АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЮРИСПРУДЕНЦИИ И ФИНАНСОВ

ИЗУЧЕНИЕ ВИДОВ И МЕХАНИЗМОВ СЕТЕВОГО МОШЕННИЧЕСТВА, АНАЛИЗ СПОСОБОВ ПРОТИВОДЕЙСТВИЯ

Азява О.А.,
студентка 3-го курса Полоцкого колледжа ВГУ имени П.М. Машерова,
г. Полоцк, Республика Беларусь
Научный руководитель – ***Губская И.О.,*** *магистр педагогических наук*

Количество людей, активно использующих возможности сети Интернет, социальные сети, электронные платежные системы возрастает с каждым днем. И, как следствие, в последнее время мы всё чаще сталкиваемся с киберпреступностью. Причиной этого может являться как неосведомлённость людей в компьютерной сфере, так и неосознание всей тяготы данных преступлений.

Цель исследования – изучить виды и механизмы киберпреступлений, проанализировать способы противодействия.

Выделяют следующие виды преступлений в сети: финансовоориентированные киберпреступления (фишинг, кибервымогательство, финансовое мошенничество, брачные аферы, покупки в интернете, кардинг, вишинг, скимминг, шимминг – в среднем каждый месяц киберпреступники успешно атакуют 1–2 банка, средний ущерб от атаки – $2 млн. Таким образом, за прошедший год через электронные системы банков было похищено 1,3 млрд. рублей); киберпреступления, связанные со вторжением в личную жизнь (кража персональных данных, шпионаж, нарушение, авторского права); спам, социальные и политически мотивированные киберпреступления, преступления на почве ненависти и домогательства (терроризм, кибербуллинг), киберпреступления, связанные с формированием доверительных отношений с ребенком с целью его сексуальной эксплуатации или сексуального насилия (груминг).

Материал и методы. В рамках исследовательской работы было проведено анкетирование 40 участников образовательного процесса Полоцкого колледжа ВГУ имени П.М. Машерова.

Результаты и их обсуждение. Среди опрошенных – учащиеся (16–18 лет) и преподаватели (32–58 лет) колледжа. В ходе исследования выяснилось, что большинство преподавателей (85%) и учащихся (70%) колледжа оплачивают услуги через Интернет, при этом 25% преподавателей сообщали данные банковских карт через Интернет. Следует отметить, что 60% преподавателей и лишь (30%) учащихся используют двухфакторную аутентификацию. Также обращает на себя внимание тот факт, что 15% учащихся ответили, что сразу переведут деньги, если их об этом попросит знакомый человек в личном сообщении, а также 10% учащихся ответили, что всегда переходят по ссылкам, которые приходят им в сообщениях (не обязательно от знакомых людей), 55% преподавателей и учащихся всегда переходят по ссылкам от друзей.

Преподаватели считают, что в сети Интернет большинство преступлений связано с кражей денег и взломом личных страниц (80%), а также кражей личных данных (50%), и фотографий (50%). 15% опрашиваемых считают, что существует такой вид киберпреступления как запись телефонных разговоров.

Анализ анкет учащихся дал следующий результат: 60% считают, что в сети преобладает кража денег, 85% считают, что чаще встречается взлом страниц, реже встречается кража личных данных (40%) и кража фото/видео (20%), запись разговоров – в 15% случаев.

Среди респондентов были двое учащихся нашего колледжа, которые стали жертвами киберпреступников, в то время как ни один преподаватель не оказывался в данной

ситуации, хотя необходимо отметить тот факт, что 35% преподавателей и 25% учащихся смогли предотвратить киберпреступление в их отношении.

Наиболее распространёнными социальными сетями и мессенджерами среди учащихся колледжа являются – Instagram и Vk, среди преподавателей – Viber, Vk. 50% респондентов отметили, что нет ни одной безопасной сети или мессенджера, в то время как 27,5% считают наиболее безопасным использование Telegram, а Viber и Vk безопасными считают 17,5% участников опроса.

О том, что киберпреступность является, в том числе, и уголовно наказуемым преступлением известно 100% опрашиваемых, и 57,5% участников опроса знают, что предусматривается статьёй 212 УК РБ. [6]

Большинство участников опроса считают, что люди становятся жертвами киберпреступников, т.к. они не осведомлены должным образом (55%). Поэтому в рамках исследовательской работы были разработаны информационные буклеты «Как не стать жертвой киберпреступника», в которые включены рекомендации по предотвращению мошенничества с банковскими картами, взлома страниц социальных сетей, выстраивания линии общения в сети.

Заключение. Азбукой поведения современного человека должно стать применение надежных неповторяющихся паролей, отказ в передаче третьим лицам логина, пароля, использование надежных менеджеров паролей, настройка двухфакторной аутентификации, применение антивирусного программного обеспечения, лицензионного программного обеспечения, переход только по надежным ссылкам из достоверных источников, отказ в переводе денежных средств лишь по сообщению пусть даже от знакомого человека и др. [1, 2, 7] Если каждый будет следовать таким весьма простым рекомендациям, то количество жертв киберпреступников значительно сократиться.

Материалы исследовательской работы можно использовать на занятиях по информатике, информационных технологий, на внеучебных мероприятиях, кураторских часах.

1. Как не попасть в сети онлайн-мошенников [Электронный ресурс]. – https://digitalrights.center/blog/kak-ne-popast-v-seti-onlayn-moshennikov/ – Дата доступа: 01.11.2019.
2. Кибер-вымогательство [Электронный ресурс]. – https://itmatika.pro/blog/novye-it-terminy/kiber-vymogatelstvo – Дата доступа: 15.11.2019.
3. Киберпреступления: понятие, виды и методы защиты [Электронный ресурс]. – https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnostponyatie-vidy-i-metody-zashchity.html – Дата доступа: 05.01.2020.
4. Откуда приходит киберпреступность? Происхождение и эволюция киберпреступности [Электронный ресурс]. – https://levpn.com/ru/cybercrime-history/– Дата доступа: 10.12.2019.
5. Статистика УРПСВТ за 2018 год [Электронный ресурс]. – https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sferevysokih-tehnologij-upravlenie-k/stastistika-urpsvt – Дата доступа: 01.11.2019.
6. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З [Электронный ресурс]. – http://уголовный-кодекс.бел/ – Дата доступа: 20.10.2019.
7. Фишинг [Электронный ресурс]. – https://ru.malwarebytes.com/phishing/– Дата доступа: 11.12.2019.

ПРАВОВЫЕ АСПЕКТЫ ДОГОВОРА ОБ ОКАЗАНИИ УСЛУГ, ЗАКЛЮЧАЕМОГО МЕЖДУ ГОСУДАРСТВЕННЫМ УЧРЕЖДЕНИЕМ (ЦЕНТРОМ) С БЮДЖЕТНЫМИ ОРГАНИЗАЦИЯМИ

Амельченя Ю.А.,
кандидат юридических наук, доцент, ведущий научный сотрудник НЦЗПИ,
г. Минск, Республика Беларусь

Актуальность исследования правовых аспектов нового для правовой системы Республики Беларусь договора об оказании услуг, заключаемого между государственным учреждением (центром) с бюджетными организациями (далее – договор) в соответствии с Указом Президента Республики Беларусь от 23.12.2019 г. № 475 «Об обеспечении деятельности бюджетных организаций» (далее – Указ № 475), обусловлена необходимостью выстраивания соответствующих правоотношений между его сторонами при осуществлении государственных закупок.