УДК 378.095

ПРОБЛЕМЫ ПОДГОТОВКИ БУДУЩИХ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ К ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ, ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Кислицин И.А.[1], Батюшкин М.В.[1]

[1]*Федеральное государственное казенное образовательное учреждение высшего образования «Омская академия Министерства внутренних дел Российской Федерации», Омск, e-mail: ikisla@gmail.com*

В условиях стремительной цифровизации всех сфер жизнедеятельности современного общества неизбежно возникают инновационные формы совершения преступлений и правонарушений. Ежегодно правоохранительными органами регистрируется все большее количество преступных деяний, связанных с использованием информационно-телекоммуникационных технологий. Между тем результаты противодействия киберпреступности в настоящее время нельзя назвать удовлетворительными. Данная ситуация связана, в том числе, с наличием значительных проблем в системе подготовки сотрудников органов внутренних дел к эффективному осуществлению деятельности, направленной на выявление и раскрытие преступлений данного вида. Актуальность формирования профессиональной компетенции будущих сотрудников органов внутренних дел в области противодействия киберпреступности определяется социальным заказом на подготовку специалистов, способных оперативно решать профессиональные задачи с использованием современных программных и технических средств, а также находить нестандартные решения. В статье проанализированы статистические данные о результатах противодействия органов внутренних дел Российской Федерации преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, рассмотрены отечественные и зарубежные публикации в сфере подготовки специалистов по противодействию киберпреступности, приведены результаты интервьюирования действующих сотрудников и курсантов образовательных организаций МВД России. В результате проведенной работы сформулированы проблемы, имеющиеся в системе подготовки специалистов в сфере информационной безопасности. В качестве одного из возможных путей их решения рассмотрен опыт Омской академии МВД России по интеграции в образовательный процесс современных проблемно-ориентированных программных средств. Намечены перспективные направления совершенствования рабочих программ учебных дисциплин, непосредственно связанных с информационными технологиями и информационной безопасностью.

Ключевые слова: киберпреступления, подготовка сотрудников органов внутренних дел, противодействие киберпреступности, информатизация образования, специализированные проблемно-ориентированные программные средства.

ISSUES OF TEACHING FUTURE INTERNAL AFFAIRS EMPLOYEES TO COUNTERACT CYBERCRIMES, POSSIBLE SOLUTIONS OFFERED

Kislitsin I.A.[1], Batiushkin M.V.[1]

[1]*Federal State Public Institution of Higher Education «Omsk Academy of the Ministry of the Interior of the Russian Federation», Omsk, e-mail: ikisla@gmail.com*

Rash digitalization of all spheres in life activity of modern society leads inevitably to innovative forms of crimes occurrence. More and more crimes committed with the help of information and telecommunication technologies are registered annually by law enforcement. The results of anti-cybercrime strategies, however, currently cannot be called satisfactory. Among others, this situation is connected to existing significant issues in the system of preparing internal affairs employees for efficient activity aimed at detecting and investigating these types of crime. The urgency of professional competence formation in future internal affairs employees in the field of cybercrime counteraction is determined by social demand for educating specialists capable of performing promptly professional tasks with the help of modern program and technical tools, finding creative solutions. In this article statistical data on internal affairs bodies of Russian Federation cybercrime counteraction results is analyzed, foreign and domestic publications on educating specialists in cybercrime counteraction topics are reviewed, the results of interviewing with current internal affairs employees and cadets of educational organizations of the the Ministry of Internal Affairs of Russia are provided. As a result of work accomplished existing issues in the system of educating internal affairs employees in the field of information security are formulated. As one of possible solutions Omsk Academy of the Ministry of Internal Affairs of Russia experience in integrating modern problem-oriented software tools is considered. Promising enhancement strategy in work programs of disciplines related to informational technologies and information security has been mapped.

Keywords: cybercrimes, training of internal affairs employees, cybercrimes counteraction, informatization of education, specialized problem-oriented software.

