внедрение этих технологий требует соблюдения правовых норм и защиты личных данных. В будущем ожидается дальнейшая интеграция IT-решений, что повысит возможности для раскрытия и предотвращения преступлений в условиях цифровой трансформации общества.

Секушенко С. И.

ВИКТИМОЛОГИЯ ЦИФРОВОЙ ПРЕСТУПНОСТИ

Секушенко Снежана Игоревна, студентка 3 курса Белорусского государственного университета, г. Минск, Беларусь, snezhana.sekushenko.2004@mail.ru

Научный руководитель: канд. юрид. наук, доцент Красиков В. С.

Инновационная политика государства, основанная на стратегиях развития высокотехнологичных секторов, поддерживает глобальные технологические тренды, а также приоритетные для страны отрасли развития. Все это приводит к появлению определенных изменений в обществе. Так, процесс информатизации общества вызван внедрением информационных технологий (IT) во все сферы деятельности человека. Вместе с тем криминальная статистика свидетельствует о том, что с внедрением новых технологий меняются и сферы преступной активности. Так, если 15-20 лет назад угрозу представляла уличная преступность, вызывал опасение уровень регистрируемых преступлений в общественных местах, то сегодня большая масса противоправных деяний совершается удаленным способом с использованием информационно-коммуникационных технологий, интернета и средств мобильной связи. Проводимые социолого-виктимологические опросы фиксируют рост виктимизации от преступлений, совершенных дистанционным способом. Такой вид дистанционной преступной деятельности, посягающей на приватность (конфиденциальность), единство (целостность) и открытость данных и информационных систем, получил название «киберпреступность». В научном сообществе к киберпреступлениям в широком смысле относят общественно опасные деяния, посягающие, помимо компьютерных систем, на иные охраняемые законом объекты, рассматриваются новые подвиды киберпреступности.

В соответствии с соглашением стран – участнц СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) не используется термин «киберпреступность», а дается определение преступления в сфере компьютерной информации как уголовно наказуемого деяния, предметом посягательства которого является компьютерная информация. На данный момент это определение присутствует только в доктрине.

Причиной большинства совершенных преступлений становилось халатное отношение пользователя к своим личным данным в сети. Таким образом, роль потерпевшего при совершении киберпреступлений трудно переоценить. Учение о жертве преступления исследует поведение разного рода лиц, пострадавших от преступлений. Интересным, на наш взгляд,

представляется анализ поведения лица, которое совершает действия в информационном пространстве посредством компьютерных систем.

В теории выделяют ряд причин виктимности в цифровых преступлениях. Основной причиной является неграмотность пользователя, так как пользователи неразумно предоставляют пароли от своих компьютеров третьим лицам. Например, жертвы предоставляют свои данные, когда кто-либо звонит и представляется служащим банка или администратором, не проверяя при этом их личность. Это распространенный случай в таком составе преступления, как мошенничество. Второй причиной является доверчивость лиц, которые используют свои данные на непроверенных сайтах. Третьей причиной является страх, так как преступники используют методы морального давления на жертв, угрожая им тем, что их денежные средства могут быть списаны третьими лицами. Четвертой причиной является нежелание устанавливать защитные программы на свои персональные устройства, так как пользователи либо не верят в их эффективность, либо не желают нести затраты на оплату этих программ. В 2022 г. проведен опрос среди жертв киберпреступлений: было выявлено, что мужчины становились жертвами преступлений в 54,8 % случаев, а женщины в 45,2 % случаев.

Имеется еще одна особенность преступлений, так как цель преступника – это, как правило, завладение чужими денежными средствами, поэтому здесь не важны личность и физические особенности жертвы, поскольку он с ней не имеет прямого контакта. При этом из-за развития технологий злоумышленники почти перестали напрямую связываться с жертвой, а совершают преступления тайно. Большинство опрошенных узнали о преступлении только после того, как списали денежные средства с их карты. Такие методы, как убеждение и психологическое давление, больше воздействуют на женщин, чем на мужчин. Однако в настоящий момент только 23 % среди молодежи являются жертвами преступлений. С одной стороны, это хороший показатель, так как большинство не становятся жертвами, но с другой – почти каждый четвертый студент является жертвой киберпреступления, при этом молодежь – это та часть населения, которая относится к категории активных пользователей компьютерных технологий, в теории они должны понимать различные мошеннические интернет-схемы.

Как правило, результатом любого виктимологического исследования являются типичный портрет жертвы и советы по профилактике определенной категории преступлений. В случае киберпреступлений описать типичный портрет жертвы очень сложно. Как уже было сказано выше, преступнику не важен пол жертвы, возраст, так как он с ней не имеет прямого контакта. Самым эффективным методом профилактики является постоянное упоминание в СМИ о новых способах совершения киберпреступлений. Одной из причин того, что злоумышленники почти перестали звонить, писать сообщения и т. д. своей жертве, является информирование населения о распространенных способах обмана. Это подтверждает и опрос.

Следует отметить, что в настоящее все больше людей не становятся жертвами киберпреступлений, поскольку слышали об определенных приемах

мошенников. Например, при поступлении в социальных сетях предложения о вложении инвестиций в какой-либо проект преступники не сообщают практически никакой конкретной информации о проекте либо отсутствуют данные о самом злоумышленнике. Вторым способом являются разработка и последующее распространение в СМИ определенных кратких схем, в которых была бы указана информация о безопасном поведении в сети Интернет и безопасном использовании мобильных устройств. Третий способ – разработка специальных компьютерных программ, которые либо блокировали бы неправомерный доступ к данным пользователя, либо уведомляли бы о нем.

Скрипко К. В.

АСПЕКТЫ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ЗЛОУПОТРЕБЛЕНИЯ ВЛАСТЬЮ ИЛИ СЛУЖЕБНЫМИ ПОЛНОМОЧИЯМИ

Скрипко Карина Васильевна, студентка 4 курса Белорусского государственного университета, г. Минск, Беларусь, kariskripko03@gmail.com

Научный руководитель: канд. юрид. наук, доцент Хлус А. М.

Преступления против государственной власти и интересов государственной службы являются темой многочисленных исследований отечественных авторов на протяжении многих лет. Особое место занимает такое преступление, как злоупотребление властью или служебными полномочиями, предусмотренное ст. 424 Уголовного кодекса Республики Беларусь (далее – УК), под которым понимается умышленное вопреки интересам службы совершение должностным лицом из корыстной или иной личной заинтересованности действий с использованием своих служебных полномочий, повлекшее причинение ущерба в крупном размере или существенного вреда правам и законным интересам граждан либо государственным или общественным интересам.

Злоупотребление властью или служебными полномочиями представляет собой прямую угрозу интересам службы. Такое общественно опасное деяние подрывает не только доверие к институтам власти, но и наносит вред общественному благополучию. Граждане теряют веру в справедливость и беспристрастность государственных органов. Это негативно влияет на отношения между государством и обществом, усложняет реализацию государственной политики и снижает эффективность работы государственных органов.

Согласно статистическим данным, представленным Верховным Судом Республики Беларусь, за последние два года наблюдается увеличение количества осужденных по ст. 424 УК, несмотря на предшествующую тенденцию к сокращению количества выявленных преступлений в рассматриваемой области: 2023 г. – 70, 2022 г. – 74, 2021 г. – 48, 2020 г. – 49, 2019 г. – 91, 2018 г. – 60, 2017 г. – 108. В связи с вышеуказанным следует, что