Необходимо отметить, что сложность раскрытия преступлений в сфере компьютерной безопасности, в частности несанкционированного доступа к компьютерной информации обусловлена рядом причин:

быстрое старение компьютерных знаний и навыков (новые образцы компьютерной техники и программного обеспечения появляются настолько быстро, а число фирм-производителей так велико, что даже специалисту трудно уследить за нововведениями);

информационные процессы протекают с очень высокими скоростями, что отрицательно сказывается на сборе доказательств;

преступления в сфере компьютерной безопасности могут совершаться специалистами в этой области знаний, что обусловливает наличие определенного уровня противодействия;

несовершенство законодательной базы, регулирующей отношения в сфере оборота информации.

В этой связи в настоящее время правоохранительная практика стала нуждаться в разработке научно обоснованных рекомендаций по совершенствованию деятельности по выявлению и пресечению несанкционированного доступа к компьютерной информации.

Высокотехнологичный характер совершения преступлений против компьютерной безопасности значительно осложняет не только их раскрытие, но и квалификацию. Как в теории, так и в практике применения ст. 349 Уголовного кодекса Республики Беларусь существуют проблемные аспекты. При применении термина «компьютерная информация» допускается неверное его толкование, не соответствующее действительности представление о значении правовых последствий. Присутствует неоднозначность при определении места совершения преступлений данного вида.

Существует необходимость анализа практики противодействия несанкционированному доступу к компьютерной информации как в Республике Беларусь, так и за рубежом, в том числе государствах, являющихся стратегическими партнерами Республики Беларусь в области противодействия киберпреступности и правоохранительной сферах. Имеется также потребность в теоретическом обосновании и определении содержания оперативно-розыскной характеристики несанкционированного доступа к компьютерной информации. Не менее востребованным представляется исследование вопросов, касающихся способов и обстоятельств совершения несанкционированного доступа к компьютерной информации.

Развитие теории оперативной-розыскной деятельности детерминирует потребность обращения к проблеме проведения отдельных видов оперативно-розыскных мероприятий, не характерных для получения информации о лицах, совершивших несанкционированный доступ к компьютерной информации. В целях наиболее полного и всестороннего установления обстоятельств несанкционированного доступа, целесообразна систематизация возможных оперативно-розыскных ситуаций, их определения на первоначальном и последующем этапах раскрытия преступления.

Решение обозначенных проблемных аспектов представляется в разработке научно-практических рекомендаций по документированию несанкционированного доступа к компьютерной информации, предложений о направлениях совершенствования оперативно-розыскной деятельности и законодательства в данной области, а также необходимостью научной разработки отдельных аспектов выявления и фиксации преступной деятельности при несанкционированном доступе к компьютерной информации.

Таким образом, вопросы оперативно-розыскного противодействия несанкционированному доступу к компьютерной информации требуют в настоящее время комплексной научной проработки, в связи с наличием ряда проблем теоретического и прикладного характера.

УДК 343.985

О.Б. Шалагинова, Н.П. Мазанов

ИННОВАЦИОННЫЕ ПОДХОДЫ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Целью исследования являются обоснование и разработка подхода к повышению качества подготовки специалистов по направлению подготовки «Информационная безопасность», актуального на сегодня и основанного на повышении качества усвоения учебного материала дисциплин, предусмотренных учебным планом. Эта проблема требует решения в ближайшее время, так как речь идет о завтрашнем дне России и ее национальной безопасности.

Для достижения поставленной цели предлагается использовать инновационные методы обучения, основанные на использовании современных интерактивных образовательных технологий.

Исследование основано на анализе и использовании материалов исследований в области применения педагогических технологий в современном образовательном процессе, требований законодательства, которые являются обязательными при реализации основных образовательных программ высшего профессионального образования. При подготовке статьи также были использованы материалы, полученные ав-

торами в ходе планирования, подготовки, проведения и анализа лабораторных исследований со студентами, обучающимися по направлению подготовки «Информационная безопасность».

