ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МИНИСТЕРСТВА
ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(ФГКОУ ВО РЮИ МВД России)

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Сборник материалов
Всероссийской научно-теоретической конференции

(22 апреля 2022 г.)

Ростов-на-Дону
2022

УДК 004:351.74
ББК 32.973
С 568

С 568 **Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел** [Электронное издание] : сборник материалов Всероссийской научно-теоретической конференции (22 апреля 2022 г.) / отв. ред. – С. В. Лемайкина. Электрон. дан. (1,49 МБ). – Ростов-на-Дону : ФГКОУ ВО РЮИ МВД России, 2022. – 1 электрон. опт. диск (CD-R). – Систем. требования: IBM PC, 1GHz; 512 mb оперативной памяти; 3 mb ОЗУ; CD/DVD-ROM дисковод; операционная система Windows XP и выше; Adobe Acrobat Reader 8.0 и выше.

ISBN 978-5-89288-477-8.

Сборник подготовлен по итогам Всероссийской научно-теоретической конференции. В материалах сборника рассматриваются особенности применения современных информационных технологий в профессиональной деятельности сотрудников органов внутренних дел.

Предназначен для педагогических работников, адъюнктов, курсантов и слушателей образовательных организаций МВД России.

Выпускается по решению редакционно-издательского совета

ФГКОУ ВО РЮИ МВД России.

ISBN 978-5-89288-477-8

УДК 004:351.74
ББК 32.973

СОДЕРЖАНИЕ

В.Л. Акапьев,
С.Е. Савотченко,
Е.Г. Ковалева

ПРАКТИКО-ОРИЕНТИРОВАННОЕ ОБУЧЕНИЕ ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ В РАМКАХ ВНЕДРЕНИЯ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Количественный и качественный состав программного обеспечения, используемого в правоохранительной деятельности, предъявляет повышенные требования к сотрудникам ОВД, которые широко применяют современные информационные технологии в своей повседневной деятельности. В этой связи, важнейшую роль в подготовке квалифицированных специалистов играет система профессионального образования [1].

Ключевым элементом реализации образовательного процесса выступают конкретные методики формирования информационно-технологической компетентности сотрудников ОВД в рамках организации и проведения занятий по соответствующим учебным дисциплинам.

Для преподавателей важно соблюдение следующих основных методических моментов:

1. Как полно будут изучены базовые понятия информатики и информационных технологий, настолько эффективным будет результат применения средств вычислительной техники и программного обеспечения в профессиональной деятельности [2].

2. Наиболее ценными являются такие знания, которые отражают общие законы информатики и логики, и вытекающие из них практические навыки [3].

3. Основными установками при изучении тем данной дисциплины являются приобретение теоретических знаний о базовых (видовых) навыков работы со средствами вычислительной техники и программным обеспечением, и на их основе формирование умений и навыков принимать решения об оптимальном выборе таких средств для решения профессиональных задач в ОВД [4; 13].

Для каждой лекции предполагаются три вида целей: учебная, воспитательная и развивающая. Учебные цели лекции различаются в зависимости от тем. Две оставшиеся можно сформулировать по сформировавшимся шаблонам для всех тем одинаково.

Качество проведения аудиторных занятий оценивается по следующим основным критериям:

1. В сфере организации учебной деятельности:

– четкость постановки целей и задач занятия;

– соответствие выбранной формы целям и задачам занятия;

– степень вовлеченности аудитории в учебную работу;

– способность создания оптимального контакта с аудиторией;

– обеспеченность занятия методической документацией.

2. В сфере организации познавательной деятельности слушателей:

– использование в ходе занятия активизирующих методов и учебных форм (проблемного метода, метода разбора ситуации, метода мозговой атаки, дискуссионного метода);

– дифференцированное и индивидуализированное распределение учебных занятий в соответствии с учебными интересами слушателей и уровнем способностей;

– ориентация слушателей на самостоятельную поисковую деятельность.

3. В сфере организации контроля:

– соответствие форм контроля форме занятия;

– объективность оценочных суждений преподавателя;

– ориентация слушателей на самоконтроль и самооценку;

– использование форм взаимного слушательского контроля.

Рекомендации проведения семинарского занятия:

– разъяснение учебного материала и его обсуждение;

– репродуктивный, поисковый, творческий – при отработке вопросов семинарского занятия.

Местом проведения семинарских занятий является учебная аудитория согласно расписанию. Материально-техническое обеспечение: компьютеры, ученическая доска. Учебно-материальное обеспечение: конспект лекций, учебники, рабочие тетради.

Для каждого семинара предполагаются три вида целей: учебная, воспитательная и развивающая. Учебные цели семинаров различаются в зависимости от тем. Две оставшиеся можно сформулировать следующим образом для всех тем одинаково:

– развивающая цель семинаров: развитие познавательных способностей, мышления, памяти, способности сравнивать и анализировать.

– воспитательная цель семинаров: формирование у курсантов профессионально-значимых качеств: умения правильно и полно выполнять поставленные задачи, внимательность.

Порядок проведения практических занятий:

1. В начале занятия преподаватель проверяет наличие обучаемых в учебном взводе.

2. Преподаватель объявляет тему и цели занятия.

3. Обучаемые изучают цели занятия, учебные вопросы, задания.

4. Преподаватель осуществляет групповое рассмотрение изученных вопросов.

5. В конце занятия преподаватель проверяет выполненную работу, подводит итоги.

6. Задание на самоподготовку преподаватель выдает индивидуально каждому курсанту, с учетом его подготовленности.

Рекомендации проведения практических занятий

1. На занятиях используется практический метод обучения.

2. Обучаемые работают под руководством преподавателя.

Местом проведения практических занятий является учебная аудитория согласно расписанию.

Материально-техническое обеспечение: компьютеры, мультимедийный проектор.

Для каждого практического занятия предполагаются три вида целей: учебная, воспитательная и развивающая. Учебные цели практических занятий различаются в зависимости от тем. Две оставшиеся можно сформулировать следующим образом для всех тем одинаково:

– развивающая цель практических занятий: развитие познавательных способностей, мышления, памяти, способности сравнивать и анализировать.

– воспитательная цель практических занятий**:** формирование у курсантов профессионально-значимых качеств: умения правильно и полно выполнять поставленные задачи, внимательность [5; 137–139].

По итогам практического занятия работа каждого курсанта должна быть оценена преподавателем с выставлением оценки в электронный или «твердый» журнал.

Основными формами контроля усвоения знаний и формирования практических навыков по дисциплине являются оценки за своевременность и качество выполнения заданий на практических занятиях; оценки за выполненные рефераты и доклады; оценки за результаты самостоятельной работы курсантов и слушателей под контролем преподавателя; оценки, полученные в ходе индивидуальных консультаций и собеседований; оценки при сдаче экзамена по данному курсу [6].

В случае невозможности проведения устного экзамена промежуточная аттестация по учебной дисциплине проводится в соответствии с Методическими указаниями для сотрудников, проходящих профессиональное обучение (профессиональную подготовку) по заочной форме обучения с использованием дистанционных образовательных технологий. Определяют порядок проведения экзамена у слушателей факультета заочного обучения в дистанционной форме с использованием электронной информационно-образовательной среды БелЮИ МВД России [7].

Данная форма итоговой аттестации также применима и к курсантам, обучающимся по очной форме.

Под дистанционными образовательными технологиями (далее – ДОТ) понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и профессорско-преподавательского состава. ДОТ может выступать в качестве подсистемы более общей технологии, описываемой понятием – электронное обучение.

Под электронным обучением понимается организация образовательной деятельности с применением содержащихся в базах данных и используемых при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических

средств, а также информационно-телекоммуникационных сетей, передачу по линиям связи указанной информации, взаимодействие обучающихся и профессорско-преподавательского состава.

Под электронной информационно-образовательной средой (ЭИОС) понимается совокупность электронных образовательных ресурсов, совокупность информационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ, а также взаимодействие обучающихся с профессорско-преподавательским составом, учебно-вспомогательным, административно-хозяйственным персоналом и между собой.

Целью профессионального обучения с использованием ДОТ является формирование у слушателей творческого мышления, ориентированного на выработку наиболее рациональных методов профессиональных действий, овладение ими системой современных знаний, умений и навыков, обеспечивающих эффективное, в строгом соответствии с законом и при широком использовании положительного опыта решение оперативно-служебных задач, а также реализация возрастающих потребностей в подготовке высококвалифицированных кадров для органов внутренних дел на основе использования информационных технологий обучения, развитие образовательного пространства, снижение учебной нагрузки на профессорско-преподавательский состав и экономия денежных средств.

Промежуточная аттестация в виде экзамена проводится для определения степени достижения учебных целей по учебной дисциплине в форме тестирования.

Сегодня современный мир располагает изобилием информационно-коммуникационных технологий, применяемых в различных сферах деятельности. В современных условиях в процессе подготовки высококвалифицированных кадров для органов внутренних дел самым актуальным стало умение специалиста использовать компьютерные информационные технологии как в профессиональной, так и в повседневной жизнедеятельности. Культура общения с компьютером стала частью общей культуры человека [8].

Предлагаемая методика преподавания дисциплины предназначена для использования в качестве пособия в форме рабочей тетради в практи-

ческой деятельности преподавателей образовательных учреждений МВД России. Она составлена с учетом рекомендаций по написанию частных методик преподавания учебных дисциплин, разработанных ИМЦ ГУК МВД России, и примерных учебных программ для вузов МВД, разработанных на кафедре информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России, в соответствии с требованиями государственных образовательных стандартов, а также на основании теоретических разработок дидактических проблем, выполненных на кафедре с учетом многолетней практики обучения специалистов [2; 7–8].

Для реализации образовательных методик и технологий необходимо наличие соответствующего единого информационного пространства образовательной организации. Важное место здесь занимает разработка качественного информационно-методического обеспечения образовательных технологий [9; 82].

На используемые методики преподавания учебных дисциплин, ориентированных на формирование информационно-технологической компетентности специалиста, накладывают свой отпечаток особенности организации учебного процесса в условиях пандемии.

Литература

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг.: Указ Президента Российской Федерации от 09.05.2017 № 203. Доступ из справ. правовой системы «КонсультантПлюс».

2. Акапьев В.Л. Формирование информационно-технологической компетентности сотрудников ОВД: монография. Белгород, 2015.

3. Компетентностный подход в профессиональном образовании [Электронный ресурс]. URL: http://www.syl.ru/article/173512/new_kompetentnostnyiy-podhod-kompetentnostnyiy-podhod-v-professionalnom-obrazovanii (дата обращения: 04.09.2018).

4. Об утверждении Требований к информационному взаимодействию уполномоченной субъектом Российской Федерации организации и территориального органа МВД России, включая правила передачи данных

по каналам связи с использованием информационных систем: приказ МВД России от 22.05.2018 № 319. Доступ из справ. правовой системы «КонсультантПлюс».

5. Савотченко С.Е. Программно-педагогические аспекты формирования компонентов единого информационного пространства образовательного учреждения // Интерактивные и мультимедийные средства в предметном обучении: сборник трудов региональной научно-практической конференции. Белгород, 2009.

6. Систематизация подходов формирования профессиональной компетентности [Электронный ресурс]. URL: http://studopedia.ru/15_ 115164_-sistematizatsiya-podhodov-formirovaniya-professionalnoy-kompetentno-sti.html (дата обращения: 04.09.2018).

7. Акапьев В.Л. Методические и педагогические аспекты комплексной информатизации образовательных организаций системы МВД России // Информатизация и информационная безопасность правоохранительных органов: сборник трудов XXVI Всерос. научн. конф. М., 2017.

8. Савотченко С.Е. Разработка и применение средств диагностического контроля в преподавании дисциплин общегуманитарного цикла // Информационные технологии в гуманитарном образовании: материалы II Междунар. научно-практ. конф. Пятигорск, 2009.

9. Bovet D.P., Cesati M. Understanding the Linux Kernel, O?Reilly & Assoc., 2003.

А.В. Краинский

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОВЕДЕНИЯ ПРАКТИЧЕСКОГО ЗАНЯТИЯ В ДИСТАНЦИОННОЙ ФОРМЕ ПО ДИСЦИПЛИНЕ «ТРАСОЛОГИЯ И ТРАСОЛОГИЧЕСКАЯ ЭКСПЕРТИЗА»

В последнее время образовательные технологии претерпели значительные изменения. В силу развития науки и техники, и процесс образования стал более технологичным. Широкое применение получили так называемые системы дистанционных образовательных технологий (СДОТ),

с их помощью производится непосредственно и обучение студентов, и организуются повышения квалификации работников и т. д. С применением данной технологий проводят лекционные, семинарские и практические занятия, выполняют лабораторные работы, проводят консультации. И если с теоретическими аспектами занятий особых затруднений нет, то вот практические занятия вызывают немало проблем как у преподавателей при его проведении, так и обучающихся.

Практическое занятие в зависимости от изучаемого материала может преследовать множество целей, таких, например, как педагогическая, методическая, воспитательная, пропагандистская и т. д. Рассмотрим последовательно некоторые из них.

Первая цель практического занятия – педагогическая и для ее достижения необходимо научить и привить обучающимся необходимые знания, умения и навыки в рамках занятия.

Вторая цель – методическая. Она указывается в планах занятий и служит для закрепления навыка в рамках выполнения, какого-либо практического задания. Например, стадия оценки результатов исследования и формулирование выводов экспертизы следов неполных подошв обуви изучается на занятиях по дисциплине «Трасология и трасологическая экспертиза», которая проводится на кафедре трасологии и баллистики учебно-научного комплекса Волгоградской академии МВД России в плане семинарских и практических занятий по теме «Экспертные исследования следов обуви».

Целью данного занятия является отработка методических приемов проведения вышеуказанной стадии [1]. Для достижения данной цели в плане прописан порядок выполнения практической работы, который состоит из четырех заданий.

При выполнении первого задания обучающимся предоставляется возможность оценки существенности совокупности различающихся признаков, идентификационную значимость совокупности совпадающих признаков, а также решить вопрос об образовании следов одним тем же следообразующим объектом. Второй пункт выполняется уже на основе результатов проведенного исследования, которое проводилось как на этом занятии (при выполнении первого задания) так и еще и на предшествующем занятии.

В рамках данного задания, обучающимся необходимо сформулировать синтезирующую часть заключения эксперта и выводы. На третьем и четвертом задании нужно составить фрагмент исследовательской части заключения эксперта, выводов к нему, а также фототаблицу к заключению эксперта, выполнить разметку совпадающих признаков.

Для выполнение данных заданий, обучающимся выдаются объекты. Данные объекты представляют собой массив, в количестве десяти поверхностных следов подошв обуви (фото № 1) и неполный след подошвы обуви (фото № 2).

Фото № 1. Массив из десяти поверхностных следов подошв обуви

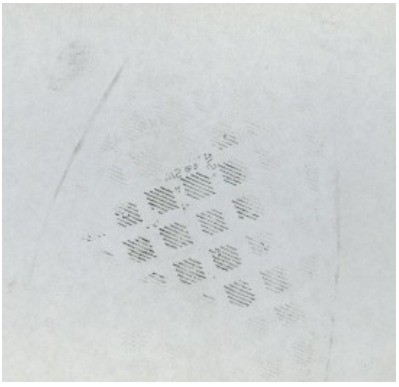

Фото № 2. Неполный след подошвы обуви

При последовательном выполнении всех перечисленных заданий обучающиеся должны приобрести необходимые знания, умения и навыки для самостоятельного выполнения экспертизы неполных следов подошвы обуви. Этого достаточно быстро и качественно можно достигнуть и проверить при аудиторном занятии, но когда обучение проводится дистанционно, то носит ярко выраженную контрольно-отчетную форму. На каждом этапе преподаватель должен практически с каждым обучающимся индивидуально проговаривать его действия и на каждом этапе просить демонстрировать полученные результаты. Только при таких условиях преподаватель может оценить, что обучающиеся правильно применяют полученные знания при выполнении заданий. Следует отметить, что при этом тратится значительная часть учебного времени. Поэтому преподаватель при подготовке к занятию должен планировать время, потраченное не только на демонстрацию результатов, но и на загрузку файлов, умение работать каждого обучающегося с софтом, в некоторых случаях объяснить обучающемуся его действия для демонстрации полученных результатов. При этом процесс демонстрации достаточно трудоемкий и не относится непосредственно к цели практического занятия. Как правило, преподавателю приходится неоднократно повторять то или иное решение проблемного вопроса, если не все обучающиеся не могут его решить самостоятельно.

Для проведения занятия на высоком педагогическом уровне приходится прибегать к нестандартным решениям. Так, например, при разметке обучающимся частных признаков в неполном следе подошвы обуви и на фрагменте следа подошвы обуви из массива, целесообразно дополнительно поделить группу обучающихся на более мелкие, по основанию однотипности объектов (неполных следов подошв обуви) по общим признакам. Далее уже с каждой группой, в которую, как правило, входит 3–4 обучающихся, проводится разбор каждого полученного результата. После чего, преподаватель оценивает полученные результаты каждым обучающимся подгруппы при решении поставленной задачи и на заключитель-

ном этапе повторяет вышеуказанные действия, при необходимости для отстающих лиц. При разметке одноименных частных признаков в следах обучающиеся зачастую не понимают, почему размеченные одноименные признаки выглядят по-разному (фото № 3). И только после демонстрации преподавателя с объяснением, в чем их ошибка, замечают, что следы сориентированы под небольшим углом по отношению друг к другу, при этом взаиморасположении одноименных признаков наблюдается по-разному. Для устранения визуального несоответствия необходимо один из следов расположить под тем же углом, что и другой.

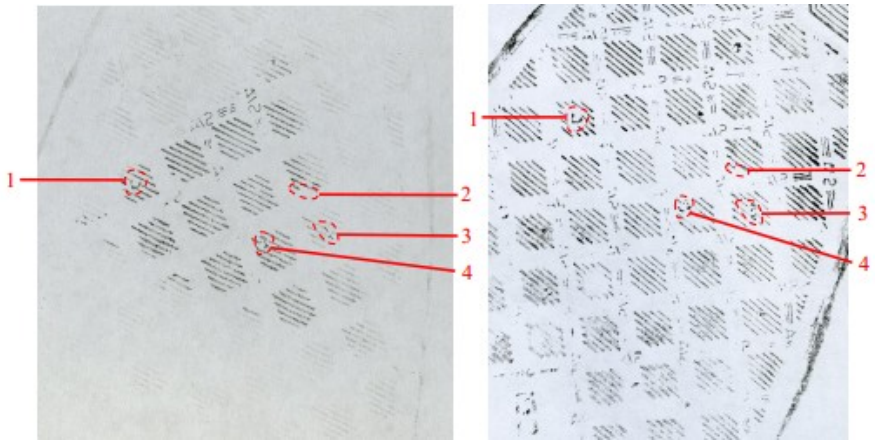

Фото № 3. Разметка частных признаков в разноориентированных следах

Исходя из вышеизложенного, очевидно, что успешное достижение поставленных преподавателем целей практического занятия, при дистанционном обучении, связано с большими трудозатратами и правильным распределением времени, с акцентом на практическую часть занятия, а также перераспределением оставшегося времени в случае возникновения технических проблем.

Литература

1. Типовые экспертные методики исследования вещественных доказательств: учеб. пособие / под ред. Ю.М. Дильдина. М., 2011.

В.В. Корбаков

ДИСТАНЦИОННЫЕ ТЕХНОЛОГИИ В ВОСПИТАТЕЛЬНОЙ РАБОТЕ

«Сейчас многое, очень многое делается в удаленном режиме. Когда восстановится обычный ритм деловой жизни, этот опыт, безусловно, будет весьма полезен, востребован», – сказал Президент России В.В. Путин на совещании по состоянию рынка труда в Российской Федерации [1].

Реалии сложившейся в мире санитарно-эпидемиологической обстановки, связанной с распространением новой коронавирусной инфекции COVID-19, вызвали потребность в расширении дистанционных форм различных направлений жизнедеятельности современного общества. За последние пару лет дистанционный формат стали обретать те направления, удаленность которых раньше даже не рассматривалась. Сегодня дистанционно можно сделать практически все: реализовать свое активное избирательное право [2], подать заявление в Пенсионный фонд России, оформить социальные выплаты, включая выплаты для владельцев сертификата на материнский капитал, узнать о мерах поддержки, отправить и получить посылку, получить банковские услуги, приобрести различные товары, включая продукты питания, медикаменты и многое другое.

Но, пожалуй, самое широкое распространение дистанционный формат обрел в сфере образования. Под дистанционным образованием мы понимаем обучение, реализуемое с помощью информационно-телекоммуникационных сетей при опосредованном взаимодействии учеников и педагогов. Не покидая дом можно не только научиться рукоделию или выучить иностранный язык, но и освоить школьную программу и даже получить высшее образование. Хотя как такового понятия «дистанционное образование» в нормативных правовых актах не существует, в них используется термин «дистанционные образовательные технологии» (далее – ДОТ). Применение ДОТ регламентируется ст. 16 Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ.

У применения ДОТ есть очевидные преимущества. Это более выгодно экономически, значительно расширяется географический охват, возникает реальная возможность освоить новые профессии тем, кто совмещает учебу с работой, людьми с ограниченными возможностями здоровья. Использование цифровых технологий в осуществлении обучения и самообучения стало трендом, укладывающимся в общий вектор развития системы образования [3]. В настоящий момент на всех ее уровнях идут попытки по индивидуализации образовательной деятельности. Школы начинают внедрять раннее профилирование учеников, а получение специальности выходит за границы вуза.

Условия пандемии способствовали применению дистанционных технологий и в таких образовательных организациях, как суворовские военные училища МВД России. Прежде всего, необходимость использования ДОТ в суворовских военных училищах обусловлена тем фактом, что там обучаются воспитанники из различных субъектов страны. Каждый раз после каникул суворовцы возвращаются из своих регионов с различным уровнем санитарно-эпидемиологического благополучия и заболеваемости населения. Вместе с тем, обучение в суворовском военном училище МВД России предусматривает не только занятия в классе в составе взвода. Отличительной чертой данных образовательных организаций также является совместное проживание суворовцев в общежитии, групповой прием пищи в столовой, коллективная помывка в банно-прачечном комплексе. Таким образом, в учебных коллективах суворовских военных училищ возникает высокий риск распространения различных острых респираторных заболеваний.

В развитии рассматриваемой темы возникает очевидная потребность в применении дистанционных технологий при проведении определенных массовых мероприятий, а именно тех, к которым относятся некоторые торжественные ритуалы и церемонии. Конечно же, невозможно полностью «оцифровать» воспитательную работу, проводимую в образовательных организациях системы МВД России, но снизить «плотность» количества участников посредством применения ДОТ вполне реально.

Безусловно, организация мероприятия на виртуальной площадке будет отличаться от организации мероприятия в классическом формате. Во-первых, необходимо привлечь дополнительных специалистов в области цифровых технологий. Во-вторых, необходимо понимать, что все участники мероприятия должны иметь доступ к стабильному интернету с высокой скоростью передачи данных. В-третьих, выбранная электронная платформа для проведения мероприятия должна быть общедоступной, простой для использования обывателем и в то же время обладать всем необходимым функционалом.

Преимуществом проведения торжественной церемонии в дистанционном режиме также является возможность рассредоточить участников на различных площадках проведения отдельных ритуалов. Положительным примером может служить опыт Астраханского суворовского военного училища МВД России в проведении церемонии выпуска в июне 2020 г. Организаторы торжественного мероприятия определили несколько площадок, на которых происходили различные элементы праздника. Первой площадкой выступил зал, где разместились первые лица училища, почетный гость – Министр образования и науки Астраханской области, знаменная группа. Вторая площадка была оборудована возле символа училища – бюста генералиссимуса А.В. Суворова, где выступал ветеранский корпус. На площадке в «Зале славы» разместились руководители образовательной организации. Свои слова благодарности от лица совета родителей, а также выпускников, участники произнесли с площадок, находящихся в местах проживания. Все участники наблюдали за происходящим через информационно-телекоммуникационную сеть. Благодаря грамотной подготовке плана-сценария, слаженной работе организаторов мероприятия на площадках, четкости действий модераторов и операторов, церемония торжественного выпуска суворовцев Астраханского суворовского военного училища МВД России прошла на высоком организационном и эмоциональном уровне и дистанционный формат никак не повлиял на атмосферу праздника.

Рассмотренное мероприятие показывает, что если с применением ДОТ возможно проведение масштабных церемоний, то осуществление отдельных ритуалов в дистанционном формате может существенно упростить их организацию и проведение. С применением ДОТ можно озвучивать приказы о поощрении личного состава с демонстрацией иллюстративного материала, к которому могут относиться фотографии поощряемых сотрудников, изображения наград. Через видео-конференц-связь возможно поздравление сотрудника со знаменательным событием в его жизни, информирование личного состава о вновь назначенных сотрудниках.

