательными на всех уровнях образования, а с другой стороны, преподаватели не в полной мере готовы к использованию таких технологий в профессиональной деятельности.

В настоящее время преподаватель уже не является единственным источником правильных знаний, а его мнение на занятиях существует наравне с обучающимися. Поэтому в традиционной системе обучения появляются другие роли преподавателя:

- преподаватель-консультант – знает готовое решение, либо владеет способами, которые указывают на решение проблемы;
- преподаватель-модератор – раскрывает потенциальные возможности обучающегося и его способности;
- преподаватель-тьютор – осуществляет педагогическое сопровождение ученика.

Основные отличия нового подхода состоят в отношении к обучающемуся как к субъекту собственного развития и ориентированы на развитие и саморазвитие его личности.

Роль современного преподавателя показана на следующей схеме (см. рис. 2):

Рисунок. 2. Роль современного преподавателя

Роль преподавателя как субъекта передачи знаний и умений, а также формирования компетенций требует от преподавателя выполнение им функций по формированию компетенции обучающегося в области постоянного и непрерывного обучения, самообразования. В настоящее время способность выпускника к постоянному и непрерывному пополнению знаний и компетенций более важна, чем те конкретные знания и компетенции, которые он приобрел ранее в определенный отрезок времени [2].

Цель инновационных образовательных систем – научить обучающегося ориентироваться определенной сфере деятельности, научить видеть возможности, соотносить их со своими потребностями, ставить цели и самостоятельно достигать их. Поэтому для обучения новым методам работы преподавателей в образовательных организациях должна быть создана новая инновационная среда обучения. Эта среда должна быть доступна для обучающихся, где им будет видна возможность траектории собственного становления, а также средства и методы достижения результатов.

Анализируя теоретические аспекты в мировом образовательном процессе, можно сделать вывод, что важнейшая роль преподавателя заключается в обеспечении поддержки развития и саморазвития личности обучающегося в условиях современного общества, при которой происходит максимальное сочетание личностных, общественных и государственных интересов [6]. Отсюда следует, что преподаватель должен помочь обучающемуся выработать опыт адаптации в условиях быстрого развития цивилизации, а также умения относительно безболезненно вписываться в эти современные процессы.

Таким образом, роль современного преподавателя предполагает с помощью информационно образовательной среды направлять самостоятельность,

предоставленную обучающемуся к целеполаганию, автономизации его познавательной деятельности как основы личностного становления и развития.

Библиографический список

1. *Андрианова Г.А.* Организация творческой деятельности учащихся в дистанционном обучении: дис. … канд. пед. наук. – Москва, 2000. – 212 с.

2. *Горбунов А.П.* Роль преподавателя высшей школы в современную эпоху. – URL: http://pglu.ru/upload/iblock/a3f/roli-prepodavatelya-vysshey-shkoly-v-sovremennuyu-epokhu.pdf

3. *Кленина Л.И.* Совершенствование профессионализма инженеров энергетиков в системе дополнительного профессионального образования: дис. … д-ра пед. наук. – Москва, 2012.

4. *Кирюшин И.И., Баумтрог В.Э.* Использование возможностей сетевых технологий при подготовке специалистов в Барнаульском юридическом институте МВД России // Педагогика и просвещение. 2016. № 1. С. 413-419.

5. *Овчаров А.В., Москаленко Е.В.* Изменение роли преподавателя в условиях современной системы образования // Педагогическое образование на Алтае. – Барнаул: АлтГПУ, 2017. С. 205-208.

6. *Осинцева Л.М., Кирюшин И.И.* Роль межгрупповых соревнований как мотивация обучающихся в Барнаульском юридическом институте МВД России / Формирование и развитие научных знаний студентов и школьников с опорой на комплексный системный подход: сборник научных трудов по материалам IV Международной научно-практической конференции. – Барнаул: Горно-Алтайский государственный университет, 2017. С. 162-166.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГИБДД (ПРОШЛОЕ И НАСТОЯЩЕЕ)

УДК 004.4

Кургузов А.В.
(Омская академия МВД России)

Аннотация: в 2016 году в подразделения МВД была внедрена единая система информационно-аналитического обеспечения деятельности МВД. В рамках этой системы для каждой службы предназначен свой сервис. Для службы Госавтоинспекции сервис называется ФИС ГИБДД-М. В статье описывается путь, который прошло информационное обеспечение ГИББД от бумажных карточек до современных сервисов. В качестве примера приводится подразделение ГИБДД Омской области.

