УДК 343.988

ФАКТОРЫ ВИКТИМНОСТИ, СВЯЗАННЫЕ С СОВЕРШЕНИЕМ КИБЕРПРЕСТУПЛЕНИЙ

А.О. ЗАЛЯЦКАЯ
(Представлено: канд. юрид. наук, доц. Ю.Л. ПРИКОЛОТИНА)

Автор данной статьи предлагает рассмотреть виктимность лиц в сфере киберпреступлений. Закономерный рост числа киберпреступлений обусловлен постоянным увеличением пользователей компьютеров. В статье выделены главные факторы виктимности жертв киберпреступлений. На основании всех выделенных факторов, сделан вывод, что данная проблема для Республики Беларусь все еще является актуальной.

Ни для кого не секрет, что в нашем современном мире информационные технологии стали неотъемлемой частью жизни современного человека. Количество абонентов фиксированного доступа в Интернет растет с каждым годом и это обстоятельство сегодня активно используется преступным сообществом и отдельными правонарушителями. По статистическим данным Управления по раскрытию преступлений в сфере высоких технологий в Республике Беларусь количество зарегистрированных киберпреступлений растет. За период январь – июнь текущего года по сравнению с тем же периодом 2019 года количество киберпреступлений увеличилось на 15,6% (с 4049 до 4679) [8]. А это значит, что проблема киберпреступности все более и более актуальна.

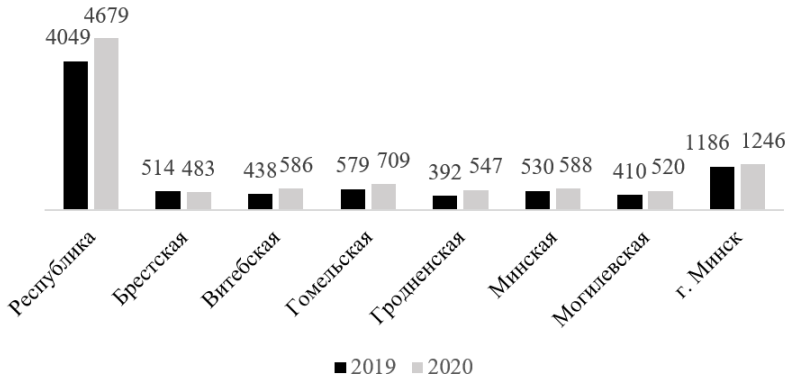

Рисунок. – Сведения о количестве преступлений, совершенных в сфере высоких технологий

Несмотря на значительный рост, киберпреступность – относительно молодой сегмент современной преступности и поэтому исследований, направленных на изучение факторов виктимности данного рода преступлений не так уж много. Это обуславливается тем, что преступность данного вида постоянно развивается и модифицируется, из-за чего правовые механизмы реагирования – по сути всегда являющиеся реакцией на преступление – зачастую запаздывают.

Следует отметить, что полного и точного определения киберпреступности не существует. Однако, если включить общие признаки понятия преступности и добавить признаки определения киберпреступления, то под киберпреступностью понимается особый вид преступности, который охватывает совокупность общественно опасных деяний, которые совершаются посредством использования информационно-телекоммуникационных систем и ее элементов [6, с. 324]. Под киберперступлением же понимается действие, нарушающее закон, которое совершается с использованием информационно-коммуникационных технологий и либо нацелено на сети, системы, данные, веб-сайты и (или) технологии, либо способствует совершению преступления [2, с. 9].

Учитывая тенденцию постоянного развития преступности в сети Интернет, можно сделать вывод, что оценить темпы расширения киберпреступности трудно, однако криминализация некоторых составов преступлений, которые учитывают степень общественной опасности какого-либо киберпреступления, происходит от виктимологического критерия. Это значит, что проявление вредных последствий от различных криминальных манипуляций в сети Интернет происходит через оценку виктимности потенциальных жертв киберпреступлений, либо лиц, которым уже фактически причинен вред. Одной из особенностей киберпреступлений является тот факт, что жертвами могут стать как обычные граждане, так и целые корпорации, поэтому факторы виктимности имеют свои специфические признаки, из-за чего становится трудным объединение их в более-менее релевантную группу [3, с. 77].

Изучив некоторые научные публикации, которые связаны с виктимностью киберперступлений, хотелось бы выделить несколько факторов виктимности на примерах хищений путем использования компьютерной техники и несанкционированного доступа к компьютерной информации, так как данные преступления преобладает в структуре криминогенной обстановки в Республике Беларусь.

Первый фактор, который хотелось бы выделить – это недостаточная «информационная грамотность». Данный фактор больше относится к лицам пожилого возраста (от 60 лет). Как известно в Республике Беларусь наблюдается старение населения. По данным переписи населения 2019 года в возрасте старше трудоспособного находится 2350 млн. человек [5], что составляет 24% от общей численности населения, а по международной классификации общество является стареющим, если доля людей в возрасте 65 лет и больше составляет 7% (в Беларуси этот показатель равен 15.2% от общей численности населения) [1]. Так сложилось, что люди пожилого возраста зачастую относятся к информационным технологиям безразлично и с презрением, из-за чего у них складывается негативное мнение к изучению и освоению компьютерной грамотности. Полагаю, что нередко бывали случаи, когда родные бабушки или дедушки подходили с вопросом: «Правда ли, что мне перечислят деньги, если я перейду по данной ссылке или отправлю данные своей карточки на этот номер?». Это как раз и свидетельствует о недостаточной компьютерной грамотности, чем и пользуются Интернет-мошенники (так за январь-июнь 2020 года по сравнению с тем же периодом 2019 года число хищений путем использования компьютерной техники увеличилось с 70,7% до 77,5% или же с 2863 до 3624 соответственно) [8]. Также такая низкая информированность зависит и от государства, которое недостаточно ведет профилактическую работу пользователей Интернет-сети. Зачастую брошюры и памятки о том, как не стать жертвой киберпреступления, размещаются на сайтах Министерства внутренних дел, на которые обычный пользователей попросту не заходит и, тем более, не ищет и не читает данного рода руководства.