В условиях пандемии важно развивать технологии и навыки обращения с ними. Это способствует и дальнейшему развитию дистанционного образования. Кроме того, стало очевидно, что от технологий зависят и государственные услуги, и система государственного управления. Но как бы то ни было, огромный плюс дистанционных технологий в том, что они позволяют любому человеку учиться непрерывно [4].

Литература

1. Материалы совещания о ситуации на рынке труда [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/news/63419 (дата обращения: 24.04.2022).

2. Чистобородов И.Г. Избирательный процесс как объект государственного управления в Российской Федерации в условиях развития электронной демократии // Проблемы экономики и юридической практики. 2018. № 3.

3. Горошко И.В., Холостов К.М., Сердюк Н.В. и др. Внедрение системы дистанционного обучения для подготовки руководителей органов МВД России: монография. М., 2015.

4. Кузнецова О.В. Дистанционное обучение: за и против // Международный журнал прикладных и фундаментальных исследований. 2015. № 8–2.

В.Л. Акапьев,
С.Е. Савотченко,
А.А. Дрога

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СПО В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ МВД РОССИИ

Правоохранительная, управленческая и образовательная деятельность в ОВД России неразрывно связана с широким применением современных информационных технологий. В контексте повышения информационной безопасности и защиты информации особую актуальность приобретают информационные технологии, основанные на свободном программном обеспечении.

Свободно распространяемое или свободное программное обеспечение (далее – СПО) представляет собой класс программного обеспечения, реализуемого на основе специальных лицензий, не относящихся к проприетарному программному обеспечению. Развитие таких программ началось достаточно давно с разработки операционных систем [1].

Процесс построения единого информационного пространства образовательной организации сталкивается с рядом проблем не только технического, информационного и программного характера. В условиях правового общества на первое место выходит необходимость правовой регламентации не только рынка программного обеспечения, но и авторского права на него [2].

Широкое распространение СПО на мировом рынке программного обеспечения приводит к необходимости его скорейшей интеграции в российское правовое пространство. Решение данной задачи становится крайне желательным в условиях импортозамещения, когда свободно распространяемое программного обеспечение может выступить в качестве основы для разработки отечественного софта, что крайне актуально в сложившихся условиях.

Юридическая специфика использования СПО, в отличие от «классического» рынка программного обеспечения может быть определена сле-

дующими особенностями. Во-первых, это реализация права на запуск программы для решения любых задач и неограниченных целях. Во-вторых, существует возможность ее изучения и адаптации к требуемым месту и условиям эксплуатации. В-третьих, отсутствует регламентация на распространение СПО, его модификацию (совершенствование). И, в-четвертых, распространение СПО осуществляется на основании свободных лицензий [3].

В соответствии с Гражданским кодексом Российской Федерации (ч. 4) передача прав на использование СПО на условиях свободной лицензии GNU GPL v3 должна осуществляться на основании лицензионного договора (ранее – авторский договор), согласно которому одна сторона – обладатель исключительного права на результат интеллектуальной деятельности (лицензиар) – предоставляет или обязуется предоставить другой стороне (лицензиату) право использования такого результата в предусмотренных договором пределах с сохранением за лицензиаром права выдачи лицензий другим лицам (простая, неисключительная, лицензия) либо без такового (исключительная лицензия).

Основным механизмом, обеспечивающим существование свободных программ в мире, являются свободные лицензии (или авторские, лицензионные договоры) – юридические документы, регламентирующие условия использования свободных (открытых) программ и передающие пользователям ряд дополнительных прав по сравнению с установленным объемом прав по умолчанию в местном законодательстве [4].

Правовые риски при использовании открытых и свободных программ заключаются в том, что при любой проверке окажется, что использование программного обеспечения не подтверждено ни одним бумажным документом. Отечественные правоохранители (зачастую не обременяя себя юридическим самообразованием) считают любое использование «без бумажки» незаконным.

Очевидно, что в общем случае конечный пользователь СПО или поставщик решений на базе СПО сможет предъявить правоохранителям лишь ссылку на сайт компании-поставщика и распечатку лицензионного договора (с его переводом на русский могут быть проблемы, тем более с нотариально заверенным). Что же касается «декларации соблюдения

прав...», подписанного оригинала договора, оригиналов документов, подтверждающих передачу программного продукта, и факта оплаты договора, упаковки от программного продукта и тем более «уникальных идентификационных номеров экземпляров свободного ПО», то указанные документы относятся скорее к области «ненаучной фантастики».

Распространение СПО происходит на условиях лицензионных договоров, оформленных в виде договоров присоединения. Оно осуществляется либо безвозмездно, либо по себестоимости носителя информации, записи на него продукта и его доставки пользователю. Никаких бумажных договоров при этом не заключается и, естественно, не оформляется никаких накладных, счетов-фактур, актов передачи экземпляров и прочих бумажных документов. Исключением здесь являются лишь отечественные поставщики СПО, законность действий которых в отношении иностранных продуктов является по меньшей мере спорной [5].

С начала разработки свободно распространяемых решений ведутся дебаты о том, могут ли они обеспечить более надежную защиту, чем коммерческие системы. Пока компьютерное сообщество не пришло к определенным выводам. С одной стороны, свободно распространяемое программное обеспечение дает равные условия как злоумышленникам, так и обороняющимся от них, с другой – открывает последним доступ к методикам защиты и знаниям, которые редко можно получить при использовании коммерческих программных продуктов. Большинство программистов, участвующих в движении Open Source, принимают дополнительные меры для защиты своего кода, поскольку в случае недостаточной безопасности программы они рискуют собственной репутацией. Кроме того, свободно распространяемый код анализируется и проверяется всем сообществом.

В условиях беспрецедентного давления «мирового сообщества» на нашу страну, ухода с внутреннего рынка мировых производителей программного обеспечения ставится под сомнение необходимость использования в образовательных учреждениях исключительно лицензионного программного обеспечения. Можно ли считать равноценной заменой приложениям Windows свободно распространяемое ПО?

Ответом на этот вопрос могут служить причины, показывающие целесообразность использования СПО в учебных заведениях, в том числе и в образовательных организациях системы МВД России [6].

Переход образовательных учреждений на СПО дает возможность снижения затрат на учебный процесс и приобретение лицензионно чистого программного обеспечения [7]. Однако для менталитета россиянина возможность бесплатного получения высококачественного программного обеспечения представляет собой нонсенс.

Наличие краткой аннотации программ, создаваемых по всему миру, делает пакет СПО максимально удобными для инсталляции и размещению дистрибутивов на машинный носитель, который предлагался потенциальному пользователю, не желавшему тратить значительное время на поиски требуемого продукта в сети. Тем более такой вариант приобретения ПО обеспечивает дополнительные гарантии, подтверждаемые товарным знаком изготовителя такого компакт-диска.

Немаловажным фактором снижения стоимости СПО является сам творческий процесс создания программного обеспечения. Вряд ли лишь увеличением финансирования можно добиться улучшения его качества. К тому же, как показывают результаты периода самоизоляции и перехода на удаленный режим работы в условиях пандемии коронавируса, плодотворность творческой работы, каковой и является процесс написания софтов, никоим образом не снизилась. Скорее наоборот, потому что сотрудничество неформальных объединений, мотивированных на самовыражение, саморекламу и самообразование специалистов, работающих в «парниковых» консигнациях свободного графика, позволяет получить результат, не уступающий коммерческим проектам [8].

Помимо этого существуют вполне реальные силы, заинтересованные в изменении правил игры на рынке программного обеспечения. Сюда завязывается и традиционная конкурентная борьба за получение некоторых преференций перед конкурентами. С другой стороны находит распространение новая идеология, определяемая позицией, основанной на доктрине подхода к программному обеспечению вообще и операционным системам в частности как нематериальным объектам, выступающим в качестве идейного базиса для реализации производственных процессов и общественных отношений.

Условия распространения СПО имеют радикальные отличия в отношении коммерческих лицензий на ПО, выдаваемых, например, Symantec,

Microsoft или Inprise. В случае коммерческих лицензий разработчик требует оплату за каждую используемую копию. Для образовательных учреждений такое положение дел является неприемлемым по причине необходимого количества финансовых средств, требующихся для оплаты каждой копии программы, устанавливаемых на рабочих местах административных работников, преподавателей или в компьютерных классах.

Предоставляемые некоторыми фирмами для вузов и школ скидки дифференцированы и носят зачастую декларативный характер. Парадоксально, но факт: если вуз еще может рассчитывать на какую-то скидку, то учреждение дополнительного образования – нет. А если институт работает по нескольким программам? При этом скидки распространяются на ограниченный перечень программного обеспечения, необходимого для организации образовательного процесса, и не способны в целом улучшить ситуацию. Применение же «пиратских», не соответствующих лицензионным соглашениям копий компьютерных программ в системе образования, кроме нарушения действующего законодательства, ведет к деформации прагматики всего учебного процесса [9].

Другим положительным аспектом использования GPL-программ является то, что они распространяются с документацией и их исходными текстами, что допускает Uni – зарегистрированная торговая марка X/Open Company.

Среди программ, распространяемых согласно GPL и лицензионным коммерческим соглашениям, также находятся Shareware (или условно-бесплатные программы), которые представлены различного рода утилитами, привязанными к той или иной коммерческой операционной системе (далее – ОС).

Несмотря на противоречия, соглашения, подобные GPL и коммерческие лицензии имеют ряд общих черт, которые касаются гарантии на программные продукты и сопровождения.

Существует и другая причина, по которой специалисты приветствуют возможность использования Unix-подобных ОС в системе высшего образования. Она определяется природой самих операционных систем, характеризующихся высокой надежностью, возможностью работать годами без перезагрузки, содержать в себе все атрибуты того, что неразрывно

связано с самим понятием «современная ОС» – многозадачность, графический интерфейс, поддержка широкого диапазона периферийных устройств, локальных сетей, Internet и т. п.

Такие ОС мобильны и обладают дружественным интерфейсом.

Идею использования СПО в образовательных системах поддерживает накопленный мировой опыт. Само развитие Unix и ее позднейших клонов неразрывно связано с высшими учебными и научными учреждениями и организациями. Практически все ведущие зарубежные вузы естественнонаучной направленности практически используют ту или иную разновидность Unix.

Следующая причина подкрепляется серией международных соглашений по стандартизации POSIX (интерфейс портативных операционных систем), делающих совместимые с Unix системы открытыми не только де-факто, но и де-юре. Разработанная и предложенная производителям компьютерной техники доктрина открытой архитектуры IBM-PC-совместимых компьютеров позволила этой фирме за непродолжительный период времени вытеснить с широкого потребительского рынка практически все прочие модели ПЭВМ, невзирая на отдельные аппаратные и программные преимущества компьютеров-конкурентов.

Очередная причина связана с психологией. Как Microsoft Windows, так и IBM OS/2 ориентированы на пользователя-потребителя. Это выражается в их дружественном интерфейсе, подчас создающем слишком навязчивую (особенно, в последних версиях) среду использования готовых программных продуктов. Для самого же разработчика это оборачивается необходимостью нести дополнительные значительные финансовые затраты на приобретение соответствующих фирменных инструментальных средств и документации.

Помимо этого, фирменные программы напичканы всевозможными «секретами» и «водяными знаками», которые никогда точно не документируются и меняются разработчиками от версии к версии программного продукта.

К указанным нюансам привычны и вполне равнодушны производители-профессионалы программ для потребительского рынка, но они абсурдны и недопустимы в системе образования, где приемлемыми и достаточно

естественными являются программы, рассчитанные, в первую очередь, на производителя-пользователя с соответствующим уровнем квалификации, создающего программы для учебных или научных целей.

И, наконец, Internet. Все буднично и уже привычно: во всем мире провайдеры услуг этой всемирной сети в большинстве случаев используют Unix-подобные системы. Под управлением такой системы компьютер легко встраивается в любую локальную сеть. Его можно использовать как маршрутизатор или мост, он может обеспечить подключение нескольких компьютеров через один IP-адрес и установить надежную защиту против вторжения в вашу сеть нежелательных посетителей и т. п. Поэтому, следуя этому практическому опыту, естественно подключаться к Internet через эти хорошо апробированные системы.

В завершении рассмотрения факторов в пользу использования СПО нельзя не вспомнить о различиях операционных систем по требованиям к аппаратным средствам, где наиболее демократичными выглядят представители СПО.

Литература

1. Барретт Дэниел Карманный путеводитель по Linux. М., 2016.
2. Белоусов А. Компьютерная программа как объект защиты авторского права [Электронный ресурс]. URL: https://crime-research.ru/library/Belous1203.html. (дата обращения: 24.04.2022).
3. Пожарина Г.Ю. Стратегия внедрения свободного программного обеспечения в учреждениях образования. М., 2018.
4. Гражданский кодекс Российской Федерации: федер. закон от 18.12.2006 № 230-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».
5. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203. Доступ из справ. правовой системы «КонсультантПлюс».
6. Акапьев В.Л. Аспекты формирования единого информационного пространства образовательной организации МВД России // Проблемы правоохранительной деятельности. 2016. № 1.

7. Акапьев В.Л. Актуальные проблемы импортозамещения программного обеспечения образовательных организаций в контексте информационной безопасности // Дистанционное и виртуальное обучение. 2015. № 11.

8. Гордейчик С. Бесплатно и безопасно: главные мифы свободного ПО [Электронный ресурс]. URL: https://habrahabr.ru/company/pt/blog/249927 (дата обращения: 24.04.2022)

9. Савотченко С.Е. Применение авторских сетевых образовательных ресурсов педагогами Белгородской области // Учитель – учителю. Из опыта работы учителей Белгородской области. Серия Информационные технологии в образовании. Белгород, 2010. Вып. 1.

В.А. Васильев,
Т.А. Ермакова

СОВРЕМЕННЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ПРИ СОЗДАНИИ СЛЕДОТЕК СЛЕДОВ ОБУВИ

В настоящее время трасологическая экспертиза следов обуви является одной из самых распространенных в экспертной практике. Это обусловлено тем, что объект исследования данного вида судебной экспертизы – это следы обуви, которые обнаруживают, фиксируют и изымают практически на каждом месте происшествия.

Как известно, следы ног, в большинстве случаев, позволяют определить ряд важных обстоятельств, используемых для розыска и изобличения преступника. Так, например, данные следы могут содержать информацию об отдельных обстоятельствах совершенного преступления, в частности о последовательности действий подозреваемого (разрешаемые в рамках ситуационной экспертизы), а также об особенностях строения подошвы обуви, образующихся в результате контактного взаимодействия со следовоспринимающей поверхностью.

В связи с развитием средств компьютеризации в ОВД, оснащением экспертно-криминалистических подразделений современными техническими

средствами, появилась возможность автоматизации криминалистических учетов. Ведомственными нормативными актами определен порядок формирования и использования следотек по наиболее часто встречающимся объектам (следам) криминалистических экспертиз, таким как орудия взлома, подошвы обуви, протекторы шин транспортных средств и др.

Следы обуви, чаще всего единичные, изымаются для проведения в дальнейшем идентификационного исследования. По данным следам также возможно решение широкого круга вопросов диагностического характера, например, определение направления и скорости передвижения преступника, роста, веса, пола, возраста, физиологических особенностей и профессиональной принадлежности преступника. Систематизация и формализация процесса исследования следов подошвы обуви основана на методике, в которой классифицированы все признаки деталей с точки зрения их идентификационной значимости.

В ходе анализа научной литературы выделены следующие основные способы фальсификации следов обуви – путей подделки, изменения свойств с целью искажения характерных признаков [1]:

– ходьба след в след – сокрытие информации о количестве идущих людей;

– использование обуви не по размеру;

– использование чужой обуви;

– использования обуви другого пола;

– надевание поверх обуви различных предметов.

Среди приоритетных направлений развития судебно-экспертной деятельности можно выделить разработку информационно-поисковых систем (реализованных с использованием эвристических подходов) позволяющих решать идентификационные задачи, в том числе и в классе криминалистических судебных экспертиз.

Широкое распространение в отечественной и зарубежной практике получил ряд автоматизированных идентификационных систем, используемых для создания следотек следов обуви. В частности, описана экспертная система следов обуви Footwear Traces 2 (рис. 1) [2].

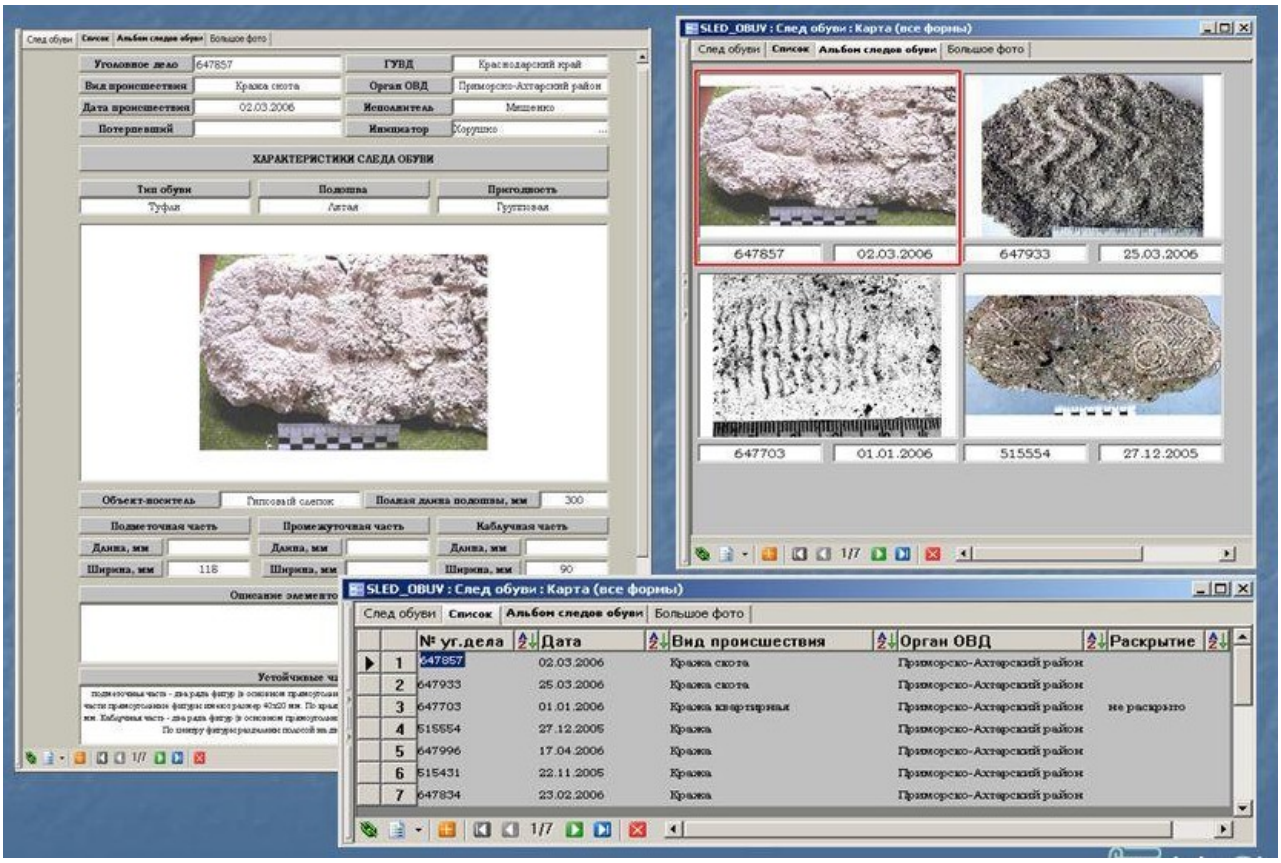

Рис. 1. Диалоговый интерфейс программного продукта Footwear Traces 2

Экспертная система следов обуви позволяет решать следующие задачи:

– осуществлять ввод (со сканера, файла) и хранение в базе данных изображений следов и (или) оттисков обуви и (или) подошв/верха обуви;

– осуществлять различные виды поиска по базе данных в т. ч. по типу рисунка, отобразившемуся в оттиске подошвы обуви;

– проводить каталогизацию, описание и поиск по запросам;

– осуществлять печать отчетов и т. д.

Аналогичным образом организована работа таких автоматизированных информационно-поисковых систем (АИПС), как Pride [3], EverASM™ [4], SICAR [5] и ряд других картотек следов обуви, позволяющая проводить кодирование следа или оттиска.

Программные продукты содержат как минимум две базы данных:

– картотеку следов обуви, изъятых с мест нераскрытых преступлений;

– оттиски обуви, полученные у задержанных лиц.

Внедрение подобных автоматизированных программно-аппаратных комплексов для решения идентификационных задач по исследованию следов обуви позволит значительно повысить эффективность решения задач судебно-трасологической экспертизы, расширить возможности информационного обеспечения, что в свою очередь будет способствовать информативности, обоснованности и достоверности выводов по идентификационной экспертизе следов обуви.

Литература

1. Baiker-Sorensen M., Koen H., Keereweer I., Pauw P., Visser R. Interpol review of shoe and tool marks 2016–2019 // Forensic Science International: Synergy, April 2020 [Электронный ресурс]. URL: https://doi.org/10.1016/j.fsisyn.2020.01.016 (дата обращения: 19.05.2020).

2. Экспертная система следов обуви Footwear Traces 2 [Электронный ресурс]. URL: http://kmtkazan.ru/node/258 (дата обращения: 01.10.2021).

3. Shoeprint matcher PRIDE [Электронный ресурс]. URL: https://hobbit-is.nl/projects/forensic-intelligence/ pride/?lang=en (дата обращения: 01.10.2021).

4. Everspry Cloud national footwear database [Электронный ресурс]. URL: https://www.shopevident.com/category/casting-footwear/everspry-cloud-national-footwear-database (дата обращения: 01.10.2021).

5. Sicar®6 [Электронный ресурс]. URL: http://www.fosterfreeman.com/trace-evidence/356-sicar-6-solemate. html (дата обращения: 01.10.2021).

Д.А. Евстропов,
О.В. Слаутин

БИБЛИОТЕЧНАЯ БАЗА ДАННЫХ КАК СРЕДСТВО АНАЛИЗА ПУБЛИКАЦИОННОЙ АКТИВНОСТИ СОТРУДНИКОВ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

В мире генерируется огромное количество данных практически по всем аспектам жизни: школьные записи, кредитные карты, товары, телефонные системы и веб-сайты и т. д. Некоторое время назад для отслеживания и сообщения этой информации использовались ручные записи, сейчас широкое распространение получили электронные базы данных. По определению, база данных представляет собой структурированный набор логически связанных данных, которые хранятся таким образом, чтобы к ним можно было легко получить доступ. Логически связанные данные включают объекты, атрибуты и взаимосвязи информации организации.

Проблема оценки научной деятельности педагогов в образовательных организациях МВД очевидна в виду непосредственной специфики заведений. Организационную структуру, учебно-методическое обеспечение и качество образовательного процесса, управление в настоящее время невозможно представить без успешного использования элементов информационной поддержки. Необходимость создания эффективных и надежных методов и систем оценки подтверждена многолетней практикой управления высшими образовательными учреждениями во многих странах мира, а ее совершенствования является одним из ключевых направлений [1–3]. Такая системная работа невозможна без анализа опыта использования уже созданных систем ориентированных на сбор, хранение и анализ научной деятельности.

Например, в Волгоградском государственном техническом университете (ВолгГТУ), параллельно с введением рейтинговой системы оценки

деятельности профессорско-преподавательского состава (далее – ППС), информационно-библиотечным центром постоянно мониторится, ведется регистрация публикаций и соответствующая база данных (БД) [4].

База данных представляет собой организованный набор структурированной информации и содержит библиографические описания публикаций сотрудников университета. Для успешной обработки информации, данные моделируются в виде строк и столбцов в ряде таблиц. Информацию можно получить в виде отчета о публикации конкретного автора, филиала, факультета, кафедры и т. д. (рис. 1–2). Как и все, она организована по полям, т. е. полная запись содержит отдельные элементы как университет, автор, факультет, вид публикации и т. д. Можно ограничить поиск одним полем или искать в нескольких полях одновременно.