Бурное развитие информационно-телекоммуникационных технологий (далее – ИТТ) в современном обществе не могло не отразиться на способах и методах совершения преступлений. Широкие возможности удаленно воздействовать на потерпевшего или осуществлять коммуникации с сообщниками, оставаясь при этом в условиях анонимности, привели к тому, что в настоящее время практически каждое преступное деяние может быть отнесено к категории киберпреступлений. В эту группу сегодня попадают совершенные дистанционным способом преступления против собственности, незаконный оборот наркотиков с использованием сети Интернет, проявления экстремизма и терроризма в социальных сетях и даже убийство или умышленное нанесение тяжких телесных повреждений, когда для организации данного деяния использовались современные информационные технологии.

Необходимо отметить, что в Уголовном кодексе РФ до сих пор нет четкого определения понятия «киберпреступление».

В статье под киберпреступлениями (или IT-преступлениями) предлагается понимать любые правонарушения, для совершения которых используются ИТТ, а не только классические преступные деяния, предусмотренные главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации».

Подобное определение киберпреступлениям дают профессор Anthony Reyes в своей монографии [1], К.Н. Евдокимов [**Ошибка! Источник ссылки не найден.**] и др.

Правильность именно такого толкования рассматриваемого понятия подтверждается подходом МВД РФ, которым в середине 2020 г. введен в действие статистический отчет, содержащий информацию более чем о 45 составах преступлений, совершаемых с использованием ИТТ.

В этих условиях в обществе возникает потребность в высококвалифицированных специалистах в сфере противодействия киберпреступлениям, однако уровень IT-компетенции выпускников вузов системы МВД России приходится признать недостаточным.

В настоящей статье автор ставит цель на основе анализа статистических материалов, изучения научных публикаций и результатов интервьюирования действующих сотрудников и курсантов образовательных организаций МВД России выявить проблемы в сфере подготовки специалистов по противодействию киберпреступлениям, а также предложить возможные пути их решения.

Материалы и методы исследования

Базой для эмпирического исследования выступило федеральное государственное казенное образовательное учреждение высшего образования «Омская академия Министерства внутренних дел Российской Федерации» (далее – Академия).

Материалом для исследования послужили статистические сведения, полученные из Главного информационно-аналитического центра МВД России. При их изучении использовались методы качественного и количественного анализа. Рассмотрение отечественных и зарубежных публикаций о киберпреступности и подготовке специалистов в области противодействия ей проводилось методами контент-анализа, сравнения и обобщения. Для сбора мнений действующих сотрудников ОВД и курсантов Омской академии МВД России использовались метод экспертных оценок, анкетный опрос и ранжирование. В интервьюировании приняли участие 60 курсантов 5-го курса факультета подготовки сотрудников полиции Академии, 12 действующих сотрудников ОВД Омской, Тюменской, Свердловской и Челябинской областей.

Результаты исследования и их обсуждение

Материалы главного информационно-аналитического центра МВД России показывают, что за последние 6 лет количество зарегистрированных преступлений, совершенных с использованием ИТТ, увеличилось более чем в 45 раз (рис. 1).

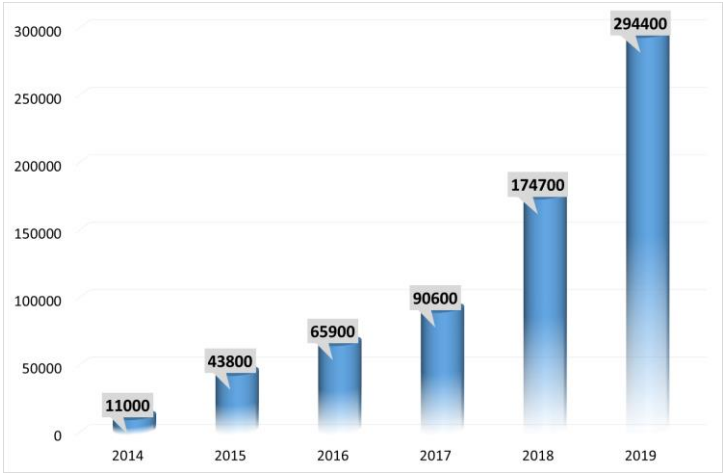

Рис. 1. Динамика числа преступлений, совершенных с использованием ИТТ, в 2014–2020 гг.