Специфика подготовки специалистов по направлению подготовки «Информационная безопасность», обусловленная высокими требованиями, предъявляемыми к ним работодателями, а также сложностью и необходимостью решения задач, стоящих перед Российской Федерацией, в области обеспечения информационной безопасности, заключается в необходимости получения знаний, наряду с фундаментальными знаниями в области информационной безопасности, современных и перспективных технологий защиты информации. Важную роль в повышении качества подготовки высококвалифицированных специалистов, профессионально востребованных и способных к саморазвитию, в настоящее время играет применение новых подходов к их подготовке, основанных на использовании инновационных методов. Предлагаемый подход заключается в разработке студентами современных и перспективных технологий защиты информации с использованием инновационных методов обучения при организации, подготовке и проведении учебных занятий. Одной из основных, наиболее важных в практических, исследовательских аспектах, форм проведения занятий в процессе подготовки специалистов по информационной безопасности является лабораторный семинар.

Предложенный подход апробирован в учебном процессе при планировании, подготовке и проведении лабораторных работ по теме «Создание виртуальной частной сети в виртуальной среде» по дисциплине «Технологии информационной безопасности». К основным особенностям данного урока можно отнести актуальность, высокую технологичность и практическую направленность темы урока, а также его интерактивность.

Результатом применения предложенного подхода стало повышение степени усвоения, широты охвата изучаемого материала и, как следствие, повышение эффективности формирования компетенций студентов, предусмотренных учебным планом.

Предложенный подход, заключающийся в применении инновационных интерактивных методов обучения при организации, подготовке и проведении обучения по актуальным, высокотехнологичным темам прикладной важности, был реализован на практике при изучении студентами дисциплины «Технологии информационной безопасности», что позволило повысить качество усвоения учебного материала дисциплины и в конечном итоге повысить качество подготовки специалистов по направлению подготовки «Информационная безопасность».

А. Тумаков рассказал о специфике подготовки специалистов в сфере кибербезопасности. Противодействие преступлениям в сфере информационных технологий, информационной безопасности подразумевает решение сразу нескольких задач. Об этом в интервью рассказал А. Тумаков, начальник кафедры гражданского и трудового права, гражданского процесса, кандидат юридических наук, доцент Московского университета МВД России имени В.Я. Кикотя. «Во-первых, это, безусловно, техническая составляющая, которой, собственно, и занимается факультет, вами обозначенный, и юридическая, безусловно, которой занимаются факультеты юридические», – отметил он. Образовательная программа факультета подготовки специалистов в области информационной безопасности, по его словам, предусматривает изучение технических дисциплин по специальности «Информационная безопасность автоматизированных систем». Она включает, в первую очередь, те учебные дисциплины, которые связаны с инженерно-техническими компетенциями, программно-аппаратными компетенциями, безусловно, отчасти организационно-правовыми компетенциями.

А. Тумаков поведал также о проводимых на факультете уникальных киберучениях. «Это комплекс учений, задачей которых является выработка компетенции технического характера и, безусловно, юридического, потому как в рамках проведения киберучений наши обучающиеся получают компетенции по проведению следственных действий, по подготовке процессуальных документов. Все это именно в рамках выявления и расследования преступлений, связанных с информационными технологиями, то есть непосредственно это различного рода хищения – пластиковых карт и так далее. Одновременно мы наших будущих выпускников готовим и с точки зрения технической, и, безусловно, с точки зрения юридической», – пояснил он.

Ученый также отметил, что факультет реализует дорожную карту по взаимодействию со стратегическими партнерами университета, которые являются специалистами в области кибербезопасности. «В частности, достаточно тесно мы взаимодействуем с Лабораторией Касперского. Специалисты лаборатории достаточно часто присутствуют на учебных занятиях, делятся опытом, помогают решать какие-то практические кейсы и так далее. Также мы взаимодействуем с ПАО «Сбербанк», кроме того, специалист Департамента обеспечения кибербезопасности активно присутствует на учебных занятиях. Это актуально не только для наших курсантов, но и для действующих сотрудников. Наши преподаватели совместно с привлекаемыми специалистами проводят повышение квалификации действующих сотрудников, следователей, оперативников и так далее», – рассказал А. Тумаков. И все это, по его словам, происходит непосредственно на том объекте, на котором

находится факультет подготовки специалистов в области информационной безопасности. «Подводя такой промежуточный итог работы факультета, я бы хотел отметить, что все-таки это решение по выработке технических компетенций практико-ориентированных и, безусловно, юридических. Поэтому данный факультет у нас является передовым и, безусловно, будет регулярно развиваться, регулярно совершенствовать образовательный процесс в рамках учебных дисциплин», – резюмировал он.