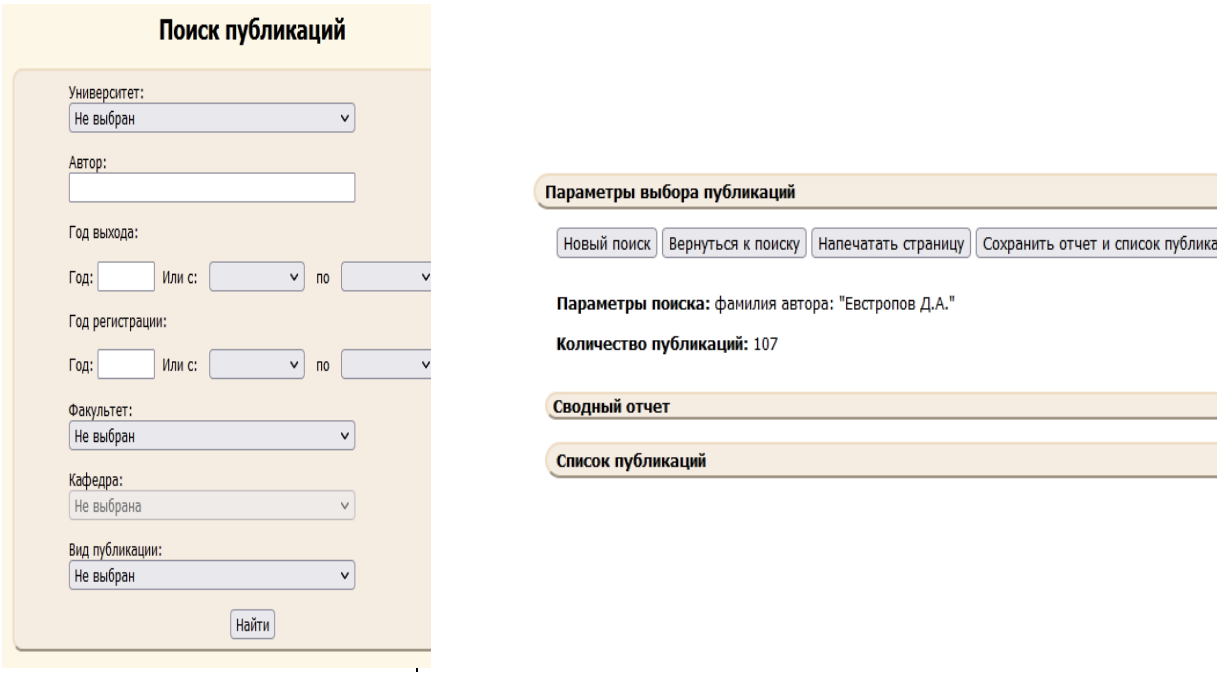

Рис. 1. Поисковое окно библиотечной базы данных с параметрами запроса на конкретного автора

Параметры поиска: фамилия автора: "Евстропов Д.А."
Количество публикаций: 107

Год	монография	учебник	учеб. пособие	учеб. пособ.(гриф)	Статья из рос. журнала	Статья из заруб. журнала	Известия ВолгГТУ	Журналы ВолгГТУ	Статья из рос. сборника	Статья из заруб. сборника	Тезисы докладов	Учебно-методический комплекс	Депониров. рукопись	Патентный документ	Свидетельство	Прочие публикации
2011	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
2012	0	0	0	0	1	0	1	0	2	0	5	0	0	1	0	0
2013	0	0	0	0	1	0	5	0	8	0	4	0	0	1	0	0
2014	0	0	0	0	3	0	5	0	4	0	3	0	0	1	0	0
2015	0	0	0	0	4	0	6	0	7	1	1	0	0	12	0	0
2016	0	0	0	0	3	2	5	0	3	1	4	0	0	3	0	0
2017	0	0	0	0	0	0	2	0	0	1	0	0	0	2	0	0
2018	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0
2019	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
2020	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Итого	**0**	**0**	**0**	**0**	**14**	**2**	**26**	**0**	**24**	**3**	**18**	**0**	**0**	**20**	**0**	**0**

1. **Кондаков, А.В.** Отдельные аспекты совершенствования методики выявления следов рук человека люминофорными порошками / А.В. Кондаков, Д.А. Евстропов, О.В. Слаутин // Судебная экспертиза. - 2020. - № 3 (63). - 17-29.
2. **Евстропов, Д.А.** Структура модульной образовательной программы, её пример и этапы внедрения [Электронный ресурс] / Д.А. Евстропов, А.В. Кондаков, Д.В. Проничев // Мир науки. Педагогика и психология : электронный журнал. - 2019. - Т. 7, вып. № 1 (январь – февраль). – Режим доступа : https://mir-nauki.com/PDF/88PDMN119.pdf.
3. Износостойкость диффузионных прослоек в композите системы Ti–Fe после сварки взрывом и термической обработки / В.Г. Шморгун, О.В. Слаутин, Д.А. Евстропов, А.С. Кайгородов, А.Г. Серов // Известия ВолгГТУ. Сер. Сварка взрывом и свойства сварных соединений. - Волгоград, 2018. - № 11 (221) Ноябрь. - С. 52-56.
4. Оценка износостойкости покрытий систем Cu-Ti и Cu-Ni-Ti методом царапания / В.Г. Шморгун, О.В. Слаутин, А.С. Кайгородов, А.Г. Серов, Д.А. Евстропов // Известия ВолгГТУ. Сер. Проблемы материаловедения, сварки и прочности в машиностроении. - Волгоград, 2018. - № 9 (219) Сентябрь. - С. 84-86.
5. Contact Melting Mechanism in the Cu-Ti System [Электронный ресурс] / В.Г. Шморгун, О.В. Слаутин, Д.А. Евстропов, В.П. Кулевич // Key Engineering Materials. Vol. 743 : High Technology: Research and Applications 2016 (HTRA, Tomsk Polytechnic University, Russia, December 5-7, 2016) : conf. proceedings / ed. by G.E. Osokin, E.A. Kulinich. – [Switzerland] : Trans Tech Publications, 2017. – P. 58-62. – URL : https://www.scientific.net/KEM.743. – doi: 10.4028/www.scientific.net/KEM.743.58.

Рис. 2. Оформленные результаты запроса на конкретного автора в табличной и печатной форме

Пополнение БД проводится следующим образом: ППС передает сведения о публикации, по мере ее (их) выхода отвечающему за этот процесс сотруднику библиотеки, который вносит библиографическую запись, составленную в соответствии с требованиями «ГОСТ 7.1-2003 Библиографическая запись. Библиографическое описание. Общие требования и правила описания» в базу данных вуза. Электронные издания регистрируются при наличии регистрационного свидетельства Научно-технического центра «Информрегистр» на базе Государственного регистра баз данных.

Доступ к базе открыт для всех зарегистрированных пользователей (ППС, студентов, аспирантов) и в случае необходимости сотрудники учебно-методического, научного отдела и т. д., могут получить всю

необходимую достоверную информацию об опубликованных работах за любой временной промежуток, согласно заданной выборке без обращения к автору.

Аналитическая информация и плановые показатели соответствующего характера постоянно требуются в текущей деятельности академии: для формирования отчетов структурных подразделений, написания заявок на участие в проектах и контроля.

Предполагается, что появление собственных библиотечных баз данных в вузах МВД России:

1) положительно отразится на взаимодействии структурных подразделений между собой и социальном климате в коллективе образовательной организации;

2) позволит оперативно анализировать и информировать о ситуации по публикациям как у конкретного преподавателя, так на кафедре, факультете и в вузе в целом, а также формировать разнообразные отчеты;

3) снизит нагрузку на преподавателей, связанную с заполнением электронных, бумажных отчетностей, хранением материалов и ведомостей, подтверждающих результаты их научной деятельности, что, несомненно, позволит им сконцентрироваться на учебном процессе и научной работе.

Стоит отметить, что пользователи предпочитают электронные базы данных только в том случае, если они облегчают их работу и предоставляют им необходимую информацию. Удобство использования остается самым важным фактором библиотечной электронной базы данных, непонимание ее ключевой функции может привести к неправильным проектным решениям, которые могут иметь серьезные последствия для организации. Из негативных моментов отметим, что централизация ресурсов увеличивает уязвимость системы. Поскольку все пользователи зависят от доступности, отказ некоторых компонентов базы данных может привести к остановке операций, связанных с документооборотом. В этой связи, при ее разработке, должна учитываться специфика документооборота внутри вуза, а также детально проанализирована работа аналогичных систем в сторонних организациях.

Литература

1. Rabinovich M.I., Morozova A.V. Rating System for Personnel Professional Effectiveness: Principles, Models and Algorithmic Modules // International Scientific Conference Far East Con (ISCFEC 2018). Atlantis Press. 2019.

2. Текеев К.Х., Кочкарова П.А. Разработка информационной системы учета научной активности сотрудников кафедры // Тенденции развития науки и образования. 2021. № 74–2.

3. Румянцев А.А., Хабибулин Р.Р., Александров А.С. Разработка среды автоматизированного проектирования рейтинга научных сотрудников КНИТУ-КАИ // Образовательные технологии и общество. 2019. № 1.

4. Информационно-библиотечный центр Волгоградского государственного технического университета // БД «Публикации сотрудников ВолгГТУ» [Электронный ресурс]. URL: http://library.vstu.ru/node/34 (дата обращения: 24.04.2022).

А.О. Молчанов

РАЗВИТИЕ МОТОРНЫХ НАВЫКОВ ПОСРЕДСТВОМ КИБЕРСПОРТИВНОЙ АКТИВНОСТИ В РАМКАХ УЧЕБНЫХ ДИСЦИПЛИН ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ

Активность в жизни человека присутствует постоянно и поддерживает баланс системы, без нее человек не сможет приспособиться к окружающей среде. Основным проводным механизмом в жизни человека между организмом и окружающей средой является движение. Также в процессе совместной работы организма с окружающей средой происходят внутренние изменения в организме человека, корректируется его характер и поведение. Дополнительно к этому человеческая система основывается на учебной и практической деятельности, от которой непосредственно зависит координация движений рук человека, а именно сигналов, которые производились руками [1].

Согласно истории и современным учебникам о доисторических людях передача информации нашими предками состояла из невербального общения, а именно мычание и попытки издания звуков. В дальнейшем у человека происходит развитие артикуляционного аппарата, а речь продолжает формироваться именно из-за того, что та часть головного мозга, которая отвечает за двигательную активность пальцев человека, расположена рядом с речевым центром. В последствие чего первый элемент стимулировал второй элемент и в процессе такого взаимодействия происходит одновременное развитие механизмов человека [2].

Большинство ученых уверены, что все человечество должно быть обязано именно труду, который начал развиваться именно с мелкой моторики. Возьмем, например, В.А. Сухомлинского, который писал, что ум человека находится на кончиках его пальцев. Также рассмотрим мнение И. Канта, который называл «руки живой частью полушарий головного мозга и именно из-за этого любая активность руками сопровождается развитием мышц, отделов головного мозга, а также благодаря тесному развитию речи и моторики происходит нейрогенез (дополнительное развитие нейронных связей)» [3].

В момент работы пальцев рук осуществляется совместная работа отдельных элементов нашего головного мозга, а именно лобной и височной.

Практические разработки А. Лурия говорят нам о наличии трех основных функциональных блоков головного мозга, раскрывающих представление о прямой зависимости двигательной активности от мелкой моторики для стимуляции активности мозга. Лобные доли отвечают за контроль сложных форм деятельности. При нарушении активной зоны, отвечающей за двигательную активность, речевой центр благополучно прекращает работу. С другой стороны, нарушение артикуляционной системы без повреждения слухового анализатора и наличие умственной отсталости корректируется развитием мелкой моторики. Области речи формируются импульсами, исходящими от пальцев. Речевые движения, как и движения пальцев, начинаются с напряжения мышц, где возникают первые ощущения.

Чувства – это источник наших мыслей, которые затем перерождаются в словах. Развитие мелкой моторики начинается с первых лет жизни

человека. Чтобы проследить развитие познавательной сферы в целом, необходимо обращать внимание на его реакцию на внешние раздражители, улавливание рефлексов и тактильную чувствительность. Если развитие мелкой моторики соответствует возрасту, то развитие суставного аппарата в норме. Чем более развита у детей пальцевая деятельность, тем больше у них творческих способностей и познавательного интереса. Знаменитый итальянский врач и профессор М. Монтессори упоминает об этом в своих теоретических рассуждениях, которые связывают каждое движение рук ребенка с небольшим отверстием, новой складкой в коре головного мозга.

Как это ни парадоксально, коннотации использования этого явления могут различаться по полярности – от сравнений с наркоманией до признания принципиально новой интеллектуальной спортивной дисциплиной. В иных странах спортивные чиновники отказываются признавать киберспорт как вид деятельности, а в некоторых считают это отличной идеей.

С точки зрения внедрения киберспорта в образовательный процесс учебных заведений МВД России стоит отметить, что согласно множественным современным исследованиям благодаря киберспорту происходит развитие мышления. К положительным качествам, которые может извлечь из киберспорта курсант образовательной организации МВД, относятся:

– ***реакция.*** Абсолютное большинство киберспортивных игр требует высокоскоростную реакцию на игровые моменты. Летящий «стан», «микробаш», быстрый «хилл» от «сапорта» и т. д. требует молниеносной реакции в игровом процессе и что немало важно владение хорошей мышечной памятью. Человек, которое длительное время увлекается киберспортивными играми и постоянно улучшает свои результаты быстрее всех и лучше всех «прожимает» необходимые комбинации для победы. В дальнейшей перспективе развития реакция может быть использована в жизни, например, при скоростной стрельбе или в боксе;

– ***скорость мышления.*** В процессе игры мы используем неосознанно быстрое мышление, как навык, с помощью которого, можно принять необходимое решение за доли секунды. Тут все, как и с реакцией, зависит от уровня тренированности игрока. Вследствие чего развивается навык быстрого решения, который будет постоянно необходим в опасной работе сотрудника полиции;

– ***концентрация.*** В исследовании, проведенном в Рочестерском университете, было установлено, что любители «стрелялок» раньше всех находят необходимые предметы вокруг себя. Благодаря киберспорту визуальное внимание курсанта позволяет удерживать свое зрение сразу на нескольких вещах одновременно. Вследствие чего развиваются концентрационные навыки, которые помогают бороться со стрессом на работе;

– ***социальные навыки.*** Раньше считалось, что соревновательные игры – это просто тренировка отзывчивости и скорости мышления, но теперь страсть к киберспорту имеет и другие положительные последствия. В первую очередь это касается социальных навыков. Общение – это важнейший навык нашего времени, от которого зависит общий успех человека в его карьере и других начинаниях. Вы можете быть гением хоть трижды, но вы не сможете выжить в мире без надлежащего общения, а киберспорт специально нацелен на развитие коммуникативных навыков. Коммуникация – это целый пласт полезных качеств, который включает в себя культуру общения, умение объединять людей, самоконтроль, умение выражать свою точку зрения так, чтобы ее могли понять другие. Благодаря социальным навыкам развивается и укрепляется общий труд, который в современном мире давно вытеснил индивидуальные достижения. Теперь все создается командами – учеными, изобретателями, разработчиками, строителями и представителями других профессий. Киберспорт – это ключ к эффективной командной работе и в бизнесе, когда каждый профессионал знает свои функции и выполняет их для достижения общей цели.

Благодаря этому умению курсант сможет разрешать конфликтные ситуации, находить общий язык с товарищами, вести переговоры с другими людьми. От этих характеристик зависит будущее благополучие. Киберспорт позволяет прививать и укреплять личные достижения, которые, несомненно, окажут положительное влияние на будущую карьеру и профессиональный успех;

– ***борьба со стрессом.*** В современном быстро меняющемся мире важно сохранять эмоциональную стабильность и способность принимать решения даже в критических ситуациях. Нет сомнений в том, что киберспортивные дисциплины создают эффективную систему управления стрес-

сом. Психическая устойчивость во времена сильного стресса – это качество, не имеющее цены.

Молодой игрок не сдается, когда терпит поражение. Напротив, игры учат сражаться даже после воображаемых поражений. В конечном итоге курсант, интересующийся киберспортом, не будет обижен неудачами на экзаменах или неудачами в личной жизни. Вместо этого он сохраняет самообладание, достоинство и, самое главное, психическое здоровье.

Яркий пример – это игра Dota 2, где почти всегда возможен так называемый «камбэк». Команды, проигравшие с самого начала, могут легко изменить ход игры благодаря уверенности и управлению стрессом;

– ***мотивация.*** Спортивные игры наглядно показывают цель и способы ее достижения. Традиционные виды спорта давно считаются лучшим способом мотивации. Навыку правильной и эффективной мотивации также учат в киберспорте. Неудовлетворенность достигнутым результатом и поиск мечты – это бесценная характеристика для подростков и детей.

Мотивация также предрасполагает к непрерывным тренировкам, которые необходимы во многих сферах деятельности в нынешних условиях. Обучающийся, которому нравится киберспорт, не сдастся на полпути – он «дочитает» английский язык, новый закон или учебник, необходимый для изучения;

– ***стратегическое мышление и логика.*** Киберспорт – это умная индустрия. Профессионалы и любители электронных соревнований регулярно оказываются в ситуациях, в которых необходимо «повернуть голову». Игроки создают общий план игры, ставят цели и задачи, как и в реальной жизни. Без бизнес-плана невозможен бизнес, без стратегии и логики немыслим успех. А спортивные игры научат планировать свои действия;

– ***адаптация к технологиям.*** В современном мире технологии развиваются безумно быстрыми скачками. Уже существует такой прогноз, что в недалеком будущем человек не будет успевать за свежими технологиями. В связи с этим, необходимо уметь адаптироваться к новым технологиям и именно от этого зависит, сможет ли курсант умело обращаться с новыми технологиями. Именно благодаря киберспорту и компьютерным играм человек начинает быстрее обучаться. Развиваются моторные, мыслительные и реакционные навыки, социальное взаимодействие

и командообразование, адаптивные навыки. Киберспорт дает основу для более продуктивного изучения других теоретических дисциплин, а именно повышает концентрацию, повышает уровень навыков в запоминании информации, а также скорость приятия решений в стрессовой обстановке.

Литература

1. Зборовский Г.Е., Александрова Т.Л., Журавлева Л.А. и др. Основы социологии для преподавателей и студентов. Екатеринбург, 1993.

2. Панкина В.В., Хадиева Р.Т. Киберспорт как явление XXI века // Физическая культура. Спорт. Туризм. Двигательная рекреация. 2016. № 3.

3. Симонович Н.Е., Горбунова О.С., Петрякова С.В. и др. Проблемы внедрения профессиональных стандартов: психологические особенности // Образование и право. 2019. № 5.

В.А. Медведев

КИБЕРСПОРТ КАК УЧЕБНАЯ ДИСЦИПЛИНА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ МВД РОССИИ

Уже много лет компьютерные и цифровые технологии используются в системе МВД. Они служат для облегчения работы с базами данных, организации составления именных списков, создания общей базы данных хранения протоколов и выполняют множество иных функций в области программирования и реализации многих функций МВД России [1].

На данный момент в системе МВД киберспорт не значится ни как теоретическая, ни как практическая дисциплина. Сущность киберспорта состоит из нескольких факторов таких, как четкая регламентация проведения таких соревнований законодательно.

Создание и моделирование виртуального киберпространства, внутри которого, располагаются различные виртуальные объекты, которыми и управляет сам игрок.

Если рассматривать киберспорт, как дисциплину, задействованную в обучении курсантов системы МВД, то можно выделить следующие потенциальные навыки: социальное взаимодействие, командообразование, навыки общения, навыки быстрого реагирования, навыки своевременного исполнения необходимых действий, умение анализировать оперативную обстановку, моторные навыки, реакция, скорость движений, скорость движений в мелкой моторике.

Такой широкий список навыков и умений, рассматривающийся в парадигме введения киберспорта в жизнь обуславливается тем, что киберспортивные соревнования организуются и проводятся в виртуальном пространстве, которое тоже имеет свои характерные особенности.

К основной характеристике применения киберпространства можно отнести безграничную моделируемость и изменяемость абсолютно всех составляющих киберпространства. В данном факторе могут быть предложены разнообразные варианты построения киберсистемы и подстраивания под необходимые для отработки навыков задачи и цели.

Для этого могут внедряться новые сценарии проведения игры, некоторые особенности управления, реагирования на отклик, состояния самого игрового пространства и выполнение действий [2]. Полученные навыки могут быть полезны в дальнейшей служебной деятельности и реализации практических предписаний.

Из этого можно сделать вывод, что добавив одну дисциплину в образовательный процесс, можно получить весьма большое количество полученных навыков и умений.

Таким образом, моделируя киберпространство и изменяя условия осуществления и реализации разнообразных моделей и концепций можно достичь формирования и развития разных навыков, которые будут играть большую роль в осуществлении практической деятельности [3]. К существенным навыкам, приобретаемым благодаря киберспорту можно отнести:

1. Командообразование – это процесс, который характерен не каждой группе людей, осуществляющей одну и ту же деятельность, но очень важный для слаженной командной работы в коллективе. Данная работа сможет существенно лучше и качественнее протекать, если каждый будет, подобно распределению ролей в игре, знать собственные сильные стороны и сильные стороны своих союзников.

2. Навыки общения в зависимости от той или иной дисциплины киберспорта могут меняться и принимать различные формы. Ключевыми формами являются скорость, точность передачи информации, а также ясность и истинность полученного сообщения. Именно от этих параметров в игре зависит, как тебя поймет союзник, зная данную информацию. Каков будет шанс, что он примет правильное решение в той или иной ситуации.

3. Навыки, настроенные на обеспечение быстрого реагирования, могут быть полезны для курсантов, чья будущая профессия будет связана с осуществлением оперативной деятельности. Именно этот вид деятельности, осуществляемый полицией, может быть улучшен путем развития навыков быстрого реагирования и повышения скорости ответных действий на то или иное поведение субъекта. Повышая скорость реакции на ту или иную ситуацию, поможет добиться повышения успеха.

4. Своевременное реагирование и быстрое реагирование – понятия тождественные, но они имеют одно важное различие, которое и определяет применение данного навыка и делает его полезным в определенных условиях. Таким условием является ситуативность. Мало просто осуществить быструю реакцию, нужно помимо этого среагировать в нужный момент или же, оценить оперативную обстановку и не спешить с ответной реакцией. Такой навык может улучшить тактическое мышление, добавив к нему оттенок стратегического анализа и продумывания ходов на несколько десятков вперед. Стратегический элемент позволяет в определенных условиях выиграть время путем сокращения действий, которые заведомо приведут к неверному результату или же не дадут его вообще.

5. Умение осуществления анализа в оперативной обстановке – это ключевой элемент в действиях оперативника. Прежде всего, анализ осуществляется только при наличии необходимых условий. В оперативной обстановке нет времени на такие условия, как отвлеченность и наличие времени на осуществление мыслительных операций. По сути, компьютерные игры ставят людей в такое же положение и заставляют принимать решение и анализировать ситуацию в кратчайшие сроки, при этом еще и параллельно занимаясь иными операциями. Таким образом, путем тренировки в играх, сотрудник оперативного подразделения будет учиться принимать решения в кратчайшие сроки и осуществлять анализ обстановки,

при этом тренируя навык быстрого изменения условий анализа и кардинально меняя цель от одного гейма к другому.

Далее стоит рассмотреть такое действие киберспортивной подготовки как влияние на формирование и развитие моторных навыков. Моторные навыки, как обособленный вид деятельности, имеют несколько не только главных и поверхностных значений, но и отдельно взятые значения, которые имеют непрямое действие в развитии качеств курсанта и сотрудника полиции.

Прежде всего, мелкая моторика делает реализуемым процесс мышления исходя из двигательного аппарата человека. Не является новшеством, и то, что человеку свойственно осуществлять мыслительную деятельность, одновременно подключая к ней двигательный аппарат. Таким образом, человек сам лично задает темп мыслительной деятельности и фокусирует внимание на чем-то отвлеченном, одновременно исполняя некоторые моторные действия. Роль мелкой моторики состоит в том, что повышение точности и стабильности действий (движений) рук, пальцев и кистей могут развивать такие качества как память, выстраивать более тонкое и точное мышление, а также в некоторых случая могут послужить средством снятия мышечного напряжения и нервного стресса.

Наиболее применяемыми техниками в развитии мелкой моторики, конечно, могут служить игра на музыкальных инструментах или занятия рукоделием, но сейчас появляется новая категория развития навыков мелкой моторики – киберспорт и тренировки в киберпространстве. Выполняя множество точных моторных движений, игрок достигает определенных результатов в игре, т. е., выполняет главное требование проведение состязания. И соответственно с этим, участники не только добиваются результатов в киберспортивных состязаниях, но и улучшают собственные навыки мелкой моторики.

Также необходимо проведение сравнительной параллели киберспорта и иных действий, развивающих мелкую моторику путем сопоставления их влияния на согласованность в работе полушарий мозга. Такая функция также очень важна в функционировании любой системы мышления. Поскольку киберспорт осуществляется путем использования обеих рук одновременно, и без данной связки существовать не может. Можно смело го-

ворить о том, что киберспорт задействует оба полушария и соответственно, развивает их согласованность.