Анализируя структуру киберпреступности 2020 г., можно сделать вывод, что большинство криминальных деяний, совершенных с применением ИТТ, носят имущественный характер: 81,2% – кражи и мошенничества. Значительную долю – 12,0% – составляют преступления, связанные с наркотиками. Среди оставшихся 6,8% свыше 8 тыс. IT-преступлений связаны с экономической деятельностью, около 4 тыс. совершены в сфере

компьютерной информации, чуть менее чем по 2 тыс. составляют посягательства на свободу, честь и достоинство личности, а также распространение порнографических материалов.

Основным критерием эффективности противодействия преступности является отношение числа раскрытых преступлений к общему числу преступных деяний, по которым приняты процессуальные решения (или так называемая раскрываемость преступлений). Следует отметить, что данный показатель для IT-преступлений традиционно крайне низкий и в 2020 г. продолжил демонстрировать тенденцию к снижению, составив 20,1% (2019 г. – 24,0%) (рис. 2).

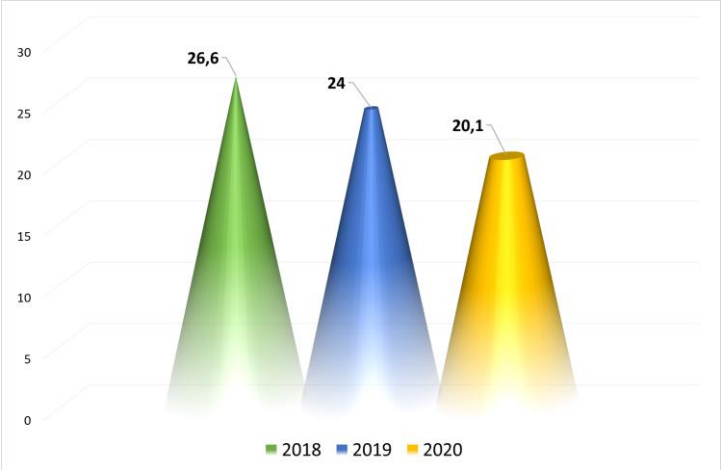

Рис. 2. Динамика раскрываемости IT-преступлений в 2018–2020 гг.

Иначе говоря, из почти 450 тыс. киберпреступлений, по которым приняты процессуальные решения, раскрыто и доведено до суда лишь каждое пятое. Это объясняется особенностями криминальной деятельности в данной сфере, в том числе: постоянным возникновением новых способов совершения противоправных деяний, связанным с активным развитием ИТТ, широкими возможностями обеспечения анонимности преступников, виктимным поведением потерпевших. Нельзя не отметить недостаточную компетентность действующих сотрудников органов внутренних дел в сфере информационных технологий.

Последнее подтверждается мнением научного сообщества. Такие авторы, как И.Н. Архипцев [3], О.Р. Идрисов [4], А.В. Царегородцев [5] и иные, указывают на недостаток квалифицированных специалистов, способных эффективно противодействовать IT-преступности, а также на ряд проблем, имеющихся в системе подготовки кадров, в том числе недостаточную оснащенность вузов современными стендами и оборудованием, стремительно устаревающие учебные материалы, раскрывающие в основном теоретическое вопросы, лишь расширяющие кругозор обучающихся.

Исходя из вышеизложенного можно выделить основную проблему, требующую углубленного исследования: каким образом обеспечить приобретение, развитие и

закрепление знаний, умений и навыков курсантов образовательных организаций МВД России, позволяющих им в перспективе максимально быстро включиться в профессиональную деятельность и эффективно осуществлять выявление и раскрытие киберпреступлений?

В качестве одного из возможных способов решения указанной проблемы и в конечном итоге повышения качества подготовки будущих сотрудников полиции предлагаем рассмотреть опыт Омской академии МВД России.

