УДК 343.34: 004

ОСОБЕННОСТИ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Бабкова Н.С.

магистр 3 курса обучения

Академия права и национальной безопасности

ЧОУ ВО ЮУ (ИУБиП), e-mail: akadem_prava@iubip.ru

Научный руководитель

к.ю.н.,Фоменко А.И.

Доцент кафедры «Уголовно-правовые дисциплины»

ЧОУ ВО ЮУ (ИУБиП)

Аннотация: Статья посвящена преступлениям в сфере информационных технологий. Рассмотрены основные виды таких преступлений и рекомендации для самозащиты граждан от таких посягательств.
Ключевые слова: интернет, киберпреступность, информация, Уголовный Кодекс РФ.

FEATURES OF COMMITTING CRIMES IN THE FIELD OF COMPUTER INFORMATION

Babkova N.S.

Abstract: The article is devoted to crimes in the field of information technology. The main types of such crimes and recommendations for self-defense of citizens from such attacks are considered.
Keywords: Internet, cybercrime, information, criminal Code of the Russian Federation.

Мы привыкли работать и практически жить в интернете, и совершенно забываем о том, что защищать свое онлайн-пространство надо точно так же, как и свой дом. Преступления в сфере информационных технологий уже давно перестали быть редкостью. За первые восемь месяцев 2019 г. в России было зарегистрировано 180153 киберпреступления. Это на 66,8% больше показателя за аналогичный период предыдущего года, сообщает нам Генпрокуратура. Речь идет о преступлениях, совершенных с использованием

ИКТ или в сфере компьютерной информации. Если сравнивать с другими видами преступлений, то темпы роста в данном виде оказываются самыми высокими.

Для сравнения рассмотрим небольшую статистику: количество тяжких преступлений выросло всего на 16,7%, а особо тяжких уменьшилось на 3,1%. Количество краж выросло на 3,5%. Количество случаев присвоения или растраты уменьшилось на 1,4%, грабежей — на 7,9 %, разбоев — на 8,9 %. Количество преступлений в сфере незаконного оборота наркотиков уменьшилось на 3,4%. С рекордным ростом киберпреступности сопоставим только рост количества случаев посредничества во взяточничестве на 46,4%, и случаев дачи взятки на 35,4%. При этом общий рост числа преступлений коррупционной направленности составил всего 3,6%. Также одним из самых быстрорастущих является сегмент мелкого хищения — здесь количество инцидентов выросло на 38,9% [2, с.193].

В данной статье будут рассмотрены особенности преступлений в сфере компьютерной информации, кто и при каких обстоятельствах подлежит уголовной ответственности за использование вирусных программ, взломы компьютерных систем, распространение конфиденциальной информации и многие другие виды киберпреступлений.

Такие преступления, во-первых, связаны с нарушением авторских прав. Каждая программа, созданная для той или иной модели ЭВМ– продукт автора, владельца. Копирование, продажа дисков с этими программами, взлом все это действия незаконные. С преступлениями такого вида ведется борьба во всем мире. В большинстве случаях киберпреступники взламывают чужие страницы социальных сетей, такие действия являются нарушением частных прав таких как: право на личную жизнь, переписку и т.д. Очень часто преступник совершает противозаконные деяния удаленно, то есть может находиться в другом городе относительно от потерпевшего или вообще заграницей. Уголовная ответственность за такие деяния

предусмотрена ст. 137, 138 УК РФ[1]. Об этом можно подробнее узнать из статьи о неприкосновенности частной жизни.

В последнее время все более актуальной проблемой становится мошенничество через сети интернет. Почти каждый из нас сталкивается с противозаконным списанием денежных средств со счетов, карт, электронных кошельков и т.д. В случаях, когда деяния связаны с несанкционированным доступом различного рода программам, то они подпадают под уголовные преступления, которые посягают на безопасность компьютерной информации.

Незаконные посягательства на информационную безопасность в литературе делят на два вида. Первый вид, это противозаконные действия в отношении материальных носителей информации, то есть заражение вирусом, приведение в негодность карт, дисков, а также незаконное их копирование [3, с.208].

Второй вид, это противозаконные действия по использованию информации, а именно похищение конфиденциальных баз данных, уничтожение важной информации и (или) сбыт личной информации, полученной незаконно.

По каждому делу в обязательном порядке проводится компьютерная экспертиза, в рамках которой происходит техническое исследование содержимого различных устройств, оперативной памяти, определение айпи-адреса и его регистрационных данных. Выводы эксперта о незаконном нарушении информационной безопасности строятся на специально разработанных методиках отечественных и зарубежных ученых. Используя специальные познания в области техники, специалисты могут установить местонахождение пользователя ПК, его полные данные и время совершения противоправного деяния. Ответственность за преступления в сфере компьютерной информации предусмотрена в главе 28 Уголовного Кодекса РФ, в ней содержится четыре самостоятельных преступления[4, с.215].

Как же избежать преступных посягательств киберпреступников? Достаточно придерживаться определенных правил самозащиты и риск попасть в руки злоумышленников будет очень низок. К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее. Старайтесь регулярно проверять состояние своих счетов, чтобы убедиться в отсутствии каких-то странных операций. Поставьте лимит на сумму списаний или перевода в личном кабинете банка. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно. Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках.

Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма. Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно[5, с.6]. Перечень таких рекомендаций самозащиты неисчерпывающий и соблюдать их, конечно, сложно, но возможно. Как показывает практика стоит в уже школе на уроках ОБЖ рассказывать детям об этих правилах, так как в ловушки такого рода попадаются не только взрослые, но и дети.

Библиографический список

Уголовный кодекс Российской Федерации от 13. 06. 1996 года № 63 – ФЗ (ред. от 27.12.2019) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 18.02.2020).

Сачихин Р.А. Электронные деньги и цифровые права. Очередной путь в неизвестное? // Молодой ученый. — 2019. — №14. — С. 193-197. — URL https://moluch.ru/archive/252/57833/ (дата обращения: 27.01.2020).

Фоменко А. И., Флюстунова А.А. Понятие и виды преступлений в сфере высоких технологий в зарубежном уголовном законодательстве // Интеллектуальные ресурсы – региональному развитию. – 2015. – №5. – С. 208-212.

Фоменко А.И. К вопросу об уголовно-правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития // Интеллектуальные ресурсы – региональному развитию. – 2015. – №5. – С. 217-222.

Фоменко А.И. Преступность в сфере высоких технологий: криминологические проблемы борьбы в России // Ученые записки Интситута управления, бизнеса и права. Серия: Право. – 2016. – №7. – С. 6-11.