Важным фактором, дающим киберспорту право на существование как теоретической, так и практической дисциплины, является постановка его осуществления в формате общей дисциплины, в своем пассивном действии, выстраивающей новые нейронные связи в коре головного мозга. Касаемо связей в коре головного мозга можно сказать то, что они создаются путем запоминания информации, проведения мыслительных операций и открытия для себя новых алгоритмов. Игровая деятельность содержит в себе все виды данных активностей, что благоприятно способствует формированию новых нейронных связей в коре головного мозга.

Литература

1. Корепова В.В. Киберспорт как основа создания спортивных кластеров // Кластеры. Исследования и разработки. 2017. № 3(8).

2. Панкина В.В., Хадиева Р.Т. Киберспорт как явление XXI века // Физическая культура. Спорт. Туризм. Двигательная рекреация. 2016. № 3.

3. Паныч Р.Б., Петровский С.С., Огурцов Д.А. Формирование положительного отношения к киберспорту как спортивной дисциплине // Педагогика. Вопросы теории и практики. 2019. Т. 4. Вып. 1.

4. Солодников В.В., Тимофеева В.И. Киберспорт в России как объект маркетинга и социальный феномен // Социологическая наука и социальная практика. 2020. № 1.

А.Г. Карпика,
Я.Е. Босенко

АНАЛИЗ БОЛЬШИХ ДАННЫХ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Интеллектуальный анализ больших данных и предиктивная аналитика получают признание в уголовных расследованиях и общественной безопасности. Предсказуемость насильственных преступлений является

основой поведенческого анализа насильственных преступлений. Во многих отношениях терроризм – это насилие с более широкой повесткой дня.

Терроризм и усилия по его поддержке также охватывают другие преступления, включая мошенничество, контрабанду, отмывание денег, кражу личных данных и убийства, которые в странах Европы были успешно расследованы с использованием интеллектуального анализа данных и прогнозной аналитики. Как и многие другие технологии, в Российской Федерации изучаются возможности использования интеллектуального анализа данных и предиктивной аналитики в криминалистике и анализе оперативных данных с некоторыми очень многообещающими предварительными успехами [1]. Эти инструменты далеко не предназначены исключительно для академических аналитических центров или крупных организаций, они легко доступны и доступны в среде персональных компьютеров. Дополнительная подготовка в области статистики, или искусственного интеллекта также не требуется. Скорее, знание предметной области является необходимой предпосылкой. Экспертиза в предметной области означает, что у вас есть практические знания о криминальной среде, которыми уже обладает большинство аналитиков и криминалистов.

Экспертиза предметной области позволяет проверять аналитические продукты на предмет их надежности, точности и ценности. Например, выявление надежной связи между террористами-смертниками и религиозным экстремизмом вряд ли улучшит способность бороться с терроризмом.

С другой стороны, способность точно характеризовать, обнаруживать, предвидеть и в конечном итоге предотвращать последующие атаки на основе тщательного анализа прошлого поведения, планирования и наблюдения будет иметь огромное значение в борьбе с терроризмом и защите общественной безопасности.

Недавние инновации в технологии позволили использовать аналитические продукты или алгоритмы оценки для оперативного персонала без формального обучения статистике. Эти модели можно использовать в полевых условиях для различных функций, включая оценку рисков, а также прогнозирование будущих событий или поведения. Подобно преступникам, террористы не уважают, а зачастую даже злоупотребляют юрисдикционными и национальными границами.

Во многих странах интеграция информации между уровнями исполнительной в лучшем случае ограничена. Это так называемое дублирование подвергалось широкой критике, потому что оно значительно компрометирует деятельность, дублируя ресурсы и усилия, ограничивая при этом доступ к информационным ресурсам между различными ведомствами.

Сложные программы для анализа больших данных и текстов доступны в настольной среде, для анализа, а также для широкого и быстрого развертывания в областях, где они нужны больше всего, особенно в правоохранительной деятельности. Безопасная информационная сеть и обмен информацией, связанные с этим, позволят аналитикам обмениваться информацией и выявлять более крупные закономерности и тенденции, в том числе те, которые выходят за рамки их оперативной экспертной оценки.

Во многих отношениях недостаточно просто обнаружить связи между событиями, фигурантами дела, необходимо иметь возможность быть в состоянии предвидеть следующий ход. Поведение человека, даже чрезвычайно агрессивное или необычное, часто следует предсказуемым закономерностям или тенденциям. Далее его поведение можно охарактеризовать, смоделировать, классифицировать и даже в некоторых случаях предсказать.

Фактически вся область оперативно-розыскного и следственного анализа, основана на этом выводе. Хотя поведенческий анализ может быть не в состоянии идентифицировать конкретного человека или подозреваемого, он часто может предоставить следователям дополнительные знания или понимание того, какой тип человека может быть связан с конкретным преступлением или серией преступлений. И, что более важно, этот тип анализа также может дать некоторое представление о том, какой тип поведения может предсказать насилие.

Во многих случаях и сценариях интеллектуальный анализ данных и предиктивная аналитика могут выявить вероятные мотивы, характеристики правонарушителя и факторы риска потерпевшего в насильственных преступлениях, если для анализа доступны соответствующие данные. Во многих смыслах терроризм можно охарактеризовать как насилие с более широкой целью. Хотя механизм может быть другим, предполагаемый результат один и тот же, т. е. достижение поведенческого контроля посредством запугивания, насилия или угроз насилием.

Способность охарактеризовать и предсказать такое поведение может иметь огромную тактическую и стратегическую ценность для организаций, профессионально противодействующих глобальной угрозе терроризма. Способность точно и надежно прогнозировать риски также может быть огромным преимуществом при принятии решений о направлениях деятельности в этой области.

Использование интеллектуального анализа данных и прогнозной аналитики для анализа исторических данных привело к созданию моделей, которые предсказывают, когда и где могут произойти инциденты. Определяя время и места, связанные с повышенной вероятностью риска инцидента, можно активно маневрировать имеющимися силами и средствами во времени и пространстве, тем самым более эффективно используя наши ресурсы и повышая вероятность быстрой идентификации и задержания, или сдерживания посредством усиленного присутствия правоохранительных органов.

Например, записи телефонных переговоров подозреваемых представляют собой бесценный источник информации, о конкретных лицах и группах. Как правило, анализ телефонных данных может занимать достаточно много времени и усилий, тем не менее, это одна из областей, где интеллектуальный анализ данных и прогнозная аналитика могут существенно повлиять на аналитические возможности [2].

Кроме того применение аналитики позволяет обнаруживать кражи личных данных, которые в различных формах присутствуют в большинстве мошеннических схем. Жертвы мошенников сталкивались и продолжаются сталкиваться с фактами злонамеренного использования своих личностей в попытке совершить мошенничество [3].

К сожалению, обнаружение кражи личных данных обычно происходит после того, как произошло преступление, либо злоупотребление, либо что-то еще более серьезное. Однако ручной поиск в этих наборах данных с целью упреждающего выявления случаев кражи личных данных или неправомерного использования является чрезвычайно сложным и неэффективным, учитывая чрезвычайно большой объем задействованной информации. В качестве альтернативы можно предложить автоматический поиск существующей информации с помощью технологии интеллектуального анализа данных, который может помечать недействительные, подозри-

тельные или повторяющиеся персональные данные, обнаруживая возможную их кражу до того, как наступят серьезные последствия.

Дополнительная информация, включая использование нескольких дат рождения или адресов, псевдонимов и мошеннических адресов, также может быть идентифицирована с помощью инструментов интеллектуального анализа данных. Этот подход не является панацеей от всех проблем, но он позволяет обнаружить достаточное количество случаев незаконного использования учетных данных, чтобы затруднить этот тип кражи персональных данных и сдержать преступное использование действительных данных в будущем. Это также может ограничить возможность террористов и киберпреступников использовать чувствительные для граждан и организаций информационные ресурсы, требующие для входа персональные данные, либо конфиденциальные данные организаций.

Литература

1. Дремлюга Р.И., Решетников В.В. Правовые аспекты применения предиктивной аналитики в правоохранительной деятельности [Электронный ресурс]. URL: https://atr.dvfu.ru/jour/article/view/61 (дата обращения: 10.04.2022).

2. Драгосавац Г. Аналитика больших данных в уголовных расследованиях [Электронный ресурс]. URL: http://www.bigdatanalysis.com/big-data-analytics-criminal-investigations (дата обращения: 10.04.2022).

3. Лемайкина С.В. Использование искусственного интеллекта в противодействии преступности // Юристъ-Правоведъ. 2021. № 2(97)

А.Г. Карпика,
Я.Е. Босенко

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ДИСТАНЦИОННОЙ ДЕЯТЕЛЬНОСТИ

2020–2021 гг. стали уникальными в истории человечества по причине появления новой коронавирусной инфекции. Пандемия, охватившая весь мир, существенно повлияла на повседневную жизнь людей.

Для предотвращения распространения эпидемии были использованы ряд мер, такие как: соблюдение социальной дистанции не менее метра; соблюдение масочного перчаточного режима; запрет на проведение массовых мероприятий. Когда стало понятно, что подобные способы противодействия неэффективны, ряд стран приняли беспрецедентное решение: всеобщий локдаун. Люди перешли в режим работы преимущественно в дистанционном формате. Единственными способами связи с окружающим миром остались интернет, радио и мобильная связь. Все это увеличило нагрузки на беспроводные сети.

Но что более важно в рамках данной темы – увеличилась целевая аудитория для совершения киберпреступлений. Исходя из причин изложенных ранее, а также обращаясь к данным, приведенным на официальных ресурсах [1], можно констатировать, что число совершенных киберпреступлений резко возросло по сравнению с предыдущим периодом. По различным подсчетам рост составляет 94 %.

Анализ данных показал, что большее всего выросла динамика следующих видов преступлений:

– неправомерный доступ к компьютерной данные (срыв дистанционных занятий, осуществление несанкционированный дистанционного управления компьютерами пользователей);

– обман граждан путем создания фишинговых веб-сайтов;

– сбор и продажа в даркнет персональных данных граждан, а также иной чувствительной конфиденциальной информации;

– обмен информацией о технологиях распространения наркотических веществ;

– осуществление кибератак на веб-сайты органов государственной власти, учреждений здравоохранения, социальных служб в целях неправомерного доступа к данным, нарушения порядка их работы, а также в целях вымогательства;

– вымогательство за счет направления гражданам сообщений в социальных сетях либо на адреса электронной почты, связанных с угрозами разоблачения якобы совершенных ими преступлений.

Кибератаки осуществляются не только на частных пользователей, но и на сайты государственных органов и организации, получая тем самым

не только личную информацию клиентов и пациентов, с целью последующего вымогательства.

Вымогательство осуществляется также с помощью создания различного рода благотворительных организаций и сайтов, собирающих денежные средства для противодействия и предотвращение последствий вирусной инфекции.

Обычно, в аналогичных обращениях законопреступники просят перевести деньги на счет в криптовалюте, потому что передвижения денежных средств в этом случае сложно проследить.

С целью борьбы с незаконным оборотом криптовалют задолго до пандемии Российская Федерация в ходе 74 сессии Организации Объединенных Наций предложила согласовать и утвердить конвенцию по борьбе с преступлениями в сфере применения информационно-коммуникационных технологий, которая бы позволила реализовать высокоэффективное международное сотрудничество в сфере борьбы с киберпреступностью.

В ключе данной статьи нельзя не упомянуть об инициированной Председателем Правительства М. Мишустиным реформы государственного аппарата. В рамках ее осуществления предполагается оптимизировать штат государственных гражданских служащих в центральных и территориальных органах государственной власти, что, как отмечает Глава Аппарата Правительства Д. Григоренко, позволит системе государственного управления стать более четкой, закономерной, ответствующей условиям времени [2].

Схемы интернет мошенничества, как правило, весьма изощрены и для того чтобы правоохранительные органы могли взять под контроль подобный способ правонарушений, органам внутренних дел необходимо работать на опережение.

Это возможно только при непрерывном совершенствовании законодательной базы, а также организационного механизма функционирования соответствующих органов власти. Работа по предотвращению киберпреступлений проводится постоянно. В штате каждой государственной структуры включен специальный отдел по противодействию преступлениям в сфере информационных технологий. На большинстве официальных сайтов

государственной власти работают специальные программы, защищающие информационные ресурсы от киберпреступников.

Таким образом, в качестве итога проведенного анализа можно предложить активизировать деятельность государственных и коммерческих организаций, направленную на социальное информирование и просвещение граждан и деловых клиентов о методах и средствах, которые используются киберпреступниками. Эту необходимую составляющую социальной политики возможно реализовать посредством социальной рекламы, внесения в художественные произведения сюжетов, демонстрирующих безопасные способы получения, хранения и распространения информации, безопасные способы предоставления своих персональных данных.

Литература

1. Сборник Генеральной прокуратуры о состоянии преступности в стране [Электронный ресурс]. URL: http://crimestat.ru/analytics (дата обращения: 10.04.2022).

2. Правительство утвердило дополнительные параметры реформы госаппарата [Электронный ресурс]. URL: http://government.ru/news/41299/ (дата обращения: 10.04.2022).

О.В. Кашникова,
Н.В. Задохина

ЦИФРОВОЙ ПОДХОД К ПРОФИЛАКТИКЕ СУИЦИДОВ

Согласно данным Всемирной организации здравоохранения (далее – ВОЗ), в настоящее время суициды (самоубийства) занимают одно из лидирующих мест в рейтинге причин смертности, уступая лишь сердечно-сосудистым заболеваниям, онкологии и травматизму. В этой связи всесторонний анализ природы суицида с целью выявления эффективных способов его профилактики становится особенно актуальным. Под суицидом понимается преднамеренное (осознанное) лишения себя жизни. Однако следует заметить, что самоубийством не считается:

– лишение себя жизни по неосторожности самого потерпевшего;

– лишение себя жизни человеком, не осознающим смысла своих действий или их последствий (лица, находящиеся в состоянии невменяемости, дети в возрасте до пяти лет).

Вышеуказанные ситуации относятся к категории несчастных случаев.

Суицид – смерть, являющаяся результатом поступка человека, совершенная умышленно и добровольно. Лишить себя жизни люди могут как психически здоровые, так и душевно больные.

Существуют разные виды суицидов – истинный, демонстративный, скрытый. Истинному суициду соответствует угнетенное состояние, депрессия, мысли о самоубийстве. И случается так, что даже близкие люди и друзья не замечают этого состояния. Можно выделить группы риска, в которую входят в основном подростки, размышляющие о смысле жизни и не находящие ответ на этот вопрос, и пожилые люди, которые, наоборот, думают, что их жизнь прошла впустую. Истинный суицид – это обычно хорошо подготовленный план действий. Человек выбирает дату, место, способ самоубийства.

Демонстративный суицид – такой вид самоубийств, при котором человек пытается достучаться до кого-то, показать свои проблемы. Примером может послужить ребенок, который хулиганит, чтобы привлечь внимание своих родителей, учителей, знакомых. Демонстрационный суицид может носить характер своеобразного шантажа.

Следующий вид суицида – скрытый. Самый распространенный вид самоубийства. Например, поездки в горячие точки, наркомания, алкоголизм и т. д. Иногда люди даже не задумываются о том, что таким образом сокращают свою жизнь.

Анализ статистических данных указывает на увеличение количества самоубийств за последние полвека на 60 %. Так, статистика ВОЗ за 2019 г. выделяет ряд стран, лидирующих по числу самоубийств. Первое место среди 183 стран занимает Лесото с показателем 87,5 человек на 100 тыс. человек населения. Второе место занимает Гайана с показателем 40,9. Далее идет Эсватини с показателем 40,5, одиннадцатое место занимает Россия с показателем 21,6, семнадцатое место занимает Казахстан с показателем 18,1, девятнадцатое место Украина с показателем 17,7, двадцать второе место занимает Беларусь с показателем 16,5.

Очевидно, что в создавшихся условиях поиск новых путей профилактики суицида трудно переоценить. Своевременно распознать потенциальных самоубийц способна, в первую очередь, психологическая служба, работающая совместно с медицинской службой. В России такой службой является, например, служба психологической помощи «Антикризис».

Предотвратить самоубийства могут и службы предотвращения суицидов, которые созданы международной ассоциацией по предотвращению самоубийств. Эти службы анонимны и охватывают большой круг людей, особое внимание уделяется людям, которые испытывают психологический кризис, являясь суицидо-опасными. Стоит отметить то, что все подразделения данной службы не находятся в психиатрических учреждениях.

Следующей службой является так называемый телефон доверия или анонимная телефонная служба, которая функционирует во многих странах мира. Целью данной службы, впервые заявившей о себе еще в 1953 г. в Лондоне, является анонимное общение пациента с сотрудником. Сотрудник, компетентный в области профилактики совершения самоубийств, может не только выслушать абонента, но и помочь ему преодолеть ту кризисную ситуацию, с которой абонент столкнулся.

В 2011 г. в США была введена программа Signs of Suicide Middle School and High School Prevention Programs, рассчитанная на возрастную категорию от 11 до 17 лет. Цели этой программы состоят в уменьшении числа самоубийств, поощрении личного обращения за помощью, привлечение родителей и школьного персонала в профилактике самоубийств. Эта программа каждый год внедряется в школы (средние и старшие) и включает в себя: уроки о признаках депрессии и ее предотвращении, скрининг выявления фактов риска суицида.

Существует также ряд антисуицидальных программ, функционирующих в виртуальном пространстве. Это, например, европейский сайт SUPREME, доступный для широкого круга лиц, но в первую очередь, для подростков от 14 до 24 лет. Сайт дает возможность человеку использовать чат и форум, в котором модераторы, специалисты в области психического здоровья, предоставляет информацию, указывающую на проблемы психического здоровья. Это и российский сайт «Тебе стоит жить», который позволяет получить исчерпывающую информацию о том, как удержать человека от самоубийства.

В настоящее время для профилактики суицидов успешно используются и системы искусственного интеллекта, способные выполнять творческие функции, которые традиционно считаются прерогативой человека.

Так, например, ученые Израиля, а именно из Израильского технологического института и Еврейского университета, создали систему искусственного интеллекта, с помощью которого определяется склонность к самоубийствам на начальных стадиях, благодаря анализу текста из всех социальных сетей. Эта система включает обработку естественного языка на основе использования многоуровневых нейронных сетей. Алгоритмы, реализуемые этой системой, хорошо извлекают любую информацию, содержащуюся в тексте. Изначально ученые акцентировали внимание именно на такие слова, как суицид, смерть, убийство. Круг слов расширился, когда было доказано, что люди, особенно из группы риска, редко используют в сети данные слова, предпочитая описание негативных эмоций или ругательства. Люди, не имеющие склонность к самоубийству, пишут в основном о позитивных эмоциях и событиях.

В Канаде разработали также приложение @Psy ASSISTANCE. Функция этого приложения – кризисный план безопасности. Это приложение предупреждает суицидальное поведение, дает оценку окружающего мира человека. Если человеку требуется неотложная психологическая поддержка, то приложение само может вызвать скорую помощь из ближайших медицинских учреждений.

Литература

1. Вихристюк О.В. К вопросу о современных программах профилактики суицидального поведения подростков и молодежи (обзор некоторых зарубежных программ) // Социальные науки и детство. 2020. № 1.

2. Пучнина М.Ю. Меры профилактики криминального суицида несовершеннолетних // Вестник Воронежского государственного университета. 2020. № 3(42).

3. Suicide rate estimates, age-standardized Estimates by country [Электронный ресурс]. URL: https://apps.who.int/ gho/data/node.main.MHSUICIDEASDR (дата обращения: 20.11.2021).

В.М. Смирнов,
Д.Д. Еремина

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 И ВВОДИМЫХ ОГРАНИЧЕНИЙ НА ЦИФРОВИЗАЦИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Актуальность исследования влияние пандемии COVID-19 на образовательный процесс, связана с его трансформацией в дистанционное обучение, которое невозможно без использования новейших цифровых технологий.

В результате интенсивного распространения коронавирусной инфекции Всемирная Организация Здравоохранения рекомендовала странам ввести ограничительные меры в связи с пандемией COVID-19. В России ограничительные меры затронули и сферу образования, которые выразились в установлении дистанционного образования для школ и вузов. Перевод на дистанционное образование невозможно без цифровизации образовательного процесса.

В конце 2019 г. в Китае был выявлен факт заражения COVID-19, а уже в 2020 г. была объявлена чрезвычайная ситуация в связи с быстрым распространением заболевания по территории страны. В России, начиная с марта 2020 г. отмечается увеличение количество лиц, заболевших COVID-19, что отражено на рис. 1.

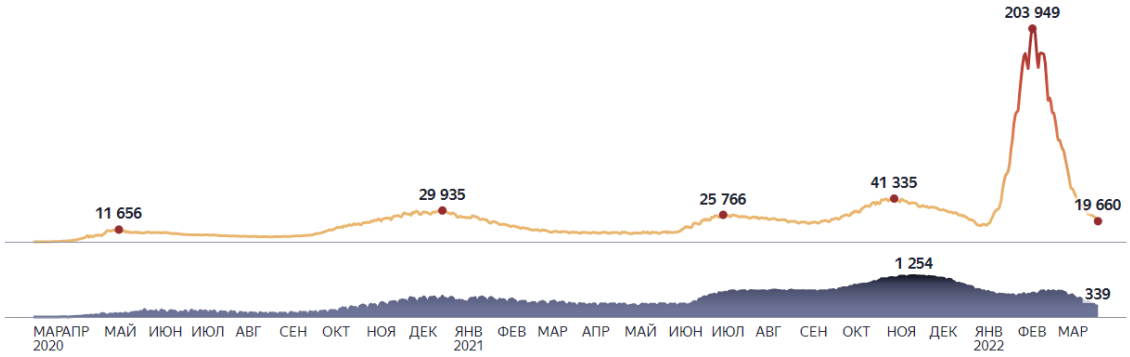

Рис. 1. Распространение коронавирусной инфекции в России с марта 2020 по март 2022 г. [1]

В связи с пандемией COVID-19 и вводимыми ограничениями цифровизация образовательного процесса связана с реализацией следующих направлений:

1. Создание цифровых платформ и инструментов, связанных с образовательным процессом. Пандемия внесла существенные коррективы в образовательный процесс, который трансформировался в дистанционное обучение.

По мнению представителей Юнеско, в России цифровизация школьного и вузовского образовательного процесса находится на должном уровне. Так выделяют следующие образовательные платформы и инструменты:

– портал EDU, который функционирует при поддержке Министерства образования и включает в себя самые разнообразные образовательные ресурсы;

– «моя школа» представляет собой образовательный сервис, включает в себя комплекс школьных уроков, информационную образовательную среду, которая позволяет наладить коммуникационный процесс между учениками, родителями и учителем;

– worldskills – цифровая платформа, где ученики и учителя смогут повысить уровень цифровой грамотности [2];

– образовательная Discord позволяет общаться преподавателям и обучающимся [3]. Преимуществом данной платформы является то, что она является бесплатной;

– система управления обучения Moodle, которая позволяет создать свой сайт для организации онлайн-обучения. Данное приложение является не только бесплатным и характеризуется открытым кодом, т. е. дает возможность организовать образовательный процесс в соответствии с потребностями образовательной организации [4].

2. С другой стороны, вопросы и проблемы цифровизации высшего образования решается не столь централизовано и комплексно. Каждое высшее учебное заведение самостоятельно определяет площадки и ресурсы, которыми будет пользоваться во время образовательного процесса.

Наличие технологических средств для цифровизации образовательного процесса, который подразумевает наличие компьютера, планшета, смартфона или специального устройства у преподавателя и обучаемого.

Однако, реализация данного пункта вызывает затруднение у малообеспеченных граждан, которые не в состоянии купить современный смартфон или планшет. Опрос показал, что около 9 % школьников не смогли продолжить образовательный процесс дистанционно ввиду отсутствия необходимых устройств [5].

Внедрение телекоммуникационных технологий. Образовательный процесс – это не только получение знаний, но также и налаживание эффективного коммуникационного процесса между преподавателем и обучающимся.

В условиях пандемии данный вопрос решался посредством использования таких приложений, как Zoom и Skype.

Вместе с тем чиновники обращали внимание на то, что данные, полученные в результате использования иностранных коммуникативных платформ, могут использоваться зарубежными государствами. Поэтому в этом году планируется запустить цифровую образовательную платформу «Сферум» [6].

Цифровая грамотность преподавателей обучающихся, находится не на должном уровне.

Одной из проблем цифровизации образовательного процесса является отсутствие либо низкий уровень цифровой грамотности преподавателей. При этом курсы по повышению квалификации в данном направлении для преподавателей стартовали только в октябре 2021 г. [7]. Обучаемые должны самостоятельно вникать в особенности нового дистанционного обучения, который осуществляется посредством цифровых технологий.

Введение дистанционного образования и цифровизация образовательного процесса оказало негативное влияние на сам уровень образования, который имеет тенденцию к снижению, как в общеобразовательной, так и высшей школе [8]. Данная проблема связана с тем, что отсутствуют программы и механизм самоорганизации школьников и студентов.

