В сфере информационной безопасности на данный момент ответ на вопрос, следует ли доверять искусственному интеллекту, а не человеческому анализу – часто «нет». В некоторой степени должен произойти сдвиг в том, каким образом мы оцениваем современные технологии и их возможности, прежде чем в полном объеме доверим принятие решения развитым технологиям искусственного интеллекта.

Следующие несколько лет будут интересны в контексте информационной безопасности. Огромные объемы данных, которые могут быть сгенерированы, наряду с проблемами проведения крупномасштабного анализа, для принятия оптимального решения, являются идеальным сочетанием для обширных и успешных архитектур обучаемых нейронных сетей.

УДК 343.3

Н.С. Сорокун, Р.А. Карапетян

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ПРИЧИН И УСЛОВИЙ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ОСНОВА ПРОФИЛАКТИКИ ТАКИХ ДЕЯНИЙ

В настоящее время наблюдается активное преобразование всех сфер жизнедеятельности граждан. Не остается без внимания и область информационных технологий, развитие которых стремительно возрастает. Становится невозможно уследить за всеми событиями в данной сфере. Создание современной техники, различных программ и приложений приводит к тому, что совершается множество преступлений в информационной среде. Данные обстоятельства ведут к неблагоприятным условиям в обществе. Уровень воспитания и нравственности становится низким, в результате чего падает и уровень развития людей. Современные технологии помогают не только развиваться и совершенствоваться, но и терять те качества, которые необходимы любому человеку для хорошей жизни.

Вопрос раскрытия и расследования преступлений, совершаемых с использованием компьютерных технологий, становится очень остро в последнее время. Прежде всего данный факт обусловлен необходимостью развития и совершенствования существующих методик расследования преступлений. Очевидно, что с развитием информационных технологий возникает необходимость в преобразовании стандартных ме-

тодик и средств. Однако внимание также стоит уделять и предупреждению преступлениям данного вида. В связи с чем видятся актуальными рассмотрение вопросов, связанных с причинами и условиями совершения компьютерных преступлений, а также изучение характеристики личности преступника и потерпевшего.

В настоящее время наблюдается повсеместное внедрение компьютерных технологий во все сферы жизнедеятельности общества. Основное внимание уделяется внедрению в производственные, экономико-финансовые и общественные отношения. Рассматриваемый процесс компьютеризации способствует развитию и совершенствованию жизни общества, а также приводят к появлению новых категорий преступных деяний. Такие преступления совершаются с использованием компьютерной информации и посредством компьютерных технологий.

По общему правилу данные преступления делятся на три категории: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для электронно-вычислительных машин (ЭВМ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Данные противоправные деяния находят свое отражение в нормах Особенной части Уголовного кодекса Российской Федерации.

Рассматриваемые группы преступлений представляют особый интерес, который прежде всего обусловлен характеристикой субъекта совершения компьютерных преступлений. Данный аспект объясняется тем, что обычный гражданин вряд ли способен совершить неправомерный доступ к компьютерной информации или создать вредоносную программу, не обладая специальными знаниями в области информационно-телекоммуникационных систем.

В 2020 г. наиболее распространены мошенничества в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70 % всех хищений, совершенных путем обмана или злоупотребления доверием (+73,4 %, 237,1 тыс.).

В 2021 г. мошенничество в сфере информационно-телекоммуникационных технологий составило 73 % всех хищений (249,2 тыс.), совершенных путем обмана или злоупотребления доверием. При этом существенно замедлились темпы их прироста (с 73,4 % в 2020 г. до 5,1 % в текущем).

За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 % до 25 %. Большинство «киберпреступлений» совершается с использованием сети Интернет (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.).

Кроме того, по своей природе компьютерные преступления носят латентный характер. Немаловажным элементом выступает также и харак-

тер совершения данных преступлений. Все преступные деяния, которые совершаются с помощью использования информационно-телекоммуникационных систем, всегда скрыты от обычных людей и выявление таких преступлений представляет собой особый процесс. Прежде всего для выявления и последующего раскрытия компьютерного преступления необходимо обладать специальными знаниями в области компьютерных технологий, так как доказательственная база будет формироваться в большей степени путем нестандартных методов.