Ключевые слова: информационное обеспечение, ГИБДД, база данных, программа.

INFORMATION SUPPORT OF TRAFFIC POLICE (LAST AND INSISTED)

Kurguzov A.V.
(Omsk Academy of the Ministry of the Interior of Russia)

Abstract: in 2016 in divisions of the Ministry of Internal Affairs the uniform system of information and analytical ensuring activity of the Ministry of Internal Affairs has been introduced. Within this system the service is intended for each service. For traffic police service is called FIS GIBBD-M. In article the way which there has taken place information support of GIBBD from paper cards before modern services is described. As an example it is given divisions of traffic police of the Omsk region.

Key words: information support, traffic police, database, program.

Подразделение ГИБДД последние два десятилетия является одним из лидеров среди подразделений МВД по темпам внедрения различных информационных технологий.

Развитие программного обеспечения ГИБДД началось с середины 90-х годов. До этого времени весь учет велся исключительно в бумажном виде (различные учетные карточки). Сведения о зарегистрированных автомототранспортных средствах хранились в специальных картотеках.

Во второй половине 90-х годов была поставлена задача перевести всю имеющуюся информацию, хранящуюся в картотеке, в электронный формат (к этому времени накопилось уже очень много: данные о зарегистрированных автотранспортных средствах, выданных водительских документах за последние 10 лет). Каждый регион России самостоятельно выбирал технические решения для реализации этой задачи. Например, в Омской области в Информационном центре УВД была разработана программа для внесения уже имеющихся сведений. Программа была консольной, а в качестве СУБД была выбрана популярная в то время система Betrive. Интерфейс разработанной программы был достаточно простой, но в то же время позволял вести учет всех имеющихся сведений.

Почти сразу, после проведения небольших доработок, эта программа стала использоваться в подразделениях ГИБДД для учета при проведении регистрационных действий с автотранспортными средствами. Так появилась первая программа для автоматизированного учета автомототранспортных средств. Учет велся в каждом подразделении ГИБДД по своему району. Во всех подразделениях была рабочая станция и сервер, на котором сохранялась вся информация. Для того чтобы получить базу данных автомобилей всего региона, необходимо было объединить почти три десятка фрагментов. Для поддержания базы в актуальном состоянии эта процедура проводилась ежедневно. Для этих целей в каждом подразделении ГИБДД был установлен dial up модем. Посредством этого модема сведения о совершенных операциях за предыдущий рабочий день передавались в Информационный центр МВД. Это требо-

вало от сотрудников определенных навыков работы с компьютером. Иногда случались сбои, что приводило к потере данных.

Существенным минусом организованной таким образом информационной системы является то, что данные поступают в центральную базу с задержкой. Иногда из-за технических проблем эта задержка могла составлять от нескольких дней до 2-х недель. Эта проблема приводила иногда к существенным трудностям. Например, при совершении ДТП, при котором автомобиль скрылся с места происшествия, невозможно установить его собственника.

Такая организация информационного обеспечения ГИБДД просуществовала почти до конца 2000-х. В 2009-2010 годах на территории Омской области были проведены работы по подключению всех подразделений МВД к единой информационной телекоммуникационной сети МВД (ЕИТКС МВД). С этого момента все подразделения стали работать в единой сети. Это позволило ввести в эксплуатацию новую программу для ведения учета автомобилей, водительских удостоверений и административных правонарушений. Эта программа была уже единой для всех подразделений и работала уже с единой базой данных Oracle всего региона on-line. Появление единой базы данных позволило организовать прием граждан в любом подразделении ГИБДД независимо от их места жительства.