Анонимный опрос студентов и школьников показал, что повысилась частота списывания в процессе сдачи контрольных испытаний:

– около 40 % списывали на экзаменах. При этом преподаватель не имеет реальной возможности проверить, сам ли студент подготовился к ответу или воспользовался интернет-ресурсами;

– 30 % учащихся халатно относились к семинарским занятиям;

– 25 % скачивали доклады из Интернета, и сдавали преподавателю, не читая их.

Помимо этого, у 75 % учащихся отмечается психологическое неблагополучие, вызванное отсутствие реального общения с преподавателями и сверстниками [9].

Для решения указанных проблем необходимо:

– разработать программы по оказанию психологической поддержки учащимся и преподавателя;

– внедрить систему аудита, которая отслеживала уровень образования;

– изменить цифровую инфраструктуру образовательного процесса, методы контроля за студентами и школьниками, инструменты обучения и выставления оценок.

Таким образом, цифровизация образовательного процесса является неотъемлемой частью внедрения дистанционного обучения и характеризуется комплексным подходом к решению данной проблемы.

Литература

1. Коронавирус в России [Электронный ресурс]. URL: https://index.minfin.com.ua/reference/coronavirus/geography/russia/ (дата обращения: 24.04.2022).

2. Национальные учебные платформы и инструменты [Электронный ресурс]. URL: https://en.unesco.org/covid19/educationresponse/nationalresponses (дата обращения: 24.04.2022).

3. Образовательная платформа Discord [Электронный ресурс]. URL: https://discordgid.ru/dlya-distancionnogo-obucheniya/ (дата обращения: 24.04.2022).

4. Moodle [Электронный ресурс]. URL: https://moodle.org/?lang=ru (дата обращения: 24.04.2022).

5. Цифровые технологии кибербезопасности в контексте распространения COVID-19. М., 2020.

6. Сферум – образовательная платформа [Электронный ресурс]. URL: https://sferum-russia.ru/ (дата обращения: 24.04.2022).

7. Стартовала программа по цифровой трансформации образования для педагогов [Электронный ресурс]. URL: https://ficto.ru/novosty/1172 (дата обращения: 24.04.2022).

8. Депутат о цифровизации образования: Москве грозят демографические риски [Электронный ресурс]. URL: https://news.rambler.ru/-education/47124856-deputat-o-tsifrovizatsii-obrazovaniya-moskve-grozyat-demograficheskie-riski/ (дата обращения: 24.04.2022).

9. Как вузы перестали бояться дистанта, и как это связано с качеством образования [Электронный ресурс]. URL: https://skillbox.ru/-media/education/kak-vuzy-perestali-boyatsya-distanta/ (дата обращения: 24.04.2022).

10. Данилова Л.Н. COVID-19 как фактор развития образования: перспективы цифровизации и дистанционного обучения // Вестник Сургутского государственного педагогического университета. 2020. № 5.

А.И. Харитонова,
Н.М. Дубинина

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ЛИЧНОСТИ

Биометрические технологии идентификации и аутентификации личности в настоящее время быстро развиваются и интегрируются в повседневную жизнь. Внедрение биометрических технологий стало прорывом в области защиты конфиденциальных данных и новой мировой тенденцией: практически каждый смартфон оснащен сканером отпечатка пальца или системой FACE-ID (распознавание лица), по всему миру стали популярными биометрические паспорта, в которых на электронном чипе сосредоточена вся необходимая информация о человеке и пр. В связи с этим остро встает вопрос о защите конфиденциальных данных пользователей, о сведении к минимуму угроз их распространения и утечки, обеспечения безопасности персональных данных и иной информации о физических и юридических лицах.

Традиционными способами защиты конфиденциальных данных являются использование сетевого имени и пароля. Однако все это, особенно в современном мире, является ненадежным. Учитывая те массивы данных, с которыми человек сталкивается и использует каждый день, очень сложно сохранить конфиденциальность только лишь с помощью пароля, который можно забыть или потерять. Биометрия же основывается на идентификации пользователя по статистическим и динамическим параметрам, что позволяет быстрее и точнее работать с информацией.

Биометрические методы идентификации пользователя классифицируются на основании использования отдельных особенностей человеческого организма и разума [1].

К статистическим средствам относятся физиологические особенности человека, которые он приобрел от рождения. Это ДНК, отпечатки пальцев, радужная оболочка глаза и другое.

К динамическим средствам относятся поведенческие особенности человека, то, что он совершает на подсознательном уровне в процессе какого-либо действия. Например, походка, голос, воспроизведение подписи и иное.

На современном этапе развития технологий биометрическая идентификация пользователя является действенной, точной и более надежной по сравнению с другими методами. Благодаря процессу идентификации человека, то есть анализу его характеристик с теми, что заранее внесены в базу данных, удается с максимальной точностью определить, имеет данный человек доступ к интересующей его информации или нет.

Рассмотрим самые популярные и наиболее распространенные способы и методы защиты конфиденциальных данных [2].

1. Распознавание по отпечатку пальца. Данный метод основан на распознавании уникального узора, расположенного на подушечке пальцев руки. При помощи специального сканера отпечаток пальца сравнивается с тем, который был задан ранее. Такой способ из-за своего удобства и простоты использования получил, пожалуй, самое широкое распространение во всех сферах жизни человека. Как мы знаем, не существует людей с одинаковыми отпечатками пальцев, такой узор является индивидуальным и даже у близнецов они совершенно разные.

2. Распознавание по радужной оболочке глаза. По ней создается специальный код, который помогает идентифицировать пользователя. Этот метод также крайне сложно обойти, так как рисунок радужной оболочки глаза формируется еще до рождения ребенка и является довольно сложным, но четким. Особую популярность этот метод приобрел с 2015 г., когда стал широко использоваться для работы с мобильным телефоном.

3. Распознавание по форме кисти руки. Каждый человек обладает своей неповторимой геометрией рук. Метод основывается на описании длины и ширины пальцев, изгибов, расстоянию между суставами. При помощи диодов и камеры создается трехмерная модель кисти руки и происходит распознавание человека. Несмотря на то, что по некоторым показателем у разных людей можно заметить сходство, полное соответствие маловероятно. Однако данный метод имеет довольно существенный недостаток: различные повреждения, а именно, царапины, ушибы, порезы довольно сильно снижают эффективность аутентификации человека.

4. Распознавание по форме лица. Этот метод заключается в описании основных элементов лица человека: формы губ, уголков глаз, бровей и т. д. Далее на основе полученных данных строится объемное изображение. Стоит отметить, что распознавание формы лица также учитывает и различные вариации, в случае наклона головы или изменения выражения лица.

5. Распознавание голоса. Основано на сочетании статистических и частотных характеристик голоса. Однако этот метод является далеко не самым надежным. Ведь правонарушитель может воспользоваться диктофонной записью, что сильно снижает степень защищенности. Также не стоит забывать и о том, что в течение жизни и с изменением состояния здоровья голос может изменяться.

6. Графологическое распознавание. Представляет собой распознавание почерка человека. Для считывания таких данных используют приборы-стилусы, фиксирующие информацию о силе давления на поверхность.

В настоящее время ни один метод не может дать пользователю абсолютной гарантии его точной идентификации, бесперебойной аутентификации личности и полной защиты конфиденциальных данных, однако,

чтобы обойти систему безопасности, использующую биометрические данные, необходимо иметь высокий уровень подготовки и осведомленности в данном деле. Каждый процесс имеет сильные и слабые стороны. Использование биометрических методов не исключение.

К преимуществам можно отнести: высокий уровень надежности, легкость и удобство применения и использования, низкая вероятность завладения данными злоумышленниками, а также всеобщность, уникальность, измеримость [3].

К недостаткам относятся: высокая цена, т. к. сложная аппаратура требует больших финансовых затрат, социальные и религиозные предрассудки. Биометрия позволяет точно идентифицировать пользователя, однако полагаться на нее как на единственный уровень защиты не стоит.

Использование биометрических методов помогает сделать жизнь человека удобнее и в то же время безопаснее.

Широкий спектр возможностей биометрия открывает в банковском деле, что сильно облегчает жизнь банку и его клиентам. Биометрические технологии способны снизить количество краж данных, случаи мошенничества, а также намного упростить процедуру работы клиента с банкоматом.

Руководство Сбербанка в 2017 г. запустило пилотный проект по идентификации клиента банкоматом по лицу. А уже в 2021 г. Сбербанк внедрил идентификацию в 21 000 своих банкоматов. Таким образом, почти половина банка оснащена подобной технологией. Многие эксперты в целом поддержали данную идею, но указали на риск роста случаев мошенничества и предложили ввести дополнительный способ подтверждения транзакции. Для того, чтобы клиент мог совершать операции без материального носителя, через биометрический банкомат, он должен предоставить банку свои биометрические данные (слепки лица). После этого данные будут внесены в специальную базу данных или будут записаны на чип карточки. Внутри самого биометрического банкомата находятся сенсорные устройства, которые и считывают уникальные данные человека. Эти данные отправляются в банк и сверяются с базой данных. В случае их совпадения клиент получает доступ к своему счету и может продолжить работу с ним.

Каждого клиента волнует сохранность и безопасность предоставляемых персональных данных. Несанкционированное использование биометрии может угрожать финансовой безопасности граждан, что вызывает опасение среди пользователей.

В первую очередь клиентов волнует утечка данных. Ведь они предоставляют свои персональные данные в Единую биометрическую систему (ЕБС) или собственные биометрические системы данных. Несмотря на то, что существует риск утечки биометрических данных, использовать их для несанкционированной идентификации довольно сложно. Ведь при предоставлении биометрической информации в базе данных остается лишь некий слепок в виде набора характерных признаков. Биометрические системы банков используют более продвинутые алгоритмы биометрической системы, чем современные смартфоны. И обмануть их с помощью, например, фотографии владельца не получится.

Современные технологии постоянно развиваются, и мошенники придумывает все новые и высокотехнологические способы получения конфиденциальной информации [4]. Например, использование дипфейков. С помощью данной методики нейросеть способна сгенерировать видео, изображение или голос, который имитирует реального человека. Все это действительно несет серьезные риски. Однако данный метод является очень дорогим, что скорее всего не окупится проворачиванием данной махинации. Стоимость создания качественного дипфейка намного выше, чем остатки на счетах обычного среднестатистического клиента банка.

Банки дорожат своей репутацией и клиентами, поэтому стремятся обезопасить их персональные данные от несанкционированных операций и сделать процедуру идентификации личности как можно надежнее. Именно поэтому биометрическая идентификация используется в совокупности с дополнительными средствами защиты. Например, многофакторное подтверждение проводимой операции: система безопасности проверяет не только полученные биометрические сведения, но и IP-адрес, номер телефона, местоположение устройства, с которого приходит информация. И уже учитывая все компоненты безопасности, пользователю открывается доступ к системам.

В заключении хотелось бы подчеркнуть, что внедрение биометрической идентификации позволило повысить уровень защиты конфиденциальных данных. К перспективным направлениям развития можно отнести: мультимодальную биометрию – использование биометрических данных в их сочетании, например, отпечатков пальцев и радужной оболочки глаза; поведенческую биометрию (динамические методы аутентификации); распознавание эмоций при биометрическом распознавании лиц.

Литература

1. Вихман В.В. Биометрические системы контроля и управления доступом в задачах защиты информации: учебно-метод. пособие. Новосибирск, 2016.

2. Болл Руд М., Коннел Джонатан Х., Панканти Шарат и др. Руководство по биометрии. М., 2007.

3. Биометрические технологии идентификации личности: учебное пособие / Ю.А. Брюхомицкий. Ростов н/Д, Таганрог. 2017.

4. Ворона В.А. Биометрическая идентификация личности. М., 2021.

А.В. Макарова,
Р.И. Черкасов

К ВОПРОСУ ОХРАНЫ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В КОНТЕКСТЕ РАЗМЕЩЕНИЯ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ СРЕДЕ

На протяжении всего процесса развития человека, как разумного существа, результаты интеллектуальной деятельности тем или иным способом увековечивались в истории. К таким попыткам можно отнести и наскальную живопись, благодаря которой мы можем узнать о жизни древних людей, и различные записи, сделанные на поверхностях различного характера, доступных для людей. Современный этап развития человечества, можно смело считать этапом всеобщей информатизации. И конечно,

информация, как результат умственной деятельности человека, вносится в различные электронные базы, в том числе и в глобальную сеть Интернет.

Если говорить об интеллектуальной собственности в широком смысле слова, то на уровне государственного устройства, результаты умственной деятельности человека, оформленные в виде научно-технических и исследовательских трудов, выступают необходимым фактором развития страны в целом. Важность и актуальность активности в сфере инноваций в настоящее время находится на достаточно высоком уровне и зачастую играет решающую роль при определении положения страны на экономической и политической карте мира. Интеллектуальная собственность на современном этапе развития общества, уже по праву считается одним из важнейших стратегических ресурсов государства, обеспечивающим его конкурентоспособность фактически во всех сферах деятельности. Именно поэтому процесс развития норм правовой защиты отрасли интеллектуальной собственности является одним из важнейших в правоохранительной и правоприменительной деятельности органов власти [1].

В настоящее время в Российской Федерации существует большое количество нормативных правовых актов, несущих под собой цель охраны интеллектуальной собственности. Гражданский кодекс Российской Федерации (далее – ГК РФ), в ст. 1225 «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации» результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются, в числе прочего: программы для электронных вычислительных машин (программы для ЭВМ); базы данных; изобретения; полезные модели [2].

Здесь так же необходимо отметить, что интеллектуальная собственность обладает рядом характерных признаков. Во-первых, данный вид собственности фактически всегда нематериален. Данное свойство обеспечивает возможность одновременного, порой параллельного и независимого использования одного объекта несколькими субъектами. Во-вторых, правоотношения в данной сфере имеют абсолютный характер, обусловленный тем, что обладателю права на интеллектуальную собственность

противостоят все посторонние лица, не имеющие права препятствовать его деятельности или распоряжаться данным объектом без разрешения правообладателя. И в-третьих, объекты интеллектуальной собственности, имея нематериальный характер, зачастую выражены в материальных носителях, права собственности, на которые необходимо отделять от рассматриваемых нами прав на интеллектуальную собственность.

Закон так же предусматривает ряд прав на интеллектуальные объекты. Основным можно выделить конечно же имущественное право, которое предполагает то, что правообладатель или, иными словами, субъект права наделен возможностями использования объекта теми способами, которыми посчитает нужным, при этом для третьих лиц данные действия без получения согласия для правообладателя строго запрещены, однако данное право может быть передано. Так же здесь можно выделить личные неимущественные права, такие как: право на имя, на авторство и т. д. Данный вид прав не имеет срока давности и подлежит охране на бессрочной основе и является неотчуждаемым.

ГК РФ предусматривает ряд достаточно эффективных способов защиты интеллектуальных прав, в основном отнесенных к группе личных неимущественных прав. Среди них можно выделить: признание права обществом и государством; восстановление положения правообладателя в отношении прав на интеллектуальную собственность; безусловное пресечение деятельности или действий посягающих на интеллектуальное право; возмещение, пострадавшей от действий третьих лиц стороне, морального вреда и наконец достаточно действенная мера предназначенная для восстановления имени и репутации автора – публикация в различных источниках судебного решения о нарушении норм интеллектуального права.

На современном этапе развития информационных технологий, немаловажную роль в вопросе выявления случаев нарушения прав на интеллектуальную собственность играют системы распознавания текстов. В данном направление вот уже как несколько лет ведется серьезная, кропотливая работа, результат сотрудничества ученых и программистов в Российской Федерации и в зарубежных странах. В данном направлении важно осознавать значимость практического опыта, приобретенного в период, скажем так, ручного сличения различных текстов в самых разных

источниках публикаций. На данный момент системы мониторинга имеют возможности полного сканирования текстов, выявления неправомерного использования интеллектуальной собственности, а также при необходимости и вынесении решения соответствующими органами, их удаления [3].

Но нельзя не отметить и ряд достаточно серьезных проблем, связанных с защитой прав на интеллектуальную собственность. В первую очередь, в условиях, когда многим российским учены вменяется, как обязанность, публикация материалов в изданиях из так называемой библиографической и реферативной базы цитирований Scopus. Материалы, публикуемые в таких, в основном зарубежных изданиях, автоматически становятся доступны для изучения фактически во всех странах мира. Да, если говорить о принципах глобализации и мирового научного сотрудничества, данную практику можно считать положительной. Однако сегодняшнее, пока еще возможно сугубо теоретическое научное исследование, завтра может стать основой для серьезного изобретения в одной из критических сфер отечественной науки. Как же быть в случае, когда опубликованная ученым в зарубежной базе научная работа стала как раз основой для новой разработки государственной важности?

Не совсем ясен и механизм защиты интеллектуальной собственности наших ученых, вынужденных публиковать результаты своей научной деятельности в зарубежных изданиях. Ведь необходимо понимать, что не всегда такие исследования успевают быть защищены, а именно запатентованы согласно ответственным правила патентования, а уж тем более зарубежными патентными бюро. Да и сам механизм защиты российских исследований патентами службы по интеллектуальной собственности, в условиях, когда информация из этих патентов публикуется в глобальной сети Интернет, на наш взгляд имеет широкие перспективы для доработки.

Хотелось бы немного поговорить о зарубежном опыте защиты прав на интеллектуальную собственность. Регулирование вопросов интеллектуальной собственности в ведущих странах запада происходит по-разному, но при этом имеют и некоторые сходства. В ведущих европейских государствах, а также в Японии исконно сильны структуры государственного уровня,

работа которых направлена на успешную коммерциализацию результатов интеллектуальной деятельности ученых, полученных за счет средств государственного бюджета. В Соединенных Штатах Америки при соблюдении определенных условий права на интеллектуальную собственность, полученную за счет государственных ассигнований, могут быть переданы третьим лица или подрядным организациям-разработчикам. В этой стране наибольшее распространения получила такая модель деятельности, при которой конкретно организации-подрядчики наделены самыми большими возможностями для управления коммерциализацией.

В заключении хотелось бы отметить, что в связи со всеобщей цифровизацией человеческой деятельности, вопрос развития отрасли права, связанной с защитой интеллектуальной собственности, приобретает достаточно серьезный характер и является достаточно актуальным. Развитие данной отрасли права должно быть направлено на совершенствование механизмов выявления нарушений прав интеллектуальной собственности в глобальной сети Интернет, ужесточение ответственности за правонарушения в данной области, а также изменение принципов защиты результатов интеллектуальной деятельности на различных уровнях.

Литература

1. Гаджиева А.М. Оценка, правовая охрана интеллектуальной собственности и защита интеллектуальной собственности // Экономика и предпринимательство. 2018. № 7(96).

2. Макаричев А.В. «Интеллектуальная собственность» и «право интеллектуальной собственности»: соотношение понятий // Юридические науки. 2011. № 3.

3. Rizaev N.K. Improving analysis of the intellectual property objects // Международные стандарты учета и аудита: практика применения в условиях цифровой экономики: сб. статей Междунар. научно-практ. конф. М., 2020.

Р.Ю. Рунаев

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ВУЗАХ МВД РОССИИ

Начало XXI в. характеризуется интенсивным ростом потока информации. В этих условиях понятие грамотности, образованности должно включать в себя и владение компьютером как необходимым инструментом анализа, обработки и хранения информации в любой области интеллектуальной деятельности. Компьютер стал символом сегодняшнего дня, и использование в сфере образования современных информационных технологий открывает перспективы для реализации принципиально новой методики преподавания. Сейчас на каждом занятии слушателю приходится усваивать большое количество учебного материала. Отсюда вытекает необходимость пересмотра образовательного процесса, с целью его приведения в соответствие с требованиями времени.

В условиях современной парадигмы образования «учись учиться», задача обновляющейся педагогики состоит в том, чтобы не только создать условия для роста и развития молодого человека, но и научить его без посторонней помощи находить нужную информацию и умело ее использовать. Педагогика, нацеленная на стимулирование самостоятельной учебы, приобщение каждого слушателя к ежедневному напряженному умственному труду и воспитание познавательной независимости как качества личности, укрепление в каждом слушателе чувства уверенности в своих силах и способностях, строится на представлении об активном человеке. Переход к таким формам работы, в которых акцент делается на инициативу, самостоятельное приобретение знаний, означает изменение культуры преподавания, заключающееся в систематическом применении в учебном процессе современных компьютерных технологий.

Иначе говоря, компьютер становится не только и не столько объектом изучения, сколько средством обучения, необходимым инструментом, без которого в современных условиях достаточно сложно себе представить

процесс получения новых знаний. Как средство обучения персональный компьютер открывает преподавателю практически неограниченные возможности для достижения дидактических целей.

Например, проведение деловых и ролевых игр, анализ и моделирование конкретных профессиональных ситуаций с использованием компьютерной техники (например, *интерактивная «реалистик»-игра, где слушатель осуществляет осмотр жилого помещения или обысковые мероприятия в отношении подозреваемого*) способствует наглядному представлению изучаемых тем профильной учебной дисциплины, повышению у слушателей интереса к решению поставленной проблемной ситуации, развитию творческого мышления и, как следствие, более глубокому и прочному усвоению учебного материала [1].

Однако для того, чтобы с достаточной эффективностью использовать преимущества современных компьютерных технологий в предстоящей профессиональной деятельности, будущему специалисту потребуются хорошие знания этих технологий с учетом внедрения дистанционных программ профессионального обучения, устойчивых навыков владения компьютером как инструментом познания и решения конкретных задач. Уже на стадии обучения, приобретения знаний компьютер дает слушателю возможность глубже вникнуть в смысловое содержание предлагаемых к закреплению учебных дисциплин.

Объектом изучения персональный компьютер становится, как правило, на первом году обучения в курсе информатики. В рамках этой дисциплины преподаватель должен заложить хорошие теоретические знания, привить слушателям навыки выполнения элементарных операций, дать принципы действия компьютерной техники и организации работы программных продуктов общепрофессиональной направленности. Это в дальнейшем позволит легко осваивать новые программные продукты, станет надежным «трамплином» для последующего самообразования и прочной опорой в профессиональной деятельности.

Но привить устойчивые навыки работы с персональным компьютером возможно только в случае систематического его использования для решения тех или иных задач, постоянного общения с ним. В настоящее время сложилась ситуация, когда после сдачи экзамена по информатике

на первом курсе, последующее эпизодическое использование компьютера (либо использование его не по *учебному*, а, например, по *игровому* назначению) лишает слушателя возможности углубления своих знаний по выбранной специальности. Слушатели второго курса еще помнят что-то из курса информатики, но они пока не приступали к изучению специальных дисциплин. К старшим курсам, когда начинается преподавание профилирующих предметов, приобретенные год или два назад навыки применения компьютерных технологий в оттачивании профессиональных знаний и умений неизбежно утрачиваются, что в немалой степени затрудняет освоение профилирующего программного обеспечения.

Решением проблемы может стать проведение на втором и третьем году обучения учебных занятий по тематике специализированных кафедр, а в дальнейшем – создание интегрированного комплекса дисциплин, изучаемых на базе компьютерных технологий последнего времени. Без прикладного аспекта использования персонального компьютера будущему полицейскому совершенно невозможно обойтись в некоторых областях своей профессии, например, в экспертно-криминалистической деятельности. Сложно отработать «на коленке» или нарисовать «по памяти» приметы подозреваемого без обращения к соответствующей базе составления композиционных портретов преступников со слов очевидцев, либо совершенно невозможно проверить пальцевые отпечатки возможных злоумышленников без обращения к специализированной базе данных АДИС «Папилон».

К сожалению, любительский уровень пользования компьютерными технологиями может быть присущ не только слушателям, но и некоторой части профессорско-преподавательского состава, которая испытывает неудобства не столько из-за отсутствия навыков программирования, без которых в подавляющем большинстве случаев в процессе обучения можно обойтись, сколько из-за недостатка знаний об идеологии, методах и возможностях информационных технологий. Многим специалистам «старой школы» достаточно сложно преодолеть психологический барьер перед компьютером в силу своей инертности, особенно тем, кто уже проработал в области педагогики долгие годы, и до сих пор обходился имеющимся наборов обучающих средств. Они рассуждают так: «Прежде и без

компьютера готовили специалистов высокой квалификации, почему теперь нельзя?»

Но использование компьютера позволит освободить и преподавателя, и слушателя от многих рутинных действий, оставит время для индивидуальной работы, результатом которой будет развитие навыков исследования, мышления и общения. В ситуации приобщения к актуальному информационно-технологическому сопровождению учебных занятий, будет всемерно возрастать интерес самих слушателей к учебному процессу. Так, вполне очевиден выбор обучающихся в пользу того преподавателя, который с помощью мультимедийной презентации, ярко и красочно, с наглядно-иллюстрированным материалом, предлагает к закреплению тему учебной дисциплины, в противовес его коллеге с закоснелыми педагогическими взглядами, который убежден, что сможет только лишь своим «лекторским» красноречием в течение нескольких академических часов удерживать внимание обучающихся на актуально-высоком уровне.