В связи с указанным ранее фактором следует сказать о том, что профилактика в таком случае должна базироваться на уяснении причин и условий совершения преступления данного вида. На этом вопросе, полагаем, нужно остановиться более подробно.

Анализируя разные источники по данному вопросу, был сделан вывод, что причины совершения преступлений в сфере компьютерной информации можно подразделить на две основные категории. Первая категория характеризуется общими причинами преступности с использованием возможностей информационно-телекоммуникационной системы. В данную категорию могут входить причины различного уровня, которые присущи как компьютерным преступлениям, так и иным видам преступности.

Что касается второй категории, то она характеризуется специфическими причинами компьютерных преступлений. В частности, причины данной группы выражаются в формировании мотивации лица и решения совершить компьютерное преступление под влиянием изменений, связанных с появлением автоматизированных систем обработки информации. В рамках этой категории выделяют следующие причины компьютерной преступности:

уязвимость и зависимость компьютерных систем друг от друга;

несоответствие уровня развития юридических и политических структур уровню развития компьютерных и телекоммуникационных технологий;

динамичное развитие зависимости современных технологий от компьютерных систем;

отсутствие должного информирования граждан об уязвимости компьютерных систем;

существующие сегодня пробелы уголовного законодательства в части, касающейся регулирования общественных отношений в сфере компьютерной информации, а именно, отсутствие некоторых составов в уголовном законодательстве;

различия в законодательной базе с точки зрения соответствия отечественного и международного законодательства.

Однако, полагаем, необходимо отметить, что данные причины не могут рассматриваться в качестве непосредственных. В юридической

литературе отмечается, что основной причиной, подталкивающей лицо на совершение компьютерного преступления, будет являться детерминация преступного поведения.

Что касается условий совершения преступлений в сфере информационно-телекоммуникационных технологий, то стоит обратить внимание на следующие:

открытый доступ к автоматизированным информационным системам, с помощью которых могут совершаться финансовые операции различного характера;

отсутствие должного контроля за отдельными категориями сотрудников, что позволяет злоумышленникам использовать ЭВМ предприятий в качестве оружия преступления;

низкий уровень защиты компьютерных систем;

легкий доступ к данным ЭВМ, ввиду отсутствия надежной парольной системы;

отсутствие во многих организациях специально уполномоченного субъекта, отвечающего за сохранение конфиденциальности отдельных информационных данных;

отсутствие соглашений сотрудников о неразглашении данных, составляющих конфиденциальную информацию, в том числе пароли и иные ключи доступа к ЭВМ.

Необходимо отметить, что большинство условий создаются непосредственно потерпевшими лицами. Основной причиной является неосмотрительность лица. Помимо указанных условий могут отмечаться и иные. Нами были рассмотрены наиболее актуальные условия совершения информационных преступлений.

Рассмотрев причины и условия совершения преступлений в сфере компьютерной информации, вытекает вывод о том, что их круг достаточно обширен. На основании рассмотренных данных, считаем, стоит перейти к характеристике лиц, способных к совершению преступлений в сфере информационных технологий.

Анализируя практическую деятельность, можно сделать вывод о том, что субъектом совершения преступлений в сфере компьютерной информации в большинстве случаев выступает лицо мужского пола. Возрастная группа данных лиц, как правило, варьируется от 18 до 24 лет. Иными словами, совершают такое преступление лица студенческого возраста или же те, которые только завершили обучение в учреждении образования. Считаем, что именно в таком возрасте на человека можно оказывать некое воздействие, которое будет способствовать формированию у него устойчивого преступного поведения.

Полагаем, нужно акцентировать внимание на том, что огромная доля компьютерных преступлений носят латентный характер, соответст-

венно, не могут быть выявлены и проанализированы. В связи с этим возникает сложность в точном определении возрастных рамок субъекта совершения преступления, а также отдельных черт, характеризующих его.