В рамках научно-исследовательской работы в 2019–2020 гг. на кафедре информационных технологий в деятельности органов внутренних Академии разработан программный комплекс «Эмулятор сервисов системы информационно-аналитического обеспечения деятельности МВД России» (далее – Эмулятор).

Единая система информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) представляет собой масштабный проект, функционирующий с 2015 г., одной из составляющих которого являются сервисы, содержащие информацию, необходимую для эффективной работы практически всех подразделений органов внутренних дел, в том числе направленной на пресечение и раскрытие преступлений в сфере IT-технологий.

Доступ к сервисам ИСОД МВД России строго ограничен, что обусловлено требованиями информационной безопасности и делает невозможным непосредственное изучение функционала на занятиях в образовательных организациях.

Разработанный Эмулятор полностью повторяет интерфейс реального портала ИСОД и дает возможность обрабатывать информацию, которая по структуре и составу аналогична хранимой в реальной системе, вместе с тем сгенерирована случайным образом и не раскрывает сведения о реальных лицах и других объектах [6].

Значительный объем информации в Эмуляторе (около 30 млн записей о лицах, адресах, транспорте, оружии, банковских счетах, телефонах, паспортах, правонарушениях и т.д.) позволяет преподавателю ставить учебные задачи любой сложности.

Задача может быть сформулирована в виде сообщения суточной оперативной сводки, в котором заложена аналогия реально происходившим событиям. Для выяснения всех обстоятельств обучающийся должен проанализировать первичную информацию и выбрать поисковые и аналитические средства для последовательного установления дополнительных сведений и связей, имеющих отношение к происшествию.

Разумеется, работа осуществляется не только в Эмуляторе, курсанты учатся применять иные программные продукты, в частности предназначенные для визуализации схем связей между объектами и событиями или построения социальных графов.

Конечно, интеграция в образовательный процесс новых специализированных проблемно-ориентированных программных продуктов невозможна без разработки определенных учебно-методических материалов.

В целях проверки эффективности применения ПК «Эмулятор ИСОД МВД России» в процессе обучения руководством Омской академии МВД России было принято решение о разработке новой учебной дисциплины «Профессиональные информационные системы в деятельности ОВД».

Вышеуказанная дисциплина ориентирована на приобретение курсантами и слушателями общепрофессиональной компетенции ОПК-13 «Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности», определенной новым ФГОС ВО по специальности 40.05.02 Правоохранительная деятельность [7, 8].

Кроме того, в процессе изучения дисциплины «Профессиональные информационные системы в деятельности ОВД» у курсантов формируются профессиональные компетенции, определенные квалификационными требованиями к специальной профессиональной подготовке выпускников федеральных государственных образовательных организаций, находящихся в ведении МВД РФ: способен использовать компьютерную технику, справочно-правовые информационные системы, учеты и автоматизированные информационно-поисковые системы при осуществлении служебной деятельности, в том числе с учетом требований информационной безопасности; способен решать задачи служебной деятельности по выявлению, предупреждению, пресечению и раскрытию преступлений и иных правонарушений, в том числе совершаемых с использованием ИТТ; способен осуществлять деятельность по формированию оперативных и иных учетов, использованию информационных ресурсов и технологий для решения задач оперативно-розыскной деятельности.

Вновь разработанная дисциплина «Профессиональные информационные системы в деятельности ОВД» была включена в учебный план для изучения в десятом семестре. Следовательно, освоение дисциплины слушателями 5-го курса предполагалось после прохождения полугодовой преддипломной практики.

По окончании изучения дисциплины проведено анонимное анкетирование, результаты которого показали, что большинство респондентов отмечают ее очевидную связь с практической деятельностью, около половины считают, что полезнее было бы изучать данную дисциплину до прохождения преддипломной практики.

Рабочая программа рассмотренной учебной дисциплины подвергается переработке с основой на результатах опроса, с учетом модификации в составе ПК «Эмулятор ИСОД МВД

России» и появления новых способов совершения IT-преступлений. В частности, освоение дисциплины запланировано на 4-м курсе до прохождения курсантами преддипломной практики. Перерабатываются планы практических и семинарских занятий.