Желательно, чтобы сознание выпускников вуза было в состоянии охватить информационное пространство сегодняшнего дня, что потребует высокого уровня информированности о достижениях науки, техники и технологии. Ведь потребность обращаться к информационным системам не складывается стихийно, она воспитывается как результат активного и заинтересованного отношения к информации [2]. Коммуникабельность и продуктивность мышления, умение видеть проблему и не бояться ее новизны, ориентация в современном информационном пространстве и работа с ним – это личные качества, спрос на которые в современном обществе высок [3]. Формирование и развитие таких качеств у будущих специалистов, наряду с воспитанием активной творческой позиции, является одной из первостепенных задач образовательного учреждения МВД России.

Литература

1. Политика в области образования и новые информационные технологии. Национальный доклад Российской Федерации на II Международном конгрессе ЮНЕСКО // Информатика и образование. 1996. № 5.

2. Влияние научно-технического прогресса на юридическую жизнь / отв. ред. Ю.М. Батурин. М., 1988.

3. Психология и педагогика: учебное пособие / под редакцией А.А. Радугина. М., 1996.

В.В. Худяков,
Г.Р. Фахретдинова

О НЕКОТОРЫХ ВОПРОСАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА МВД РОССИИ

С внедрением сервиса электронного документооборота (далее – СЭД) единой системы информационно-аналитического обеспечения деятельности (далее – ИСОД) МВД России значительно упростился обмен документами и корреспонденцией между подразделениями внутри ведомства, так и за его пределами на уровне межведомственного взаимодействия. Значительно сократилось время создания документа, упростилась процедура согласования с ответственными и участными в создании документа должностными лицами. Наличие на документе усиленной квалифицированной электронной подписи позволяет установить личность подписанта и его причастность к документу, а также убедиться в целостности самого документа после его подписания. Электронная форма документа не требует дополнительных площадей и свободных полок на стеллажах в архивах, вся информация хранится на компьютере делопроизводителя или в специально отведенном цифровом хранилище данных.

В период времени, когда электронный документооборот отсутствовал повсеместно, делопроизводство на бумажной основе выглядело равномерно и обыденно во всех сферах деятельности сотрудников органов внутренних дел. С введением СЭД в эксплуатацию и переводом документооборота в область электронного обмена данными, стал отчетливо наблюдаться контраст в подразделениях органов внутренних дел, где функционал сервиса электронного документооборота был реализован. Удручающе проявили себя сферы деятельности сотрудников органов внутренних дел,

где электронный документооборот не был развернут и не получил должного распространения. Если обмен документацией внутри ведомства и в системе межведомственного электронного взаимодействия с государственными органами реализован, то обмен корреспонденцией с негосударственными и коммерческими организациями остался на бумажной основе.

Предлагается рассмотреть проблему негативного влияния бумажного документооборота на ход и качество расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Совершенно очевидна актуальность данной тематики, в виду имеющейся потребности ОВД в своевременном и оперативном получении информации от обозначенных выше негосударственных организаций [1].

Анализ преступности последних лет показал взрывной характер роста киберпреступлений и преступлений в сфере информационно-телекоммуникационных технологий, к которым также относятся преступления, связанные с хищением безналичных и электронных денежных средств с использованием кибертехнологий.

Практический опыт работы по разрешению вопросов подготовки и направления запросов в представительства компаний операторов сотовой связи, финансово-кредитных учреждений, площадок электронной коммерции (маркетплейсов), социальных сетей и т. д. показал неподготовленность и отсутствие договоренностей между правоохранительными органами и перечисленными участниками документооборота, что соответственно затрудняет расследование данной категории уголовных дел.

Значительную сложность в работе сотрудников следственных органов и оперативных подразделений представляют мероприятия по сбору доказательной базы по уголовным делам в области киберпреступлений, когда необходимо получить информацию из коммерческих компаний, операторов сотовой связи, маркетплейсов (данных о клиентах и пользователях, детализации соединений, операции с денежными средствами и др.) и т. д. с использованием бумажного документооборота. Можно предположить, что при наличии электронного документооборота общая картина эффективности работы сотрудников органов внутренних дел выглядела бы совершенно иначе. В действительности об этом говорить и не приходится по причине того, что электронный документооборот между указан-

ными участниками и правоохранительными органами развит слабо. Обмен документами (запрос – ответ) осуществляется по старинке, с использованием бумажных технологий. В свою очередь определенную сложность закладывает бюрократическая волокита, отсутствие единых шаблонов (бланков) для оформления запросов, продолжительность подготовки ответа со стороны коммерческих организаций (в течение 10–30 дней) [2; 3].

Как уже было отмечено, высокий уровень количества преступлений, совершенных с применением кибертехнологий, не требует доказательств. Каждое четвертое преступление от общего числа относится к данной категории [4]. Изучение документооборота территориальных ОВД на районном уровне одного из региона показало, что от 5 до 10 % подготовленных документов за месяц являются запросами органов следствия и дознания, оперативных подразделений в финансово-кредитные учреждения, операторам связи и IT-компаниям. На сегодняшний день в ряде регионов подписаны соглашения с ПАО «МегаФон», ООО «Скартел» (Yota), ООО «Т2 Мобайл» (Теле-2), ПАО «СберБанк», ООО «Яндекс» и др. Варианты организации электронного взаимодействия, реализованные с указанными компаниями, весьма различны как по схеме взаимодействия, так и по используемым ресурсам (закупка дополнительного программного обеспечения, организация доступа с рабочих мест, подключенных к сети Интернет). Отсутствие единообразия в организации электронного документооборота с коммерческими организациями создает препятствие на масштабное использование возможности оперативного получения информации.

Становится очевидным, что объем предполагаемой работы колоссальный, продолжать ее, используя бумажную технологию документооборота крайне затратно в финансовом плане и расточительно по времени. Уверен, что использование СЭД ИСОД МВД России в качестве платформы электронного документооборота либо создание отдельного сервиса по обработке запросов в ИСОД МВД России позволит решить проблему обмена корреспонденцией со всеми заинтересованными организациями и подразделениями. Допускаю, что основным препятствием для распространения СЭД является защищенность ведомственной сети, которая в случае ее

распространения будет значительно снижена. В этом случае предлагается использовать отечественные программные решения с возможностью обмена документами в зашифрованном виде по открытым каналам сети Интернет, где в обязательном порядке должна быть реализована возможность подписания документов усиленной квалифицированной электронной подписью [5]. Использование ИСОД МВД России как платформы по обмену электронными документами с коммерческими структурами, позволит сотрудникам ОВД получать необходимые сведения в режиме «единого окна» без дополнительных затрат на программное обеспечение, оснащение дополнительных рабочих мест, оплату доступа к сети Интернет и почтовых пересылок. Примечательно, что в аналогичном выигрыше будут и коммерческие организации, интерес в электронном взаимодействии с правоохранительными органами которых будет возрастать.

Литература

1. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений: приказ МВД России от 03.04.2018 № 196. Доступ из справ. правовой системы «Консультант Плюс».

2. Об оперативно-розыскной деятельности: федер.закон от 12.08.1995 № 144-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

3. О порядке рассмотрения обращений граждан Российской Федерации: федер. закон от 02.05.2006 № 59-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

4. Краткая характеристика состояния преступности в Российской Федерации за январь-февраль 2022 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/29152810 (дата обращения: 10.04.2022).

5. Сервис электронного документооборота «Такском-Файлер» [Электронный ресурс]. URL: https://taxcom.ru/dokumentooborot/fajler (дата обращения: 10.04.2022).

А.А. Калашникова,
Д.В. Евсеев

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Впервые понятие «искусственный интеллект» (далее – ИИ), которое так широко применимо сегодня, было использовано на Дартмутской конференции в 1956 г. Предпосылками для создания концепции ИИ стали научные труды о построении математической модели искусственного нейрона и нейронной сети на базе наблюдения за естественными нейронами и живыми организмами. Американские ученые-нейрофизиологи Уоррен Мак-Каллок и Вальтер Питтс в своих трудах «Логическое исчисление идей, относящихся к нервной активности» уже в 1943 г. выдвинули теорию, что сеть, состоящая из искусственных нейронов, подобных естественным, может выполнять логические и математические операции [4]. В 1948 г. выдающийся британский ученый Алан Тьюринг опубликовал статью «Интеллектуальные машины» (англ. Intelligent Machinery), а в 1950 г. – работу «Вычислительные машины и интеллект» (англ. Computing Machinery and Intelligence), в которых рассматриваются вопросы развития машинного обучения и искусственного интеллекта. Этим было положено начало процесса «оцифровывания» организма и представления живого существа как упорядоченного набора действий, которые можно воспроизвести и проанализировать.

Рассмотрим современные определения для терминов, связанных с искусственным интеллектом:

1) искусственный интеллект (ИИ) предполагает выполнение задач принятия решений и обучения информационными системами по аналогии с интеллектом живых существ;

2) нейронная сеть – взаимосвязанный набор искусственных нейронов, выполняющих простые логические операции с возможностями машинного обучения;

3) машинное обучение (МО) – это использование математических моделей данных, которые помогают компьютеру учиться без прямых инструкций. МО является одной из форм ИИ. Главная задача машинного обучения – построить порядок действий на основе первоначальных данных и предоставленных правильных или ожидаемых результатов – таким образом, весь процесс МО делится на начальное обучение на предоставленных наборах данных и последующих принятий решений уже обученной системы.

Рассмотрим известные способы машинного обучения:

– обучение с учителем – это метод машинного обучения, который использует помеченные наборы данных (классифицированные объекты с выбранными характеристиками), для которых определенный «учитель» (человек или обучающая выборка) задает правильные пары вопрос-ответ, на основе которых необходимо построить алгоритм предоставления ответов на другие подобные вопросы;

– обучение без учителя – это метод машинного обучения, который не использует размеченные наборы данных, не задает правильные пары вопрос-ответ, а информационная система должна находить разные отношения между ними в зависимости от известных свойств объектов;

– обучение с частичным привлечением учителя – метод машинного обучения, который объединяет небольшое количество секционированных наборов данных и большое количество не секционированных наборов данных. Такой подход оправдан тем фактом, что получение высококачественных отмеченных дат является довольно длительным и ресурсоемким процессом.

В настоящее время на практике, как результат машинного обучения, применяются следующие системы и программы:

1. UEBA (User and Entity Behavior Analytics) – с помощью данной системы правоохранители обнаруживают случаи нестандартного поведения пользователей путем анализа их действий в сети. Это позволяет детектировать внутренние и внешние угрозы, применяя шаблоны (паттерны) угроз.

2. Василиск AI [2] – данная программа разработана курсантами Московского университета МВД России им. В. Я. Кикотя, она позволяет

анализировать открытые торговые онлайн площадки в целях поиска похищенного антиквариата.

3. Антифрод (Antifraud) – платформы, которые предотвращают мошеннические транзакции, выявляя отклонения от бизнес-процессов. Компания Avito использует антифрод для выявления мошенников, использующих поддельные схемы платежных ссылок для обмана клиентов.

Несмотря на использование данных решений, уровень информационной преступности увеличивается с каждым годом. Согласно данным МВД РФ, каждое четвертое преступление совершается с использованием IT-технологий. Регионы с наибольшим и наименьшим удельным весом преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации относительно всех видов преступлений за первый квартал 2022 г. выделены на рис. 1 [3].

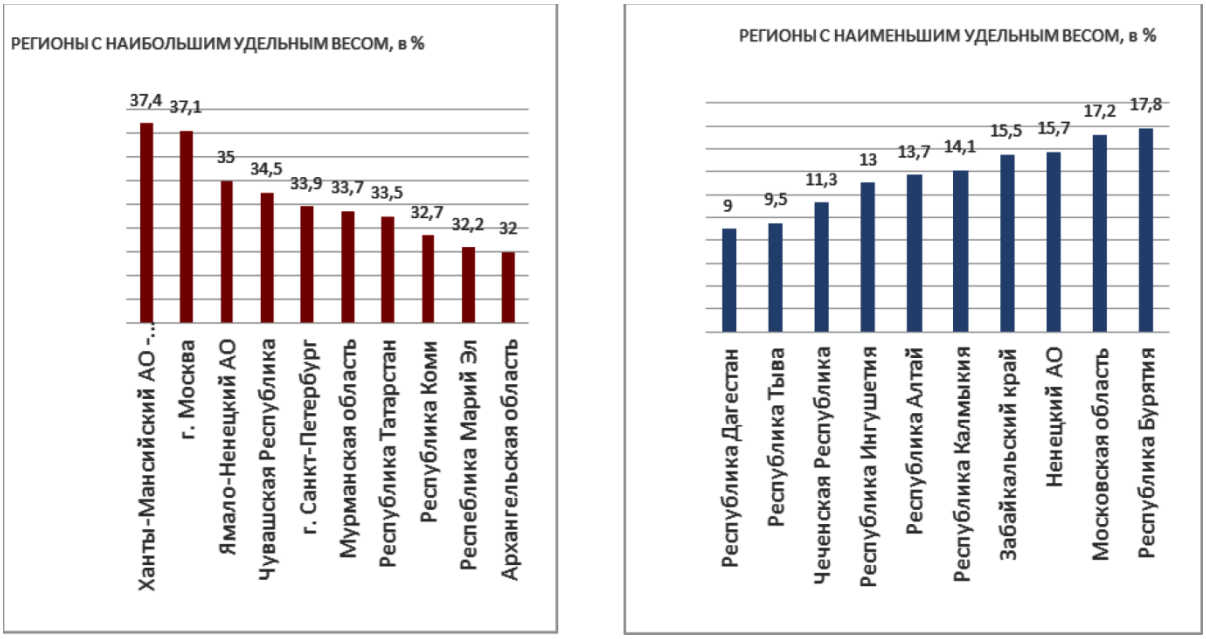

Рис. 1. Количество преступлений с использованием IT-технологий

С развитием киберпреступности развиваются и меры противодействия им. В ближайшем будущем готовятся реализовать такой проект, как система распознавания преступников и подозреваемых с помощью платформы, которая распознает по голосу преступника. Это позволит решить проблему телефонного мошенничества.

Также необходимо выделить дискуссионные проблемы развития ИИ в системе правоохранительных органов:

1. Последствия внедрения ИИ в сочетании с другими технологиями новой промышленной революции для изменения численности полиции. Предполагается, что это значительно сократит количество сотрудников полиции, как это имеет место, например, в банковских структурах. Однако прямые аналогии здесь невозможны. Действительно, использование искусственного интеллекта в технологии камер видеонаблюдения, бесспорно, позволит повысить объем поступающей информации о правонарушениях, которые должны иметь уголовно-процессуальную оценку. В свою очередь это потребует расширения кадровой численности сотрудников. На данный момент необходимо подготовить как можно больше высококвалифицированных специалистов в сфере аналитики больших баз данных. Именно поэтому внедрение ИИ запросит расширения численности полиции.

2. Этические рекомендации по использованию искусственного интеллекта в полиции и судебных органах включают в себя несколько аспектов. В различных нормативных правовых актах о применении технологии ИИ в деятельности органов исполнительной власти такие рекомендации и ограничения схожи как для полиции, так и для судей. Однако и среди них есть серьезные противопоставления. Одним из ярких примеров является принцип прозрачности баз данных к полиции и судам. И если условие прозрачности в отношении судебных баз не вызывают сомнений, то среди информационных баз для сотрудников полиции имеются серьезные ограничения, в отношении сведений разведывательной оперативно-розыскной деятельности. Это связанно с секретностью данных, а также негативными последствиями как для информаторов, так и для участников судопроизводства.

3. Применение ИИ для сбора информации о гражданах. Для осуществления этого необходимо соглашение между ОВД и обществом. Особенно это нужно в сфере предупреждения и раскрытия терроризма, коррупции и других преступлений. Поэтому подлежит использовать данную информацию для выявления преступности на основе алгоритмов и закономерностей криминологии. Между тем, не стоит забывать, что системы

на базе ИИ могут использовать и киберпреступники. Так известны мошеннические методы применения Deep fake (создание виртуального образа человека, схожий с реалистичным) для обезвреживания антифрод-систем, фейковые голоса для мошеннических звонков родственникам людей, атакованных с запросами на перевод денег, использование телефонных технологий IVR для фишинга и отвода средств известны. Вредоносная программа также использует элементы ИИ, которые позволяют злоумышленникам намного быстрее повышать свои привилегии, просматривать корпоративную сеть, находить и красть интересующие данные. Поэтому технологии, ставшие доступными широкой публике, используются как во благо, так и во зло, а значит, бороться с такими подготовленными киберпреступниками нужно, используя самые современные средства и методы защиты.

Литература

1. Искусственный интеллект в информационной безопасности [Электронный ресурс]. URL: https://www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti/ (дата обращения: 05.04.2022).
2. Искусственный интеллект на службе полиции: сб. статей Междунар. научно-практ. конф. М., 2021.
3. Краткая характеристика состояния преступности в Российской Федерации за январь-февраль 2022 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/29152810/ (дата обращения: 03.04.2022).
4. Мак-Каллок У.С., Питтс В. Логическое исчисление идей, относящихся к нервной активности / под ред. К.Э. Шеннонаи Дж. Маккартни. М., 1956.
5. Скрыпников А.В., Денисенко В.В., Хитров Е.Г. и др. Решение задач информационной безопасности с использованием искусственного интеллекта // Современные наукоемкие технологии. 2021. № 6–2.
6. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

Т.З. Хацуков

АВТОМАТИЗИРОВАННАЯ ДАКТИЛОСКОПИЧЕСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА «ПАПИЛОН»

С 2010 г. МВД России реализует Программу по внедрению АДИС, суть которой заключается в повсеместном применении автоматизированных систем подразделениями органов внутренних дел с использованием дактилоскопических учетов. Программа проводится на федеральном, межрегиональном, региональном и местном уровнях. Статистика по раскрытию преступлений в последние годы показывает о положительном применении АДИС, т. е. увеличиваются количество раскрытых общественно опасных деяний с использованием автоматизированных систем.

Но технологии не стоят на месте. Существует ряд проблем, при устранении которых применение автоматизированных систем приведет к еще большему увеличению результатов работы правоохранительных органов и органов внутренних дел в частности.

Система дактилоскопической регистрации в Российской Федерации имеет сложную и многоуровневую структуру. Связанно это с тем, что получение дактилоскопической информации охватывает различные сферы деятельности правоохранительных органов страны. В первую очередь, система дактилоскопической регистрации основывается на законодательной базе, которая позволяет легально и легитимно получать дактилоскопическую информацию от граждан, иностранных граждан и лиц без гражданства. Следующий аспект, отражающий состояние дактилоскопической регистрации, – это техническое состояние, к которому относится способы и методы получения информации, ее хранение, передача между правоохранительными органами страны, автоматизация всех процессов и многое другое [2].

Человек предоставляет свою дактилоскопическую информацию и, независимо от того было это сделано в добровольном или обязательном порядке, предоставленные им сведения регулируются нормами Федерального закона «О государственной дактилогической регистрации в

Российской Федерации» от 25.07.1998 № 128-ФЗ (далее – ФЗ № 128). Информационные технологии также требуют нормативного регулирования.

В сферу деятельности нормативного правого акта входят вопросы, касающиеся осуществления права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий, обеспечение защиты информации.

Для того чтобы полностью рассмотреть все аспекты дактилоскопической регистрации необходимо четко определить те понятия, с которыми оно сопряжено. Во-первых, необходимо рассмотреть понятие криминалистического учета. Между различными современными учеными до сих пор идут споры, о том какое именно понятие в данной отрасли является истинными. Сущность дактилоскопической регистрации определяет тот факт, что она предоставляет возможность быстро и точно получить интересующую информацию об обвиняемых и подозреваемых, отождествить личность, ответить на вопрос причастно ли лицо к общественно опасному деянию, в котором его обвиняют или подозревают. Анализируя все вышеуказанное, можно определить, что термин «государственной дактилоскопической регистрации» предложенный в ФЗ № 128 является полным и полностью раскрывающим деятельность правоохранительных органов по ведению дактилоскопических учетов. Данный термин не нуждается в доработках и исправлениях, т. к. раскрывает всю сущность исследуемого явления в ходе данной работы. Итак, дактилоскопический учет является наравне с пофамильным основным [3].

Они позволяют правоохранительным органам иметь актуальную информацию о лицах, предоставивших дактилоскопическую информацию. Выше были рассмотрены все моменты предоставления различными лицами дактилоскопической информации, ее получение и способы хранения правоохранительными органами. Теперь необходимо рассмотреть, какие же органы власти имеют право на использование таковой информации, а также ее получение иностранными государствами. Законодателем в ст. 14 ФЗ № 128 четко определен перечень органов власти, которые имеют право на использование дактилоскопической информации. К таким относятся суды, органы прокуратуры, органы предварительного следствия и другие [5].

Правовая основа поведения дактилоскопической регистрации опирается на нормы Конституции РФ, рассматриваемого ФЗ № 128 о дактилоскопической регистрации и сопряженных с ним иных федеральных законов, а также подзаконных актов, касающихся деятельности отдельных органов государственной власти. Принципы, на которых основывается деятельность субъектов, осуществляющих сбор или использование дактилоскопической информации, можно разделить на основные и факультативные. К основным принципам необходимо отнести обще конституционные принципы, такие как соблюдение прав и свобод человека и гражданина, законность, гуманизм. К факультативным же будут относиться принципы конфиденциальности, сочетания добровольности и обязательности. Проведение государственной дактилоскопической регистрации не должно представлять опасность для здоровья человека, унижать его честь и достоинство.

Обязательная дактилоскопическая регистрация может проводиться в отношении лиц, прописанных в ст. 9, рассматриваемого ФЗ № 128. Также данный Федеральный закон регулирует вопросы добровольной дактилоскопической регистрации. В нем нет конкретного перечня субъектов, которые по тем или иным причинам может подвергнуться добровольной дактилоскопической регистрации. Но стоит отметить, что не каждый человек, находящийся на территории Российской Федерации, может пройти данный процесс. Для этого необходимы определенные условия. Например, желание иностранного гражданина получить патент на работу на территории России, временно проживать в стране или получить вид на жительство [1].

Весь процесс проведения дактилоскопии лица поэтапно описан и регламентирован в Приложении № 3 совместного Приказа правоохранительных органов.

Дактилокарта выступает переходным моментом при получении от лица его дактилоскопической информации и внесении этих сведений в информационный массив. Современные технологии позволяют напрямую передавать дактилоскопическую информацию от лица в информационные массивы и регистрировать ее там. Все это осуществляется с использованием средств вычислительной техники, автоматизированных дактилоскопических информационных систем [6].

В настоящее время ряд мобильных решений «Папилон» включает в себя: мобильные комплексы различной функциональности, построенные на базе дактилоскопических сканеров «Папилон» и серийно выпускаемого оборудования – интегрированные малогабаритные носимые устройства на базе портативных компьютеров и смартфонов – комплект эксперта-криминалиста для съемки и передачи изображений следов пальцев рук и ладоней в АДИС «Папилон» непосредственно с места преступления. Статистические данные применения данных систем показывает положительные результаты [4].

Вышеизложенное позволяет использовать АДИС «Папилон»:

1. При расследовании и пресечении преступных деяний используются базы отпечатков пальцев и базы данных дактилоскопических карт и следов.

2. Осуществление пограничного контроля, контроль за пребыванием и передвижением иностранных граждан и поиск лиц в международных списках разыскиваемых лиц на основе иммиграционного контроля и регистрационных баз данных иностранных граждан и лиц без гражданства.

3. Проверка подлинности биометрического файла с помощью базы данных регистрации биометрических данных.

4. Выявление жертв террористических актов, военных операций и стихийных бедствий. Выявление недееспособных граждан и граждан, которые не могут заявить о себе, с помощью баз данных добровольной и обязательной регистрации отпечатков пальцев.

5. При реализации контроля за распределением социальных пособий и материальной помощи, исходя из информации, находящейся в базе данных лиц, имеющих право на государственные социальные пособия.

6. При обеспечении безопасности на транспорте (проверка гражданства в аэропортах, вокзалах, реках и морских портах, метро) и т. д.

Современные цифровые технологии позволяют АДИС «Папилон» формировать большое количество высококачественной информации по отпечаткам пальцев, создавая различные уровни баз данных, используемых правоохранительными органами в своей деятельности.

АДИС «Папилон» – это комплексное решение для системы биометрической идентификации и повышения эффективности автоматической регистрации отпечатков пальцев.