Вторым фактором являются психологические особенности человека. Такими качествами выступают: доверчивость, беспечность, наивность [4]. Данное обстоятельство характерно больше для лиц пожилого возраста и лиц молодого возраста (несовершеннолетние в возрасте от 12 до 14 лет), так как ими легче манипулировать. То есть пожилым человеком проще манипулировать и злоупотреблять его доверием в силу того, что характер его участия в информационных технологиях является вынужденным в силу того, что их включают в различные реестры и банки персональных данных, либо же использование ими информационных технологий необходимо лишь для удовлетворения личных потребностей общения. Примером может служить ситуация, когда пожилому человеку в силу его доверчивости к личным контактам могут позвонить и представиться их банковским оператором или агентом, чтобы завладеть, допустим, данными с банковской карточки. Что касается несовершеннолетних, то они в силу еще не полностью сформированной психики склонны гиперболизировать выгоду от использования информационных технологиях – речь идет о увлечениях компьютерными играми. Такое лицо постепенно может отказаться от реальных контактов и ему проще довериться «интернет-другу» и выдать свои данные.

Хорошо известен тот факт, что данные виды преступлений имеют высокий уровень анонимности, из-за чего такие преступления сложно раскрыть. Так, в Беларуси, уровень раскрываемости киберперступлений составляет 50% [7]. Понимая данный факт, люди крайне редко пишут заявления в случаях, когда была совершена Ddos-атака, кража логинов и паролей – несанкционированный доступ к компьютерной информации. Также зачастую пользователи не применяют никакие антивирусные программы при работе на своем компьютере, что только облегчает возможность киберпреступнику установить вредоносные программы и завладеть данными.

Еще одним фактором виктимности возможно полагать издержки информационной культуры нашего общества [3, с. 78]. Сейчас для того чтобы узнать информацию о человеке, достаточно зайти на его страницу в какой-либо социальной сети. Это связано с тем, что с развитием информационных технологий люди стали больше проводить времени в сети Интернет, чем в жизни, поэтому, чтобы как-то самовыразиться или самореализоваться, пользователи активны в социальных сетях. Это проявляется в том, что люди размещают информацию о себе (город проживания, возраст, место учебы или работы, номер телефона) на своей личной страничке. Существует множество злоумышленников, которые от лица администраторов определенных сайтов присылают уведомление о том, что на вашей странице произошли неполадки, и чтобы их устранить нужно перейти по ссылке, которая является точной копией известной социальной сети (единственным отличием является URL-адрес). Переходя по такой ссылке, пользователь вводит свои личные данные, как и в обычной социальной сети, однако, эти данные попадают прямиком в руки преступника, тем самым он сможет использовать эти данные в своих преступных целях. Также это проявляется в создании блогов, где люди рассказывают, как они ведут свою жизнь и чем занимаются. Следовательно, данной информацией могут воспользоваться интернет-мошенники.

Исходя из выделенных выше факторов, можно сделать вывод, что проблема виктимности в сфере киберпреступлений все еще актуальна. А это значит, что государство должно уделить внимание данной

проблеме. Необходимо провести анализ всех виктимологических факторов и разработать специальные методы для проведения виктимологической профилактики среди пользователей сети Интернет.

ЛИТЕРАТУРА

1. В Беларуси 15,2 процента населения старше 65 лет [Электронный ресурс]. – Режим доступа: https://www.belta.by/society/view/v-belarusi-152-naselenija-starshe-65-let-363932-2019/#:~:text=%22Белорусское%20общество%20стареет.,%22%2C%20-%20сказал%20Александр%20Румак. – Дата доступа: 25.09.2020.
2. Введение в киберперступность / Управление Организация Объединенных Наций. – Вена, 2019. – 46 с.
3. Жакупжанов, А.О. Виктимологические факторы киберпреступности / А.О. Жакупжанов // Алтайский юр. вестник. – 2019. – №3. – С. 75-82.
4. Каткова, М.Н. Профилактика виктимности в сети Интернет / М.Н. Каткова, Е.И. Чолак // Право, международное право: материалы междунар. науч.-дистанц. студ. конф., Гродно, 8 апр. 2016 г. / БИП – Институт правоведения; редкол. : А.А. Богустов. – Гродно, 2016. – Режим доступа: http://step-science-bip.csrae.ru/pdf/1/36.PDF. – Дата доступа: 25.09.2020.
5. Население Беларуси. Численность населения Республики Беларусь в 2020, состав, структура [Электронный ресурс]. – Режим доступа: https://myfin.by/wiki/term/naselenie-belarusi. Дата доступа: 25.09.2020.
6. Кравцова М.А. Понятие киберпреступности и ее признаки / М.А. Кравцова // Журнал Киев. ун-та., Криминальное право и криминология. – 2015. – №2. – С.320-325.
7. Раскрываемость киберперступлений составляет 53-55 процентов от их общего числа [Электронный ресурс]. – Режим доступа: https://www.sb.by/articles/kapkany-na-virtualnykh-tropakh.html. – Дата доступа: 25.09.2020.
8. Статистика Управления Министерства внутренних дел по высоким технологиям // Министерство внутренних дел [Электронный ресурс]. – 2020. – Режим доступа: https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/statistika-urpsvt. – Дата доступа: 25.09.2020.