Характеризуя личность компьютерного преступника, важно обратить внимание на психологические особенности данных лиц. В этом вопросе стоит рассмотреть отдельные качества личности, указывающие на поведение преступника.

Так, изучаемые лица, как правило, имеют замкнутый характер и не стремятся достичь высокого положения в обществе. В большинстве случаев они действуют индивидуально в связи с такой чертой характера, как скрытность. При общении отдельные лица этой категории конфликтны, не обладают особой эмоциональностью.

Указанные выше факторы свидетельствуют об одиночном характере осуществления деятельности данными субъектами. Однако специалистами в этой области отмечается, что они стремятся принадлежать к определенной социальной группе, откуда и вытекает создание хакерских сообществ.

Рассматривая категорию субъектов преступления в сфере компьютерной информации, можно сделать вывод о том, что указанные лица обладают высокой самооценкой. По нашему мнению, это связано с тем, что данная сфера деятельности, а именно информационно-телекоммуникационные технологии, требует высоких знаний для ее осуществления. В связи с чем лица, разбирающиеся в этой области, считают себя на ступень выше от обычных людей, так как обладают высокими знаниями в сфере компьютерных технологий. Указанные факторы позволяют говорить о спонтанном совершении преступлений без должной к тому подготовки.

Изучение поведения субъектов компьютерных преступлений свидетельствует о наличии таких признаков, как:

установление и поддержание социальных связей с иными лицами, совершающими преступления в сфере компьютерной информации;

обсуждение способов совершения преступлений в сфере информационно-телекоммуникационных технологий;

использование словесных оборотов, присущих лицам, разбирающимся в компьютерных технологиях.

В поведении рассматриваемой категории лиц могут выделяться и иные черты.

В рамках исследования данной темы была отмечена также проблематичность получения информации о типичных характеристиках личности компьютерного преступника. Это обстоятельство обусловлено высокой латентностью таких преступлений и отсутствием должного эмпирического материала, позволяющего изучать данную тему со всех сторон.

Таким образом, подводя итог настоящей статье, полагаем, следует отметить, что компьютерные преступления сегодня набирают особую популярность. В большинстве случаев преступления такого рода остаются незамеченными. Данное обстоятельство вытекает из-за отсутствия компетентных специалистов среди сотрудников органов внутренних дел, способных раскрывать и расследовать преступления в сфере информационно-телекоммуникационных технологий.

Одной из причин совершения этой категории преступлений выступает формирование преступного поведения у лиц. Такая причина рассматривается в качестве основной, поскольку именно преступное поведение может подталкивать лицо на совершение преступления.

При рассмотрении особенности личности субъекта преступлений в сфере компьютерных технологий главной характеристикой считается возраст лица, который был отмечен в диапазоне от 18 до 24 лет. Безусловно, данный диапазон не может рассматриваться в качестве основного и единственного, поскольку такие преступления совершаются лицами и в 16 лет, и в 35.

Специфические особенности личности преступника проявляются в его поведенческих чертах. Так, например, компьютерный преступник, как правило, обладает скрытным и замкнутым характером, малообщителен и обладает низким уровнем эмоциональности.

В заключение стоит отметить то, что криминологическая характеристика компьютерных преступлений будет оставаться актуальным вопросом, поскольку в настоящее время отсутствует достаточная эмпирическая база для изучения данной темы в полном объеме. Указанное обстоятельство вызвано тем, что большинство преступлений в сфере информационно-телекоммуникационных технологий носят латентный характер, ввиду чего не учитываются в общей статистике преступлений.

Список использованных источников

1. Аскольская, Н.Д. Специфика криминалистической характеристики киберпреступлений / Н.Д. Аскольская // Закон и право. – 2019. – № 8. – С. 89–92.

2. Ахмедханова, С.Т. Криминологическая характеристика преступлений в сфере информационных технологий / С.Т. Ахмедханова, Э.Х. Кахбулаева // Вестн. МГОУ. Серия «Юриспруденция». – 2018. – № 4. – С. 16–23.