Но осовремененные реалии, технологический прогресс и многие другие факторы, скорее всего, приведут к введению в Российской Федерации обязательно дактилоскопической регистрации всех лиц, находящихся на ее территории. Следующим явлением, которое обязательно приведет общество к обязательной дактилоскопической регистрации, выступает развитие биометрических систем сбора информации.

Перспективы развития дактилоскопической регистрации обуславливаются следующими причинами: технологическим прогрессом, который значительно упростит и укорит свою деятельность государственных органов по сбору, хранению, передаче, предоставлению и уничтожению дактилоскопической информации и значительно повлияет на введение всеобщей дактилоскопической регистрации; общественным мнением и деятельностью законодательных органов; формированием биометрических банков данных как внутри страны, так и за ее пределами.

Для достижения вышеуказанного, необходимо совершенствование автоматизированных дактилоскопических информационных систем, обеспечение всех подразделений органов внутренних дел, которые осуществляют сбор дактилоскопической информации, специальной техническими средствами (например, АДИС «Папилон»), приобретение и эксплуатация станций (стационарных, мобильных, ручных) бескраскового сканирования, обработки и использования дактилоскопических данных, своевременное обучение сотрудников правилами и алгоритмами пользования системой.

Литература

1. Дактилоскопия и дактилоскопическая экспертиза: учебник для студентов вузов, обучающихся по специальности «Судебная экспертиза» / Н.П. Майлис, К.В. Ярмак, В.В. Бушуев. М., 2017.

2. Криминалистическая техника: учебник для вузов / К.Е. Демин и др. М., 2019.

3. Крамская Е.А. О дактилоскопической регистрации // Полиция России. 2020. № 1.

4. Сафонов А.А. Современная автоматизированная дактилоскопическая идентификационная система органов внутренних дел Российской Федерации // Вестник экономической безопасности. 2021. № 3.

5. Хайрулова Э.Т., Шадрина Е.С. Современное состояние дактилоскопической регистрации // Ученые записки Казанского юридического института МВД России. 2019. № 2(8).

6. Эйхвальд Н.Л. Использование дактилоскопических карт, полученных посредством комплекса «Живой сканер» и Адис «Папилон», при производстве дактилоскопической экспертизы // Юридическая наука и правоохранительная практика. 2020. № 4(54).

Б.Д. Бабаева,
А.В. Рыжов

ВНЕДРЕНИЕ СОВРЕМЕННЫХ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОГРАММЫ ОБУЧЕНИЯ КУРСАНТОВ И СЛУШАТЕЛЕЙ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ

Цифровизация всех сфер жизнедеятельности общества требует от современного полицейского сконцентрированного внимания, немедленного реагирования и пресечения совершаемых преступлений или правонарушений.

Обоснованность и законность применения на практике сотрудником полиции знаний и умений, приобретенных в период прохождения обучения в образовательной организации МВД России, во многом зависит от качества и эффективности и полученной им информации.

Качество преподавания тех или иных дисциплин должно быть априори, а вот эффективность обучения и высокие результаты не всегда достигаются лишь при помощи традиционных методов и подходов преподавателей к самому образовательному процессу.

В этом случае необходимо наличие, как минимум, двух условий. Во-первых, насколько курсанты и слушатели усваивают входящий материал, а, во-вторых, насколько этот самый учебный материал восприимчив и понятен адресату.

Именно в целях улучшения организации педагогической деятельности и разнообразия методических подходов к обучению курсантов и слушателей учебных организаций МВД России стоит говорить о применении инновационных технологий в процессе образовательной деятельности.

Кроме того необходимо отметить, что в недавнее время толчком для масштабного перехода большинства образовательных учреждений страны к форматам дистанционного обучения и применения новых широкоформатных платформ и других электронных ресурсов в учебном процессе послужила коронавирусная инфекция COVID-19, результатом которой явилось дистанционное обучение и использование интернет-платформ в качестве баз для проведения занятий.

Сейчас уже многие поняли, что техническая альтернатива укоренившимся традиционным методам и способам обучения эффективна для успешного овладения образовательной программы курсантами и слушателями МВД России и намерены применять ее в дальнейшем обучении.

Говоря о применении современных образовательных технологий по дисциплинам, преподаваемым на кафедрах образовательных организаций системы МВД России, стоит отметить, что любые перемены несут с собой как положительные, так и негативные последствия.

Но, несмотря на список препятствующих негативных факторов, устранение которых станет возможным при наличии необходимых условий, наряду с ними уже есть много положительных примеров использования достижений современной научной техники в образовательном процессе при подготовке будущих сотрудников полиции.

По дисциплине «Огневая подготовка» применение интерактивных обучающих программ в ходе проведения практических занятий условно можно подразделять на три уровня:

– первоначальный (укрепление знаний теоретической базы об основах огневой подготовки, мерах безопасности при обращении с огнестрельным оружием, изучение строения отдельных видов оружия, его частей и механизмов);

– основной (обучение курсантов практическим приемам и навыкам владения оружием с использованием стрелковых тиров и иных технических средств);

– специальный (усовершенствование отрабатываемых упражнений). Каждый из этих этапов направлен на усовершенствование профессионально-пригодных качеств обучаемых [1].

В большинстве случаев проблемы с огневой подготовкой возникают в следствие недостаточного времени, уделяемого преподавателем во время занятия. Некоторые учебные группы настолько масштабны по количеству людей, что преподаватель физически не успевает уделить одинаковое количество времени для каждого курсанта.

Именно для таких случаев и рекомендуется применять интерактивный стрелковый тренажер «СКАТ» [2].

При использовании данного тренажера стрелку достаточно прикрепить к пистолету специальный датчик, который без постороннего вмешательства будет выявлять траектории движения пистолета относительно мишени. Датчик передает всю информацию на монитор компьютера в виде траектории перемещения точки прицеливания на фоне мишени. Сам момент выстрела отражается в виде пробоины.

Таким образом, преподавателю не нужно беспокоиться о том, что он не уделил достаточного внимания некоторым курсантам, а последние, в свою очередь, благодаря данному тренажеру могут извлекать свои ошибки при прицеливании и стрельбе и в дальнейшем их не допускать.

Положительной стороной таких тренировок является многократность повторений и абсолютная экономия оружейных боеприпасов.

Стоит отметить, что использование современных технологий в обучении и подготовке курсантов и слушателей возможно не только в ходе занятий по практическим дисциплинам, но и в теоретических.

В этом случае можно говорить о замене бумажных носителей информации на электронные ресурсы, применение интерактивных обучающих программ и создание виртуальных аудиторий со всеми необходимыми обучающими материалами, максимально развивающими у курсантов и слушателей способности к самостоятельному принятию решений, организации мгновенного взаимодействия с коллегами для обмена необходимой информацией, а также быстрому ориентированию в информационной среде.

Конечно, никто не утверждает, что деятельность полиции в скором времени будет осуществляться в виртуальном пространстве. Говоря о применении современных технологий при обучении курсантов и слушателей МВД России, речь идет об их более профессиональной подготовке к преступлениям нового времени, когда в эпоху цифровизации всех областей жизнедеятельности граждан преступные действия совершаются уже не традиционными способами.

Литература

1. Таков А.З., Курманова М.К. Применение современных технологий в обучении стрельбе из боевого оружия // Современные наукоемкие технологии. 2020. № 11–2

2. Архипов С.Н. Использование стрелкового тренажера «СКАТ» на занятиях по огневой подготовке с сотрудниками спецподразделений // Научно-методический электронный журнал «Концепт» [Электронный ресурс]. URL: http://e-koncept.ru/2014/55007.htm. (дата обращения: 24.05.2022).

А.Б. Малявина

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АУДИТА СОЦИАЛЬНЫХ СЕТЕЙ

Информационные технологии оказывают серьезное влияние на сферу правового регулирования коммуникации пользователей в сети Интернет. Пользователи активно используют мессенджеры, социальные сети, проходят регистрацию на различных сайтах, и при этом регулярно предоставляют свои персональные данные.

По данным на январь 2021 г. в России 99 млн пользователей социальных сетей, или 67,8 % населения. По сравнению с прошлым годом число пользователей увеличилось на 4,8 млн (+ 5,1 %).

В исследовании Hootsuite и We are Social говорится, что наиболее популярен в России YouTube (на него заходило 85,4 % пользователей Интернета в нашей стране). На втором месте находится ВКонтакте (78 %), следом идут WhatsApp (75,8 %), Instagram (61,2 %), Одноклассники (47,1%) и Viber (42,5 %). Facebook в России использует 38,9 % пользователей, TikTok – 30,3 %, Telegram – 24,4 % [1].

Учитывая тот факт, что большая часть целевой аудитории рассматриваемой социальной сети – российский сегмент Интернета, полученные данные по посещаемости являются очень высокими. По причине таких показателей активности в социальной сети можно сделать вывод о том, что наибольшая часть преступлений может совершаться именно здесь.

Согласно ч. 1 ст. 29 Конституции Российской Федерации «каждому гарантируется свобода мысли и слова». Многие пользователи Интернета ссылаются именно на данный нормативный правовой акт, не учитывая того, что в части второй данной статьи указываются темы, которые нельзя поднимать при общении «не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства» [2].

В административном и уголовном законодательстве Российской Федерации предусмотрены ответственности за невыполнение данного запрета (ст. 280 Уголовного кодекса Российской Федерации «Публичные призывы к осуществлению экстремистской деятельности», ст. 282 Уголовного кодекса Российской Федерации «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» и другие) [3].

Отслеживание действий пользователей в социальных сетях является сложной задачей для органов внутренних дел в силу отсутствия автоматизированных систем, способных обрабатывать большие потоки данных. Вручную проверять каждое сообщество в социальной сети, отслеживать сотни, а иногда тысячи комментариев – практически невыполнимая задача, которая требует длительного времени.

Под мониторингом социальных сетей понимается изучение всех действий пользователей в социальных сетях. Данный процесс анализа, как правило, относится к изучению выражения мнений пользователями в комментариях и на своих страницах.

Выполнять подобный мониторинг может либо человек с собственной страницы в социальной сети, либо должностное лицо со страницы компании.

Данную процедуру принято выполнять по нескольким основным форматам: определенным фразам, хештегам, упоминаниям.

В результате мониторинга пользователь, производящий анализ может получить большое количество необходимых для себя, либо компании сведений, которые можно будет реализовать в последующем процессе работы. Социальные сети записывают действия пользователей, это позволяет изучать интересы, социальные группы, поведение и местоположение пользователей. Многие социальные сети собирают большой объем информации, которую можно использовать, чтобы воссоздать личность пользователя [4].

В процессе мониторинга специалист, как правило, применяет специализированное программное обеспечение – парсеры.

Парсер – это программное обеспечение, скрипт, позволяющий находить определенные сигнатуры в требуемых блоках сайта. Данное ПО получает на вход объект, ключевые фразы и на выходе подготавливает отчет о проделанной работе, включающий в себя требуемые аналитику материалы (ссылки, файлы, текст, фото- и видеоматериалы. Для сервера, к которому поступают запросы, парсер представляется таким же пользователем, как и другие люди, осуществляющие действия на сайте [5].

Существует два основных метода проведения семантического анализа действий пользователей в социальных сетях: мониторинг социальных сетей вручную и мониторинг с использованием специального автоматического программного обеспечения.

Ручной мониторинг подразумевает под собой проведение самостоятельной выборки пользователем интересующей его информации и также процесс самостоятельного анализа полученных данных без использования дополнительного программного обеспечения. Пользуясь данным методом, аналитик находит интересующие его объекты анализа путем поиска через запросы поисковых систем (Яндекс, Google, Rambler и т. д.), поиска в группах, сообществах, чатах, перехода на страницы пользователей. В данном методе не используется поиск по словарю. Аналитик самостоятельно

отсеивает ненужную информацию. Поскольку не используется дополнительное программное обеспечение, то и сохраняет все данные в требуемом формате, строит все графики зависимостей специалист-аналитик вручную. Мониторинг социальных сетей вручную имеет свои неоспоримые плюсы. К их числу относится полноценная выборка нужной информации, исходя из целей, которые специалист себе ставит перед производством анализа. Следует понимать, что данный процесс является трудоемким и отнимет большое количество времени у специалиста. Особенно заметно это в случаях, когда необходимо проанализировать сообщества в социальных сетях, в которых под каждой записью имеется тысячи комментариев, половину из которых оставляют боты. Поэтому, в силу развития и укрепления в жизни человека роли социальных сетей, аналитики зачастую используют дополнительные программные продукты, которые позволяют на некоторую часть облегчить их работу.

Мониторинг социальных сетей с применением программного обеспечения заключается в том, что аналитик, использующий его, должен подать на вход первоначальные данные (URL, название группы, тип комментария, ключевые слова и фразы и т. д.). После этого программа-парсер автоматически соберет необходимую информацию со страницы и предоставит пользователю файл, из которого в дальнейшем специалист может удалить лишние данные. Например, если сотрудник органов внутренних дел ищет информацию со страницы сообщества по ключевому слову бомба, помимо интересующих его комментариев потенциально преступной направленности, программа может сохранить комментарии, в которых данное слово используется в ином контексте. Автоматическое выполнение работы программным обеспечением не исключает последующую обработку выходного массива данных аналитиком. Она лишь многократно упрощает процесс поиска, но не может заменить полноценного сотрудника. Мониторинг с использованием парсеров имеет свои плюсы:

1) программа выполняется, пока не будет достигнута цель работы (Не будут получены и отфильтрованы результаты по 100 000 записей со страницы сообщества, не будут получены комментарии, содержащие поисковые сигнатуры);

2) параметры (Программа выполняется по указанным заранее параметрам. Нет необходимости в постоянном прописывании одних и тех же команд);

3) проведение более глубокого изучения истории записей на странице (Вручную практически невозможно отследить активность пользователей в крупном сообществе за длительный промежуток времени, например, за год);

4) автоматическая подготовка файла результата работы программы (Отчет формирует сама программа и аналитик, как правило, не добавляет в нее дополнительные данные, а лишь удаляет лишнее).

Литература

1. Аудитория социальных сетей и мессенджеров в 2021 г. [Электронный ресурс]. URL: https://https://blog.skillfactory.ru/auditoriya-soczialnyh-setej-i-messendzherov-v-2021-godu (дата обращения: 28.02.2022).

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из справ. правовой системы «КонсультантПлюс».

3. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. Доступ из справ. правовой системы «Консультант Плюс».

4. Малявина В.О., Малявина А.Б. Расследование киберпреступлений: цифровые следы использования программ удаленного доступа на ПК // Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел: сб. материалов Всерос. научно-практ. конф. Ростов н/Д, 2021.

5. Парсинг: что это такое и как он создается [Электронный ресурс]. URL: https://fb.ru/article/261908/parsing-chto-eto-takoe-i-kak-on-sozdaetsya (дата обращения: 01.03.2022).

М.М. Агаев,
Ю.А. Куриленко

ВИДЫ ФИШИНГОВЫХ АТАК И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

Проблемы информационной безопасности в сети Интернет затрагивают все большие интересы обычных людей, частных компаний, бизнеса различного масштаба, государственных и правоохранительных органов. Современные достижения влияют и на развитие преступности в киберпространстве.

Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных [1, с. 48]. Киберпреступления чаще всего совершают хакеры, люди, имеющие знания в области компьютерной техники и программирования. Киберпреступники спокойно могут заработать несколько миллионов, лежа у себя дома на диване, имея лишь компьютер и достаточные знания. Киберпреступники работают в одиночку или же объединяются и создают организации.

Существует ряд причин, по которым найти киберпреступников очень сложно:

− слабая законодательная база, что регулирует вопросы киберпространства и относящихся к нему противозаконных посягательств;

− проблемы выявления киберпреступлений;

− проблемы сбора доказательств, а также процесса доказывания;

− недостаточно большой объем базы общей судебной, следственной практики по делам такой категории;

− не выработана общая программа предотвращения, а также борьбы с киберпреступлениями [5].

Выделяют несколько типов киберпреступлений:

− мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);

− кража финансовых данных или данных банковских карт;

− кража и продажа личных данных;

− кибершантаж (вымогательства денег для предотвращения утечки данных или кибератаки);

− противозаконные азартные игры;

− торговля запрещенных вещей в Интернете (наркотики, данные, оружия);

− снятие, распространение, хранение детской порнографии [2].

Фишинг также является одним из самых распространенных и одним из первых видов кибератак. Фишинг с английского переводится как рыболовля. Этот вид кибермошенничества, в котором преступник пытается получить личные данные карты, паспорта, социальных сетей.

Клоновый фишинг – создание киберпреступниками копии финансовых сайтов и загрузка их, например, в Google. Пользователь, который заходит на сайт, который полностью идентичен с оригиналом, вводит на сайте данные своего аккаунта для входа, эти данные приходят к злоумышленнику. Используя данные, преступник через оригинал сайта заходит в аккаунт жертвы и оттуда сразу переводит все денежные средства себе [4].

Телефонный фишинг – фишинговые атаки могут осуществляться через простые телефонные звонки. Мошенник звонит жертве от лица банка, полиции или налогового управления. После мошенник начинает запугивать жертву, что у него возникли какие-то проблемы и для их решения жертве нужно сказать данные своей карты. Испуганная жертва сообщает данные своей банковской карты, а мошенник сразу снимает чужие деньги и перечисляет их себе.

Наиболее популярной фишинговой атакой стал случай, произошедший в 2013 г., когда было похищено около 110 млн записей кредитных карт и личных данных.

Еще в 2017 г. была одна из мощных фишинговых кибератак на Google и Facebook, вынудившая бухгалтерские службы этих компаний перечислить в общей сложности более 100 млн долларов на заграничные банковские счета хакеров.

Заметить кибератаку не просто, но есть несколько советов и правил, которыми не стоит пренебрегать, чтобы не стать жертвой киберпреступника.

Следует обращать внимание на все, что может казаться странным, необычным и необыкновенным.

В сообщениях, которые присылают киберпреступники, всегда содержится заманивающий и выгодный текст, допустим то, что Вы выиграли лотерею, приз, машину и т. п.

Необходимо остерегаться тех лиц, которых Вы вообще не знаете, если даже они говорят, что сотрудники полиции или банка.

Киберпреступники всегда в своих сообщениях пытаются внушить страх читателю. Обычно текст сообщения содержит пугающие и тревожные слова, чтобы создать атмосферу неотложной ситуации, заставляющую сделать любые действия, требующиеся в электронном письме.

Следует всегда обращать внимание на ссылку сайта. Если ссылка сайта оказалась необычной и подозрительной, отличающейся от простых оригинальных ссылок, то не стоит переходить по ней или вводить свои данные. Переходить по ссылке нужно только в том случае, если имеется уверенность, что эта ссылка оригинальной страницы.

Открывать электронные письма от неизвестных пользователей не рекомендуется.

Обязательно нужно проверять цифровые сертификаты сайтов.

Если есть сомнения в том, что письмо пришло от киберпреступника, то следует набрать отрывок текста в поисковике интернета и выявить имеет ли этот текст или похожие тексты связь с фишингом.

Также важно иметь хорошие антивирусные программы, которые распознают фишинг [3].

Во избежание попадания в ловушку киберпреступников необходимо соблюдать максимальные меры предосторожности. В настоящее время безопасность личных данных, денежных средств находится в наших руках.

Литература

1. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24.
2. Шарыпова Т.Н., Борисенко Д.Е. Киберпреступность в реальной и виртуальной жизни // Colloquium-journal. 2020. № 5.
3. Антонова Т.С., Смирнов В.М. Фишинг как неизученное киберпреступление // StudNet. 2021. № 6.
4. Полное руководство по фишинговым атакам [Электронный ресурс]. URL: https://habr.com/ru/company/varonis/blog/544140/ (дата обращения: 05.04.2022).
5. Киберпреступления – проблема 21 века [Электронный ресурс]. URL: https://blog.studylie.ru/kiberprestuplenija-problema-21-veka/ (дата обращения: 05.04.2022).

Б.Б. Рахмонбердиев,
Ю.А. Куриленко

ПРОБЛЕМЫ УЯЗВИМОСТИ СИСТЕМЫ КЕШБЭК

С наступлением эпохи пластиковых карт в мире все чаще стали использовать безналичный расчет. В связи с высокой востребованностью применения карт, а также для привлечения клиентов оплатой безналичным платежом, стали использовать системы, которые начисляют проценты с транзакций. В начале 90-х гг. прошлого века в США стала распространяться система кешбэк (cashback, cashback – возврат наличных средств). Это и привлекло людей пользоваться безналичным расчетом. В конце 2000-х гг. система кешбэк уже была на рынке в России. Постепенно переходя от банков к сетям магазинов, возврат кешбэк средств стал рентабельным для банков. Для этой цели банки используют интерчейндж (с англ. interchange – взаимообмен) – комиссии, которые выплачивают банки один другому за осуществление безналичных расчетов. В интерчейндже принимают участие различные платежные системы банковских

карт, банки-эмитенты, банки-эквайеры. Схема выплат кешбэка выглядит следующим образом: если покупатель рассчитывается картой, используя сервис транзакции, за которую он также платит комиссию и стоимость которой уже заложена в стоимость товара. Продавец выплачивает собственному банку комиссию за безналичный перевод средств посредством платежных терминалов (эквайринг). Банк-эквайер, который осуществил данный перевод, в свою очередь, выплачивает долю банку, что выпустил карту (банку-эмитенту) [1]. А он уже делится комиссией с платежными системами за осуществление перевода. Таким образом, все без исключения члены цепочки приобретают определенную выгоду.

Выделяют следующие виды кешбэка:

– кешбэк по фиксированной ставке – процент начисляется на любые виды покупок и лимитируется 1–2 %.

– многоуровневая ставка кешбэка – размер процента зависит от суммы расходов в определенный период времени (месяц, год).

– кешбэк по типу трат – размер ставки кешбэка зависит от того, на что потрачены деньги (определенный товар или конкретный магазин, сеть). [1]

Если говорить о кешбэк при получении каких-либо банковских продуктов, то зачисление происходит на ту же карту, с которой прошла оплата. При более распространенном кешбэк-сервисе – возврате от производителей товаров и услуг – возврат денежных средств возможно оформить путем зачисления их на банковскую карту, привязанную к аккаунту, на телефонный номер, электронный кошелек.

Часто кешбэк покупатель может получить при предъявлении чека, либо считывая QR-код с этого чека. Стоит отметить, что большая часть кешбэк-начислений при распознавании QR-программного кода имеют определенный период, зависящий от срока действия QR-кода на чеке. В случае если приобретенный товар оплачивается банковской картой, то отсканировать QR-код в чеке можно не позднее 24 часов с момента оплаты. Если же купленный товар оплачивается наличными деньгами, то время считывания сокращается до 3 часов. После сканирования QR-кода при наличии в чеке товаров, участвующих в промоакциях (контроль чеков происходит в течение нескольких часов, однако в некоторых случаях может длиться до 5-ти дней),

покупателю поступает кешбэк или на банковскую карту, или на счет мобильного телефона, либо на счет электронного кошелька.

Существует несколько программ, которые считывают QR -коды с чеков и зачисляют проценты. Одна из них программа «Чекбэк». «Чекбэк» – приложение от разработчиков VK Pay, которое позволяет вернуть часть денежных средств, потраченных на различные продовольственные и непродовольственные товары. Воспользоваться возможностями данного приложения можно с личной страницы ВКонтакте [2].

В системе кешбэк есть уязвимые места, ведь данные программы позволяют зарабатывать не только непосредственному покупателю, но и любому человеку, к которому попал чек о покупке. К ним, в частности, относятся сотрудники мелких организаций, которые собирают чеки с покупок и начисляют кешбэки себе.

Так трое работников центров оказания технических услуг в Узбекистане зарегистрировали 15,9 тыс. чеков общей стоимостью 11 млрд сумов (около 78 571 428 руб.), принадлежащие 281 субъекту предпринимательства, которых они обслуживали по роду своей деятельности, а возвращенные денежные средства (кешбэк) присвоили себе [3].

Одним из методов противодействия данной мошеннической схеме предлагается привязывать возврат кешбэка по чеку на карту, с которой была совершена покупка. Также следует предусмотреть возможность при считывании QR-кода с чека открывать сайт магазина, личного кабинета покупателя для подтверждения личности смс-уведомлением или вводом пароля. И, конечно же, осуществляя покупки, не стоит забывать забирать оригинальный чек себе.

Литература

1. [Электронный ресурс]. https://quote.rbc.ru/news/article/61f7e3bb9a7947075a776106 (дата обращения: 05.04.2022).

2. [Электронный ресурс]. URL: https://lite-zarabotok.ru/zarabotok-na-skanirovanii-chekov-i-qr-kodov.html (дата обращения: 05.04.2022).

3. [Электронный ресурс]. URL: https://uz.sputniknews.ru/20220202/v-uzbekistane-annulirovan-keshbek-po-16-tys-chekov-v-chem-prichina-22502636.html (дата обращения: 05.04.2022).