Несомненно, раскрытие IT-преступлений с основой только лишь на применении профессиональных информационных систем, эксплуатируемых в органах внутренних дел, вряд ли будет эффективным. Поэтому профессорско-преподавательским составом кафедры Информационных технологий в деятельности органов внутренних дел Академии изучаются иные методы и средства (в том числе программные продукты), позволяющие пресекать инновационные преступные проявления. Каждый такой сервис или программа оцениваются с точки зрения возможности применения в образовательном процессе, так как часто для их использования требуется оформление специальных разрешений, которыми обладают только действующие оперативные сотрудники.

Заключение

В результате анализа подтвержден тезис о негативной динамике количества преступлений, совершенных с использованием ИТТ, отмечены неудовлетворительные результаты противодействия киберпреступности. Выявлены причины указанной ситуации, в том числе недостаточная компетентность в сфере информационных технологий действующих сотрудников органов внутренних дел, а также выпускников специализированных образовательных организаций.

Изучение опыта Омской академии МВД России показывает, что интеграция в процесс обучения учебной дисциплины «Профессиональные информационные технологии в деятельности ОВД», а также современных проблемно-ориентированных программных средств позволяет в некоторой степени сформировать у обучающихся необходимые профессиональные и общепрофессиональные компетенции.

Между тем, учитывая, что активное развитие информационных технологий влечет за собой изменение форм средств и методов осуществления преступной деятельности, необходимо подвергнуть глубокому анализу и переработке имеющиеся рабочие программы учебных дисциплин, непосредственно связанных с информационными технологиями и информационной безопасностью.

В рамках указанной работы следует, во-первых, с целью выявления концептуальных подходов к формированию знаний, умений и навыков, позволяющих выпускникам вузов МВД России эффективно осуществлять работу по раскрытию IT-преступлений, провести анализ научно-методической, психолого-педагогической и технической литературы; во-вторых, предложить перечень специализированных проблемно-ориентированных программных продуктов и аргументировать их применение в качестве инструментов для

изучения способов противодействия преступности в сфере ИТТ, а также разработать совокупность кейсов, которые необходимо решить с их использованием; в-третьих, подготовить комплекс для определения уровня сформированности индикаторов достижения требуемых компетенций у выпускников и в конечном итоге организовать и провести мероприятия по проверке эффективности применения разработанной методики.

Список литературы

1. Reyes A. Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors. Syngress Publishing, Inc. 2007. 434 p.
2. Евдокимов К.Н., Скляров С.В. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10. № 2. С. 322–330.
3. Архипцев И.Н., Сарычев А.В., Красников Р.В. Совершенствование подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий // Правовая парадигма. 2020. Т. 19.№ 2. С. 154-163.
4. Идрисов О.Р. Актуализация подготовки юридических кадров в условиях роста киберпреступности и необходимости борьбы с ней // Современное образование: качество образования и актуальные проблемы современной высшей школы: материалы международной научно-методической конференции, Томск, 31 января – 2019 года. Томск: Томский государственный университет систем управления и радиоэлектроники, 2019. С. 218-219.
5. Царегородцев А.В., Цацкина Е.П. Влияние информационного общества на подготовку обучающихся в сфере информационной безопасности // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2019. № 4(833). С. 191-199.
6. Дивольд В.Е., Гайдамакин А.А., Батюшкин М.В. Профессиональные информационные системы: проблемы и опыт практико-ориентированного обучения // Вестник экономической безопасности. 2020. № 1. С. 329-332.
7. Приказ Министерства науки и высшего образования Российской Федерации от 28 августа 2020 г. №1131 «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 40.05.02 Правоохранительная деятельность». [Электронный ресурс]. URL:

http://publication.pravo.gov.ru/Document/View/0001202009150044 (дата обращения: 28.10.2021).

8. Приказ Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1456 «О внесении изменений в федеральные государственные образовательные стандарты». [Электронный ресурс]. URL http://publication.pravo.gov.ru/Document/View/ 0001202105270015 (дата обращения: 28.10.2021).