Все это время на федеральном уровне тоже создавалась единая база ГИБДД, которая включала в себя сведения о зарегистрированных автомобилях, выданных водительских удостоверениях, совершенных административных правонарушениях в области дорожного движения. Она создавалась по такому же принципу, что и региональная – собиралась из выгрузок регионов. Весь информационный обмен регламентировался приказом [1]. Этим приказом определяется транспортный формат файлов при информационном обмене. Сотрудники региональных отделов информационного обеспечения ГИБДД передавали сведения в межрегиональные центры ФИС ГИБДД[1], а из них уже непосредственно в федеральный центр в Москве.

Такая система, хоть и просуществовала почти десять лет, имела существенные недостатки:

– сведения поступают в федеральный центр с задержкой даже при соблюдении всех регламентов с задержкой 1-2 дня;

– очень длинная цепочка передачи информации район – регион – МРЦ – федеральный центр, в которой в любом звене, в любой момент может произойти сбой и потеря информации при передаче ее на федеральный уровень;

– при выявлении ошибки ее необходимо исправить во всех фрагментах баз данных.

В 2014 году в связи с изменением концепции развития информационных систем МВД России был осуществлен переход с платформы ЕИТКС на современную интегрированную мультисервисную телекоммуникационную систему[2]. В результате была создана информационная система обеспечения деятельности

[1] Далее – МРЦ.
[2] Далее – ИМТС.

ОВД МВД России[1]. В 2016 году на базе ИМТС после непродолжительного тестирования в нескольких регионах по всей России началось внедрение единого программного обеспечения – ФИС ГИБДД–М. ФИС ГИБДД-М включает в себя следующие подсистемы:

1. «Транспортные средства» – регистрация автомототранспортных средств и прицепов к ним.
2. «Водительские удостоверения» – прием экзаменов на право управления ТС, выдача водительских удостоверений, учет сведений о правах лиц на управление ТС.
3. «Административные правонарушения» – учет административных правонарушений ПДД.
4. «Специальная продукция» – учет изготовленной и распределенной специальной продукции, сбор заявок о потребности в бланках специальной продукции, розыск специальной продукции.
5. «Экзаменационный класс» – проведение теоретической части – квалификационный экзамен на получение права управления транспортным средством.
6. «Запрос» – отправка и получение результатов по запросам.

Таким образом, ФИС ГИБДД-М включает в себя подсистемы для всех видов учетов, используемых в ГИБДД. Подсистемы обеспечивают структурированный доступ к различной поисковой информации, путем подачи информационных запросов. При этом поиск может осуществляться как по всем подсистемам, так и в конкретной подсистеме. Функционирование данной системы регламентируется приказом МВД России [2].

ФИС ГИБДД-М призвана значительно облегчить работу сотрудников и подразделений Госавтоинспекции. Больше нет необходимости производить ежедневные выгрузки. Любой гражданин теперь может поставить машину на учет, поменять водительское удостоверение в абсолютно любом подразделении ГИБДД России. Система является Федеральной, хотя и включает информацию регионов. Это значит, что сотрудники, находящиеся в разных регионах, могут получать одинаковый доступ к информации, которая вносилась в другом регионе. Важность данной системы невозможно переоценить. Она вносит значительный вклад в ускорение и автоматизацию многих рабочих моментов, осуществляемых ГИБДД.

Библиографический список

1. Приказ МВД России от 03.12.2007 № 1144 (с изм. и доп.) «О системе информационного обеспечения подразделений Госавтоинспекции» // СПС «КонсультантПлюс» [Электронный ресурс]. – Режим доступа. – URL: http://www.consultant.ru

2. Приказ МВД России от 02.02.2016 № 60 (с изм. и доп.) «О порядке эксплуатации специального программного обеспечения Федеральной информационной системы Госавтоинспекции» [Электронный ресурс]. – Режим доступа. – URL: https://mvd.consultant.ru/documents/1055896

[1] Далее – ИСОД.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОДГОТОВКИ СОТРУДНИКОВ ПОЛИЦИИ К СОЦИАЛЬНОМУ ВЗАИМОДЕЙСТВИЮ

УДК 378

Белимова А.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в условиях доминирования в деятельности российской полиции социальной функции, анализируются целевые установки традиционного ведомственного образования и обосновывается необходимость определения интегрированного образовательного результата в рамках ФГОС. В качестве такого результата предлагается социальный опыт обучающегося, представленный отдельными общекультурными компетенциями. Рассматривается алгоритм методического обеспечения психолого-педагогической подготовки сотрудника полиции к социальному взаимодействию в вузе МВД России.