А.Н. Прокопенко,
Ю.М. Гусев,
А.А. Страхов

ДОКАЗАТЕЛЬСТВА В ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Компьютерная информация как основа доказательственной информации при расследовании преступлений с использованием информационно-телекоммуникационных технологий (далее – ИТТ) может выступать или как предмет преступного посягательства, или в качестве средства совершения преступления. В первом случае информация в электронном виде может в процессе совершения преступления подвергаться различным незаконным воздействиям. Помимо предусмотренных уголовным законодательством уничтожения, копирования, блокирования и модификации, возможно также применение шифрования, перемещения, распространение вредоносного программного обеспечения, посредством которого осуществляются противоправные деяния. Во втором случае информация является основой для совершения таких преступлений, как вымогательство или мошенничество (например, ложные покупки на Авито, фишинг, кража денег со счетов банковских карт и т. д.).

Особенности выявления и фиксирования цифровых следов обусловлены такими свойствами компьютерной информации, как скорость обработки информации, специальные форматы данных, способность к пересылке по коммуникационным каналам связи и др. Соответственно, цифровые следы, в отличие от традиционных трасологических следов, представляют собой изменения не внешней среды, а изменения информации вне зависимости от места ее нахождения. Причем на электронном носителе могут быть как следы вмешательства преступника, так и специализированное программное обеспечение, использованное для совершения преступлений. А при совершении общеуголовных преступлений с использо-

ванием ИТТ электронные доказательства ничем не отличаются от бумажных, кроме того, что они находятся в электронном виде и не могут быть восприняты органами чувств человека без применения специальных устройств [1].

Для выявления электронных следов эксперты и специалисты применяют такое специализированное оборудование и программное обеспечение, как, например, комплекс «Мобильный криминалист», который позволяет найти и зафиксировать необходимую информацию, а также изъять ее в установленном порядке для дальнейшего использования в судебном процессе. Данный раздел криминалистики получил название судебная компьютерная экспертиза или форензика.

Электронные доказательства могут быть неотделимы от электронного носителя информации, и в этом случае они исследуются вместе с носителем. Если электронные доказательства отделимы от электронного носителя, то они могут быть скопированы на любой носитель, и исследованию подвергается только сама информация.

В соответствии с примечанием 1 к ст. 272 Уголовного кодекса РФ компьютерная информация представляет собой сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [2]. Статья 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [3], содержит похожее определение для электронного документа, который чаще всего является электронным доказательством, «документированная информация, представленная в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

К электронным носителям информации ранее относились только персональные компьютеры (их системные блоки или жесткие диски) и так называемые машинные носители информации (магнитные и оптические диски, USB-накопители, карты памяти, переносные жесткие диски). Однако в последние годы количество электронных носителей информации существенно возросло. Повсеместно используются ноутбуки, смартфоны,

планшеты, навигаторы, Smart-часы, телекоммуникационное оборудование, а также различные бытовые устройства, обладающие встроенными электронными носителями информации.

Ученые проводят классификацию электронных носителей информации, как электронных доказательств в преступлениях совершенных с использованием ИТТ, по нескольким основаниям [4; 5]. Во-первых, электронные носители можно подразделить на первичные и вторичные по отношению к расследуемому событию. Первичные электронные носители – это вещественные доказательства, связанные непосредственно с событием преступления. Например, записи, произведенные во время совершения преступления, при проведении оперативно-розыскных мероприятий. Или персональный компьютер хакера, с которого он совершил несанкционированный доступ. Вторичные электронные носители – это носители, которые содержат информацию, относящуюся к виду иные документы, и скопированную с первоначального носителя. При этом, в ходе доказывания преступных действий допускается использовать вторичные электронные носители информации, если возможно копирование информации, являющейся электронным доказательством, без потери качества и свойств. Например, если бухгалтерская база данных позволяет скопировать часть информации, которая доказывает совершение преступления, без потери ее доказательственных свойств, то возможно использование вторичных носителей информации. Если же бухгалтерское программное обеспечение этого не позволяет, то следователь будет вынужден осуществить изъятие сервера, который является первичным электронным носителем, со всем массивом данных. Во-вторых, по своим размерам и особенностям подключения электронные носители информации подразделяются на стационарные и переносные. Необходимо отметить, что подавляющее большинство электронных носителей информации имеет небольшой размер, что позволяет осуществить их изъятие. При этом не имеет никакого значения, приспособлены ли они конструктивно для внешней работы или их использование предусматривалось только внутри системного блока. К стационарным носителям относится в основном серверное оборудование, например, у компаний провайдеров оборудование может весить несколько сотен килограммов и его нельзя извлечь из сети без остановки ее работы.

В-третьих, по месту нахождения электронные носители подразделяются на локальные и сетевые. Причем сетевые могут находиться как в данной организации, так и в другом подразделении организации (удаленные), в том числе в другом городе. Кроме того, возможно использование облачной инфраструктуры, как собственной в организации, так и таких ресурсов, например, как Google-диск.

Проводимые коллегами исследования показывают, что большинство следователей постоянно сталкивается с электронными доказательствами. Так, опрос следователей органов предварительного следствия районного и регионального уровней, а также сотрудников аппаратов управления позволил установить, что использовали электронные доказательства в своей деятельности около 85 % опрошенных следователей, из них свыше 70 % отметили, что им приходилось часто получать такие доказательства. Примерно 15 % следователей и дознавателей МВД России не сталкивались с необходимостью получения электронных доказательств как на электронных носителях, так и из облачных хранилищ [6].

Получение электронных доказательств, в том числе на электронных носителях, осуществляется в ходе процессуальных действий, таких как обыск, выемка, осмотр места происшествия, личный обыск, истребование в порядке ч. 4 ст. 21 Уголовно-процессуального кодекса РФ [7]. А также предоставление носителей органом дознания с ответом на поручение и материалами оперативно-розыскной деятельности, удовлетворение ходатайства стороны защиты о приобщении электронных носителей к материалам уголовного дела. Преимущественным способом получения электронных носителей является их изъятие, дублирование же содержимого жесткого диска с помощью специализированного программного обеспечения, создающего образ диска, имеет эксклюзивный характер.

Необходимо отметить, что практически в половине случаев (46,6 %) следователи, изымая электронные носители, сталкиваются с существенными возражениями их владельцев. Это обусловлено тем, что на носителях или находится информация, необходимая для дальнейшей работы организации. Или сам носитель является критически важным для продолжения работы, например, в случае изъятия сервера в оптово-торговой организации. В соответствии со ст. 164.1 УПК РФ следователь должен предос-

тавить владельцу электронного носителя информации возможность скопировать данную информацию. Но в большинстве случаев (78 %) в удовлетворении подобных ходатайств полностью или частично отказывается по причине отсутствия процессуальных нарушений в ходе производства следственного действия, вероятности использования информации вопреки интересам следствия, и иным предусмотренным законом основаниям.

В результате владельцы информации обжалуют действия следователей по изъятию электронных носителей почти в трети случаев (30 %). Наиболее часто встречающимися основаниями для обжалования являлись непредоставление возможности для копирования информации, а также изъятие носителей информации самим следователем, без участия специалиста или эксперта. Реальными причинами обжалования было то, что на носителях информации содержалась конфиденциальная информация юридических лиц (37,3 %) или граждан (62,7 %). Для юридических лиц речь шла о коммерческой, служебной, налоговой или банковской тайне, которая была необходима для дальнейшей деятельности организации. В случае изъятия носителей у физических лиц на носителях хранилась информация, которая охранялась авторским правом, тайна частной жизни, врачебная тайна, адвокатская тайна и другие виды конфиденциальной информации. Основной претензией являлось неправомерное изъятие охраняемой законом информации без согласия правообладателя и ее применение для доказывания совершенных преступлений [6].

Обобщение следственной практики получения электронных доказательств, как на электронных носителях, так и посредством получения информации из облачных хранилищ, в процессе доказывания позволило выявить следующие проблемные моменты, возникающие в процессе расследования:

– нехватка экспертов (специалистов), участие которых обязательно при изъятии электронных носителей;

– длительность проведения компьютерных экспертиз, назначенных в экспертных учреждениях системы МВД России;

– высокая стоимость (зачастую превышающая размер причиненного преступлением ущерба) проведения компьютерных экспертиз, назначенных в коммерческих организациях;

– отсутствие у специалистов экспертно-криминалистических центров программных и технических средств раскодирования и расшифрования полученных в ходе следственных действий электронных данных, хранящихся на изъятых носителях информации;

– отсутствие возможности эффективного обнаружения и изъятия информации, хранящейся на виртуальных серверах, размещенных, в том числе, и на территории других государств.

Кроме того, одной из проблем при расследовании уголовных дел по преступлениям, совершенным с использованием ИТТ, является установление места совершения преступления и совершившего его лица. Это усложняется тем, что для сокрытия преступлений используются сим-карты, зарегистрированные, как правило, на подставных лиц. Банковские карты, на которые поступают похищенные обманным путем денежные средства, также принадлежат третьим лицам, зачастую проживающим в других субъектах Российской Федерации.

При этом, частая смена мобильных телефонов, абонентских номеров и отсутствие возможности у операторов сотовой связи предоставлять сведения по другим субъектам РФ влечет за собой сложность получения сведений от мобильных операторов, которые необходимы для расследования преступлений. Это в свою очередь, затрудняет доказывание причастности конкретного лица к совершенному преступлению.

Наиболее часто встречаемой ошибкой при проведении следственных действий, в ходе которых происходит изъятие электронных носителей, является отсутствие в протоколах следственных действий указаний на конкретную марку используемых специалистом технических средств и описания проведенных им манипуляций [8]. Другими типичными упущениями при подготовке и проведении следственных действий, в ходе которых изымаются электронные носители информации, являются:

– отсутствие достоверной информации о точном местонахождении электронного оборудования, с которого может поступить команда для сокрытия или уничтожения интересующих следствие сведений;

– отсутствие достоверных сведений об организации локальной сети и размещении всех ее составляющих;

– отсутствие данных о степенях защиты информации, применяемых в организации или физическим лицом.

В целом можно констатировать, что электронные доказательства являются основой доказывания при расследовании преступлений, совершенных с использованием ИТТ. Практика следственной деятельности показывает, что при выявлении и фиксации электронных доказательств следователи предпочитают осуществлять изъятие этих доказательств вместе с первичными электронными носителями информации. Проведенная классификация электронных носителей показала, что подавляющее большинство устройств является переносными и без особых затруднений для сотрудников полиции может быть изъято.

Возможные проблемы возникают тогда, когда электронные доказательства находятся на удаленных или облачных носителях. В этих случаях требуется помощь экспертов или специалистов для правильной фиксации доказательств.

На наш взгляд изъятие электронных доказательств, как на электронных носителях, так и из серверных или облачных хранилищ, должно осуществляться с обязательным приглашением специалиста. Это обусловлено, с одной стороны, необходимостью грамотного изъятия информации, сохранения доказательной базы. А с другой стороны, участие специалиста на стадии изъятия, а не только на этапе экспертизы, позволило бы предотвратить все рассмотренные в статье проблемы с получением электронных доказательств, которые возникают у следователей и обусловлены преимущественно недостаточностью их технических знаний и навыков.

Литература

1. Гаврилин Ю.В. Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. 2013. № 25.

2. Уголовный кодекс Российской Федерации: федер закон от 13.06.1996 № 63-ФЗ (ред. от 09.03.2022). Доступ из справ. правовой системы «КонсультантПлюс».

3. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021). Доступ из справ. правовой системы «КонсультантПлюс».

4. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: дис. ... канд. юрид. наук. М., 2020.

5. Черкасов В.С. Правовое регулирование применения электронных средств в доказывании на досудебных стадиях уголовного процесса: дис. ... канд. юрид. наук. Хабаровск, 2021.

6. Доказывание по преступлениям, совершенным с использованием информационных технологий / И.С. Завьялова, А.И. Леонов, П.Г. Смагин. Воронеж, 2020.

7. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001 № 174-ФЗ. Доступ из справ. правовой системы «КонсультантПлюс».

8. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А. В. Аносов и др. М., 2019.

Н.П. Парфенов,
С.А. Алексеев,
Р.Е. Стахно,
А.Е. Мурашкин

МЕРЫ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЕМ – НА ПРИМЕРЕ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

В век компьютеризации, постоянного роста информационных технологий, совершенствования компьютерных систем, силовые структуры все чаще сталкиваются с проблемой квалификации и раскрытия преступлений, совершаемых с использованием информационных технологий, которые с каждым днем все больше и больше развиваются. Всем известно, что

преступность идет в ногу с развитием общества, постоянно создаются новые способы и орудия совершения преступлений, увеличивается список объектов преступных посягательств. В настоящий этап существования человечества правоохранительные органы, зачастую, имеют низкую раскрываемость так называемых «киберпреступлений». Само понятие «киберпреступность» дано в рекомендациях экспертов Организации Объединенных Наций, в которых говорится, что киберпреступность – любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети [1]. В данной работе будет использоваться вышеуказанное определение киберпреступности. В настоящее время, одним из самых распространенных видов преступлений, совершаемых с использованием информационных технологий, является телефонное мошенничество.

Схема первая.

Звонок с неизвестного или незнакомого Вам, номера. Звонящий человек по телефону, представляется близким родственником, хорошим знакомым или просто сослуживцем и, волнуясь, говорит Вам, что задержан сотрудниками правоохранительных органов и обвинен ими в совершении противоправных действий или преступления.

Далее в телефонные переговоры вступает второй участник, который представляется сотрудником правоохранительных органов. Второй участник говорит о том, что совершено противоправное действие или преступление и во избежание соответствующего наказания, необходимо перевести определенную сумму на расчетный счет. При этом он говорит уверенным голосом и очень убедительно.

В данной схеме обмана участвуют, несколько человек. Если же жертва поддалась обману, то мошенники уточняют детали: место встречи, время, номер расчетного счета и др. При этом, они не дают жертве опомниться, ведут назидательный разговор с целью запугивания и получения выкупа. После получения выкупа, сообщают место, где якобы находится ваш близкий родственник, хороший знакомый или просто сослуживец.

Что нужно делать в таких случаях? Успокоиться и прервать разговор. Далее перезвонить тому человеку, о ком идет речь. Если его телефон

не отвечает или отключен, постарайтесь связаться с родственниками, друзьями и коллегами для уточнения информации. Неплохо при разговоре с якобы сотрудником правоохранительных органов, выяснить, из какого он отдела, его фамилию, должность, звание. Потом перезвоните в дежурную часть вышеназванного отдела и уточните, действительно ли находится Ваш близкий родственник, хороший знакомый или просто сослуживец в данном отделе и проходит ли службу там собеседник по телефону.

Схема вторая.

Перевод Вам денежных средств по ошибке. На телефон приходит SMS-сообщение о поступлении денежных средств на счет, переведенных с помощью услуги «Мобильный перевод» или с терминала оплат. Спустя некоторое время после этого, поступает телефонный звонок или SMS о том, что на счет по ошибке переведены денежные средства, которые просят возвратить обратно той же услугой «Мобильный перевод» или осуществить перевод на правильный номер. Осуществляется перевод денежных средств, после чего происходит списание точно такой же суммы со счета. Мошенник, для списания денежных средств во второй раз со счета, использует чек, выданный при переводе денежных средств. Он обращается к оператору с заявлением об ошибочном внесении денежных средств и просьбой перевести их обратно на свой номер.

Таким образом, Вы в первый раз переводите денежные средства по его просьбе, а во второй раз он получает их по существующим и действующим правилам возврата средств.

Что же нужно делать в таких случаях? Предложите звонящему человеку возвратить денежные средства с помощью чека из терминала.

Если же в ответ получите сообщение об его утрате, то, скорее всего, имеете дело с мошенником, просьбы которого следует игнорировать.

Схема третья.

Сообщение-просьба о помощи. На номер мобильного телефона, якобы, от ближайшего родственника, приходит сообщение о необходимости срочного перевода конкретной суммы денежных средств на телефон, причину которого объяснят позже.

Что же нужно делать в таких случаях? Попытайтесь объяснить своим родственникам и близким, что на SMS такого содержания реагировать

не надо, для уточнения информации лучше пообщаться по телефону с якобы нуждающимся в переводе денег лицом.

Схема четвертая.

Телефонный номер-грабитель. Приходит сообщение с просьбой позвонить на конкретный номер мобильного телефона. В сообщении говорится о необходимости оказания срочной помощи близкому человеку, об изменении тарифов оказания услуг связи или о возникновении проблем с банковской картой. При этом, позвонив Вам, длительное время не отвечают, но держат на связи и не беседуют, а после отключения телефона со счета списывается крупная сумма денежных средств.

Что же нужно делать в таких случаях? Не реагируйте на сообщения такого рода и не звоните на незнакомые номера.

Теперь рассмотрим статистику преступлений данного рода за последнее время.

По данным Министерства внутренних дел за два месяца текущего года в Российской Федерации зарегистрировано на 29,4 % больше киберпреступлений, чем год назад, в том числе совершенных с использованием сети Интернет – на 48,3 % и при помощи средств мобильной связи – на 32,6 %.

Если в январе-феврале 2020 г. удельный вес преступлений в IT-сфере составлял 19,3 %, то за первые 2 месяца текущего года он увеличился до 26,3 % [2]. Жертвой телефонных мошенников может стать абсолютной любой гражданин Российской Федерации, и оградить его от этого могут только лишь знания в IT-сфере. Основным контингентом, который выбирают для своих противоправных деяний преступники, являются лица пожилого возраста. Лица пожилого возраста, в силу своего воспитания, отсутствия достаточных знаний в IT-сфере и доверчивости могут не заметить обмана и, чаще всего, не распознают его.

Одной из главных особенностей данного вида преступлений является анонимность преступников, зачастую при расследовании преступлений так и не удается установить личности правонарушителей. Новшеством в совершении телефонного мошенничества является схема, с помощью которой мошенники похищают деньги с банковских карт граждан путем отправления на их мобильные телефоны ложные сведения о том, что банковская карта гражданина Российской Федерации заблокирована.

Мы считаем, что одним из путей решения проблемы совершения преступлений с использованием информационных технологий является массовое информирование граждан, оказания отдельного внимания лицам пожилого возраста, а также малолетним лицам, которые в основном становятся жертвами данных правонарушений.

Таким образом, использование информационных технологий при совершении преступлений является достаточно актуальной проблемой, с которой сталкиваются силовые структуры [3]. Динамичность развития компьютерных технологий обязывают законодателя и правоохранительные органы реагировать быстрее и действеннее на новые формы совершения противоправных деяний с использованием компьютерных технологий.

Необходимо также предупреждать рассматриваемые преступления путем доступного и эффективного информирования населения, совершенствования законодательной базы, развитием передовых технологий в IT-сфере, непосредственно используемых при раскрытии и борьбе с киберпреступлениями.

Литература

1. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Государство и право. 2000. № 9.

2. Краткая характеристика состояния преступности в Российской Федерации за январь-февраль 2021 года // Официальный сайт Министерства внутренних дел Российской Федерации. Краткая характеристика состояния преступности в Российской Федерации за январь-февраль 2021 г. [Электронный ресурс]. URL: http:// xn--b1aew.xn--p1ai (дата обращения: 24.05.2022).

3. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие / А.В. Аносов и др. М., 2019.

СВЕДЕНИЯ ОБ АВТОРАХ

Агаев М.М. оглы – слушатель факультета подготовки иностранных специалистов Московского университета МВД России им. В.Я. Кикотя.

Акапьев В.Л. – доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина кандидат педагогических наук.

Бабаева Б.Д. – командир отделения 3 курса ОФО Ставропольского филиала Краснодарского университета МВД РФ.

Босенко Я.Е. – курсант факультета подготовки специалистов по программам высшего образования Ростовского юридического института МВД России.

Васильев В.А. – доцент кафедры трасологии и баллистики учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России кандидат химических наук.

Гусев Ю.М. – заместитель начальника кафедры огневой подготовки Белгородского юридического института МВД России им. И.Д. Путилина.

Дрога А.А. – заместитель начальника кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина.

Дубинина Н.М. – начальник кафедры информатики и математики Московского университета МВД России им. В.Я. Кикотя кандидат юридических наук, доцент.

Евсеев Д.В. – курсант факультета подготовки сотрудников полиции экономической безопасности и противодействия коррупции Московского университета МВД России им. В.Я. Кикотя

Евстропов Д.А. – старший преподаватель кафедры трасологии и баллистики Волгоградской академии МВД России кандидат технических наук.

Еремина Д.Д. – курсант факультета подготовки сотрудников полиции для подразделений по охране общественного порядка Московского университета МВД России им. В.Я. Кикотя

Ермакова Т. А. – доцент кафедры судебной экспертизы и физического материаловедения Волгоградского государственного университета кандидат химических наук.

Задохина Н.В. – доцент кафедры информатики и математики Московского университета МВД России им. В.Я. Кикотя кандидат педагогических наук.

Калашникова А.А. – преподаватель кафедры математики и информатики Московского университета МВД России им. В.Я. Кикотя.

Карпика А.Г. – доцент кафедры информационного обеспечения ОВД Ростовского юридического института МВД России кандидат технических наук, доцент.

Кашникова О.В. – курсант института-факультета подготовки сотрудников для органов предварительного расследования Московского университета МВД России им. В.Я. Кикотя.

Ковалева Е.Г. – доцент кафедры информационно-компьютерных технологий в деятельности ОВД, Белгородского юридического института МВД России им. И.Д. Путилина кандидат технических наук.

Корбаков В.В. – начальник курса факультета подготовки научных и научно-педагогических кадров Академии управления МВД России.

Краинский А.В. – преподаватель кафедры трасологии и баллистики УНК ЭКД Волгоградской академии МВД России.

Куриленко Ю.А. – заместитель начальника кафедры информатики и математики Московского университета МВД России им. В.Я. Кикотя кандидат юридических наук.

Макарова А.В. – курсант института-факультета подготовки сотрудников для органов предварительного расследования Московского университета МВД России им. В.Я. Кикотя.

Малявина А.Б. – научный сотрудник научно-исследовательского и редакционно-издательского отдела Ростовского института МВД России кандидат политических наук.

Медведев В.А. – преподаватель кафедры социально-экономических и гуманитарных дисциплин Ленинградского областного филиала Санкт-Петербургского университета МВД России

Молчанов А.О. – курсант факультета № 7 Ленинградского областного филиала Санкт-Петербургского университета МВД России.

Прокопенко А.Н. – профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина кандидат технических наук, доцент.

Рахмонбердиев Б.Б. угли – слушатель факультета подготовки иностранных специалистов Московского университета МВД России им. В.Я. Кикотя.

Рунаев Р.Ю. – доцент кафедры философии Волгоградской академии МВД России кандидат философских наук.

Рыжов А.В. – старший преподаватель кафедры тактико-специальной и огневой подготовки Ставропольского филиала Краснодарского университета МВД РФ кандидат педагогических наук.

Савотченко С.Е. – профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России им. И.Д. Путилина доктор физико-математических наук, доцент.

Слаутин О.В. – доцент кафедры материаловедения и композиционных материалов Волгоградского государственного технического университета кандидат технических наук, доцент.

Смирнов В.М. – старший преподаватель кафедры информатики и математики Московского университета МВД России им. В.Я. Кикотя кандидат технических наук.

Страхов А.А. – доцент кафедры информатики и математики Московского университета МВД России им. В.Я. Кикотя.

Фахертдинова Г.Р. – заместитель начальника отдела – начальник отделения УДиР МВД по Республике Татарстан.

Харитонова А.И. – курсант факультета подготовки сотрудников для подразделений экономической безопасности и противодействия коррупции Московского университета МВД России им. В.Я. Кикотя.

Хацуков Т.З. – курсант факультета подготовки специалистов по программам высшего образования Ростовского юридического института МВД России.

Худяков В.В. – доцент кафедры информатики и математики Московского университета МВД им. В.Я. Кикотя.

Черкасов Р.И. – старший преподаватель кафедры информатики и математики Московского университета МВД России им. В.Я. Кикотя кандидат технических наук.

Научное издание

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Сборник материалов
Всероссийской научно-теоретической конференции

(22 апреля 2022 г.)

Редактор *Н.А. Тапашева*
Корректор *Н.А. Тапашева*
Технический редактор *Н.А. Тапашева*
Компьютерная верстка – *Е.Е. Пелехатой*

Издатель: федеральное государственное казенное образовательное учреждение высшего образования
«Ростовский юридический институт
Министерства внутренних дел Российской Федерации».
Адрес: 344015, г. Ростов-на-Дону, ул. Еременко, 83.
Тел.: 8 (863) 224-58-15. Сайт: https://рюи.мвд.рф
Подписано к использованию 16.12.2022.
Тираж 10 экз.

ISBN 978-5-89288-477-8