Кроме того, по мнению А. Тумакова, со временем цифровое право сформируется как отдельная отрасль. «Полагаю, что в настоящее время законодательство должно быть трансформировано. Причем трансформация должна происходить не только в области частного права, но и, безусловно, публичного права. Буквально вчера была поставлена задача Центральному банку и Министерству финансов предложить правовое регулирование цифровых финансовых активов. Думаю, что это достаточно позитивный пример, когда новые объекты, которые появляются в гражданском обороте, будут иметь соответствующее правовое регулирование. И, в целом, без выстраивания определенного категориального аппарата, в том числе в частном праве, нашим правоприменителям, судьям в том числе, достаточно сложно заниматься правоприменительной практикой, – добавил он. – Поэтому, полагаю, что законодательство в области как частного права, так и публичного права, должно трансформироваться в современных условиях и отвечать новым вызовам».

В результате исследования обоснован и разработан подход к повышению качества подготовки специалистов в области подготовки «Информационная безопасность».

УДК 343.98

И.О. Щербаков

ОСМОТР КОМПЬЮТЕРНЫХ УСТРОЙСТВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Несмотря на понижение темпа роста киберпреступлений, нельзя не отметить, что в целом все киберпреступления постоянно видоизменяются и совершенствуются, что снижает эффективность по их выявлению, раскрытию и расследованию. Развитие преступной среды предопределяет возможность обезличивания злоумышленников, а также совершение таких преступлений дистанционно, что позволяет скрыть

следы. В связи с этим растет уровень совершаемых рассматриваемых преступлений, поэтому деятельность правоохранительных органов во многом сейчас направлена на выявление, раскрытие и расследование преступлений, совершенных с использованием интернет-технологий.

Производство любого следственного действия, а особенно осмотра компьютерной техники, требует тщательной подготовки, обусловленной особенностями компьютерных средств. Осмотр электронных носителей информации возможно проводить в ходе осмотра места происшествия, либо как отдельное следственное действие [1].

На подготовительном этапе данного следственного действия следует:

проанализировать и систематизировать все сведения, имеющиеся в материалах уголовного дела, для определения вектора поиска криминалистически значимой информации;

привлечь специалиста, у которого есть необходимые компьютерно-технические средства;

разрешить вопрос об участии понятых, либо о применении технических средств, фиксирующих ход производства осмотра компьютерного устройства. Учитывая длительность и специфику производства данного следственного действия, целесообразным будет применение технических средств, что не противоречит ч. 1.1 ст. 170 Уголовно-процессуального кодекса Российской Федерации.

Для рабочего этапа характер осмотра методом «от общего к частному», т. е. сначала осматриваются внешние признаки устройства (цвет, марка, модель), а потом производится осмотр информации, содержащейся на электронном носителе. Неизменность, подлинность и сохранность источника информации обеспечивается следующим алгоритмом действий:

применять средства и программные обеспечения блокировки записи цифровой информации, копирования данных, позволяющих создавать копию, соответствующую оригиналу по содержанию и технологическим свойствам, позволяющие извлечь и проанализировать данные из устройств и облачных сервисов, такие как контакты, сообщения, звонки, геолокация, восстанавливают удаленные данные и др. [2];

не производить отключения уже запущенных программ и приложений, «авиарежима»;

не позволять самостоятельно совершать манипуляции с компьютерным устройством, если неизвестно, к какому результату это приведет;

детальный осмотр данных как на электронном устройстве, так и в «облачных» хранилищах;

удостоверение факта производства определенных действий, производимых с устройством, путем их фиксации письменно в протоколе,