Ключевые слова: социальное взаимодействие, сотрудник полиции, подготовка социальная компетентность, методическое обеспечение.

METHODOLOGICAL SUPPORT OF TRAINING OF POLICE OFFICERS TO SOCIAL INTERACTION

Belimova A.A.
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: in the conditions of domination of the social function of the police in the activities of the Russian police, the author analyzes the target settings of traditional departmental education, and substantiates the need to determine the integrated educational outcome within the framework of the GEF. As a result, it is proposed a social experience obuchayuschee submitted by individual cultural competences. The algorithm of methodological support of psychological and pedagogical training of police officers for social interaction in the University of the Ministry of internal Affairs of Russia is considered.

Key words: social interaction, police officer, training social competence, methodological support.

Институт российской полиции находится в стадии активного реформирования, обусловленного недостаточно эффективной деятельностью органов внутренних дел по обеспечению правопорядка и борьбе с преступностью. Одним из стратегических направлений этого процесса является подготовка будущих специалистов в вузах МВД России к реализации социальной функции

полиции, заключающейся в оказании услуг населению и иным потребителям в сфере правоохранительной деятельности. Министерство внутренних дел Российской Федерации последовательно реализует стратегию открытого взаимодействия органов внутренних дел с гражданами и институтами гражданского общества.

Полиция не только борется с преступностью и обеспечивает безопасные условия жизни граждан, но и является активным участником построения гражданского общества в России. Федеральные государственные образовательные стандарты по специальности «Правоохранительная деятельность» в качестве образовательного результата на первое место выдвигают социальную компетентность будущего специалиста, представленную совокупностью общекультурных компетенций. Объединяет этот комплекс компетенций целостная профессиональная деятельность сотрудника полиции, протекающая в постоянном социальном взаимодействии в процессе решения профессиональных задач. От курсанта, освоившего образовательную программу вузовской подготовки, требуется готовность и способность адекватно ориентироваться в усложняющихся условиях социально-культурной полиэтнической среды, принимать взвешенные социально значимые процессуальные решения на основе своей системы ценностных ориентаций и нравственно-этических принципов с учетом множества разнообразных факторов.

Необходимо отметить, что система социального воспитания и социального обучения в ведомственных вузах МВД России, призванная обеспечивать необходимый уровень социальной компетентности выпускника, недостаточно эффективна. Образовательный процесс нацелен на подготовку специалиста юридического профиля, но не на развитие его социального опыта, который формируется у обучающихся стихийно и без должного психолого-педагогического обеспечения.

Предоставленные вузу академические свободы по выбору содержания образования и применении образовательных технологий позволяют на уровне кафедры и предметов психолого-педагогического цикла усилить социально-психологическую и социально-педагогическую подготовку сотрудников полиции к решению предстоящих проблем и трудностей в социальном взаимодействии. Это направление оптимизации образовательного процесса в вузе МВД России требует научно обоснованных теоретических и методических рекомендаций по организации этой работы. На кафедре психологии и педагогики Белгородского юридического института МВД России имени И.Д. Путилина совместно с сотрудниками учебного отдела в течение трех лет ведется научно-исследовательская работа по подготовке сотрудников полиции к социальному взаимодействию.

В рамках этой научно-исследовательских работ разрабатываются теоретико-методологические основы данного процесса. В условиях реализации компетентностного подхода, в основу современных образовательных стандартов заложены идеи и принципы компетентностного подхода, активно разрабатываемого учеными-педагогами Г.А. Берулавой [1], В.Я. Болотовым [2], А.А. Вер-

бицким [3], В.В. Сериковым [2], идеи, теории и концепции которых являются устойчивыми ориентирами в нашей работе.