3. Маслакова, Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика / Е.А. Маслакова // Среднерус. вестн. обществ. наук. – 2018. – № 1. – С. 31.

4. Поляков, В.В. Особенности личности компьютерных преступников / В.В. Поляков, Л.А. Попов // Изв. АлтГУ. – 2018. – № 6. – С. 104.

5. Ханов, Т.А. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений / Т.А. Ханов, А.Ж. Нуркеев // Изв. АлтГУ. – 2017. – № 6. – С. 98.

УДК 347.775

П.А. Тарасов

О ГРАЖДАНСКО-ПРАВОВОМ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационное пространство имеет особое значение в жизни современного человека. В Республике Беларусь идет активное развитие информационных технологий, информационная сфера становится системообразующим фактором жизни общества, оказывает активное влияние на состояние стабильности социальной, экономической и других сфер обеспечения национальной безопасности Республики Беларусь. Все большее значение приобретает информационная безопасность как составная часть общей системы обеспечения национальной безопасности Республики Беларусь.

В соответствии с Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» информацией являются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Данные сведения часто являются объектами необоснованного распространения, в связи с чем становится актуальным вопрос о защите информации с помощью комплекса организационных, технических и правовых мер, направленных на обеспечение ее конфиденциальности, сохранности, целостности, подлинности и доступности.

В настоящее время защита информации становится неотъемлемым атрибутом обеспечения безопасности граждан, общества и государства. В нашем государстве в целях консолидации усилий и повышения эффективности государственных органов, иных организаций и граждан по обеспечению национальной безопасности Республики Беларусь, защиты ее национальных интересов, а также обеспечения комплексного подхода к проблеме информационной безопасности приняты: Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» и постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь». В Республике Беларусь также действуют законодательные акты, регулирующие общественные отношения в сфере

информации, информатизации и защиты информации, коммерческой тайны и персональных данных. Принятые нормативные правовые акты составляют комплексную систему мер, направленную на защиту информации правовыми способами, включая гражданско-правовые.

Гражданское законодательство также призвано защищать интересы субъектов информационных отношений. В Гражданском кодексе Республики Беларусь (ГК) определено, что одним из объектов гражданских прав является нераскрытая информация, к которой относятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, составляющих коммерческую или служебную тайну. Защита указанной информации осуществляется предусмотренными законодательством Республики Беларусь способами.

В ГК предусмотрена ответственность за нарушение договорных обязательств одной из сторон, связанных с незаконным ознакомлением или использованием информации, составляющей коммерческую или служебную тайну. В соответствии со ст. 19 Закона Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» лицо, по вине которого произошло незаконное разглашение, ознакомление или использование сведений, составляющих коммерческую тайну обязано возместить убытки (в том числе упущенную выгоду), которые были причинены владельцу этой информации.

ГК устанавливает также ответственность за нарушение обязательств вследствие причинения вреда одним лицом другому в связи с непредоставлением необходимой информации о товаре, работе или услуге. Статья 965 ГК определяет, что возмещение вреда, причиненного вследствие непредоставления полной и достоверной информации о данных объектах, подлежит возмещению по выбору потерпевшего продавцом или изготовителем товара, исполнителем. В данный момент гражданское законодательство Республики Беларусь не относит саму информацию о товарах, работах, услугах, частной жизни граждан, персональных данных, личной и семейной тайны к объектам гражданских прав.

Ряд белорусских и российских правоведов (Д.П. Александров, В.М. Богданов, Е.Н. Насонова) полагают, что, несмотря на отсутствие законодательного закрепления в целом информации в качестве объекта гражданских прав, ее следует считать таковым. Другие юристы (Л.Б. Ситдикова, В.А. Дозорцев) считают данный вопрос дискуссионным. В этом случае к объектам гражданских прав предлагают относить лишь ту информацию, которая определена законом, – охраняемую (нераскрытую) информацию.

При этом необходимо отметить, что принципами регулирования информационных отношений являются: защита информации о частной жизни физического лица и персональных данных, обеспечение безо-