Однако теоретико-методологические основания подготовки сотрудников полиции к социальному взаимодействию требуют соответствующего выбора содержания образования, образовательных технологий и методического обеспечения. Современные требования к вузовскому образовательному процессу обязывают неукоснительно соблюдать условия реализации основных профессиональных образовательных программ (ОПОП) в части формирования и оценивания образовательного результата. Для соблюдения этого требования преподаватели в рамках учебно-методических комплексов разрабатывают учебные программы дисциплин и фонд оценочных средств, обеспечивающих контроль за качеством достигнутого результата – сформированных компетенций. Педагоги и методисты учебного отдела сталкиваются с проблемой оценивания каждой компетенции, содержащейся в стандарте, но реализуемой в рамках отдельных преподаваемых дисциплин, порой, разными кафедрами.

Решение этой методической проблемы лежит в плоскости методологических подходов, в частности, личностно-ориентированного и системного подходов. А.Я. Данилюк, А.М. Кондаков предлагают подобные проблемы решать на основе постановки и достижения единой образовательной цели всего социума – развитие человеческого потенциала средствами воспитания и социализации в условиях модернизации России [4].

На уровне ведомственного вуза эта цель может быть декомпозирована до уровня развития человеческого, социального потенциала каждого обучающегося, посредством формирования и развития социального опыта личности. Передача социального опыта от одного поколения другому является элементом предмета педагогики, в том числе и профессиональной педагогики. Цель всестороннего развития человека провозглашена и в законе «Об образовании в Российской Федерации», однако, в реальном образовательном процессе такая цель не реализуется, а сам процесс носит ярко выраженный предмето-центристский характер.

В основу разработки методического обеспечения преподаваемых предметов психолого-педагогического цикла положена идея достижения единого, интегрированного образовательного результата – социальной компетентности будущего специалиста, включающей в себя ценностно-смысловой, социально-когнитивный, регулятивно-деятельностный и рефлексивный компоненты. Представлен каждый из компонентов предметными и процессуальными знаниями, умениями, способами выполнения соответствующего элемента (этапа) социального взаимодействия. Дискрипторы каждой из общекультурных компетенций, содержащихся в ФГОС, составляют основу содержания социальной компетенции, дополняемую недостающими элементами психологической и организационной структур социального взаимодействия. Таким образом, в качестве интегрированного результата преподаваемых дисциплин психологического и педагогического блоков выступает социальный опыт обучающегося, актуализирующийся и развивающийся в ходе освоения разных дисциплин в

виде отдельных модулей единого образовательного процесса. Такой алгоритм построения методического обеспечения требует координации усилий кафедры психологии и педагогики и планирующих образовательный процесс подструктур института.

Библиографический список

1. *Берулава Г.А., Берулава М.Н.* Новая методология развития личности в информационном образовательном пространстве // Педагогика. 2012. № 4. С. 11-20.

2. *Болотов В.Я., Сериков В.В.* Компетентностная модель: от идеи к образовательной программе // Педагогика. 2003. № 3. С. 8-14.

3. *Вербицкий А.А.* Реализация компетентностного подхода в образовательном процессе» (из материалов «круглого стола») // Педагогика. 2013. № 3. С.100-121.

4. *Данилюк А.Я., Кондаков А.М.* Развитие человеческого потенциала средствами воспитания и социализации в условиях модернизации России // Педагогика. 2011. № 1.

СОДЕРЖАНИЕ

НАУЧНОЕ ИЗДАНИЕ

ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Сборник статей
5-й Международной научно-практической конференции

12 октября 2018 г.

Редактор ***О.Н. Тулина***
Техн. редактор ***Т.Л. Ковалева***

Подписано в печать 2019 г., формат бумаги 60х90/16, уч.изд.л. 20,0,
бумага офсетная, печать трафаретная
Тираж 33 экз., заказ № 3

Отпечатано в отделении полиграфической и оперативной печати
Белгородский юридический институт МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-269-2