УДК 343.982.5

АНАЛИЗ МОТИВОВ И УСЛОВИЙ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Ковальчишина С.В.
кандидат психологических наук
доцент кафедры психологии и педагогики
ГБУ ВО «Академия МВД ДНР имени Ф.Э. Дзержинского»
Зарипова Ю.А.
курсант
ГБУ ВО «Академия МВД ДНР имени Ф.Э. Дзержинского»

Аннотация. Статья посвящена причинам и мотивам, которые побуждают к совершению преступлений в сфере экономики. В данной статье также исследуются способы предотвращения киберпреступлений.

Ключевые слова: кибермошенничество, киберпреступность, киберпространство, сеть интернет.

Введение. Киберпреступностью обычно называются различные виды незаконной деятельности, которые используются в Интернете, в частной или публичной сетях либо внутренних компьютерных системах. В то время как большинство форм киберпреступности связано с похищением конфиденциальной информации для несанкционированного использования, существуют и другие формы преступных действий, сосредоточенные на вторжении в частную жизнь [1].

Цель. Изучение мотивов совершения киберпреступлений и способах их предотвращения.

Основное содержание. Существенным фактором, оказывающим негативное влияние на криминогенную ситуацию в стране, продолжает оставаться рост IT-преступности. По сравнению с аналогичным периодом прошлого года в январе-июне 2021 года он составил 20,3%. Удельный вес указанных противоправных деяний в общей структуре преступности достиг 26,5%. Зафиксирован рост преступлений, совершенных при помощи сети Интернет – на 42,1%, с использованием компьютерной техники – на 35,6% [2].

Киберпреступность относится к электронным преступлениям. К основным видам киберпреступности относятся распространение вредоносного программного обеспечения, кража паролей, кража номеров кредитных карт и других банковских реквизитов [3].

Киберпреступность относится к преступлениям в сфере экономики. Исходя из Уголовного кодекса Российской Федерации можно выделить следующие виды электронных преступлений, за которые предусмотрена уголовная ответственность:

- Мошенничество в сфере кредитования;
- Мошенничество с использованием электронных средств платежа;
- Мошенничество в сфере компьютерной информации [4].

Важным аспектом юридической практики является установление и анализ мотивов, целей совершения преступления в сфере экономики с использованием компьютерных технологий. В общем смысле основой формирования субъективной стороны преступления (потребностей, мотивов и целей) является социальная среда обитания преступника, в особенности ее содержательная часть. Специфика данной среды в отношении киберпреступников заключается в ее двухфакторной структуре. С одной стороны социальная среда преступника включает непосредственный реальный социум (семья, школа, друзья), а с другой стороны – виртуальное пространство [5].

Виртуальное пространство специфично по своей природе: во-первых, оно не имеет реальных границ, во-вторых, оно интернационально, в-третьих, для него характерно формирование своей мощной киберкультуры.

Для киберпреступлений в большинстве своем характерны корыстные и политические мотивы преступления. Преступления в сфере экономики как правило базируются на корыстном мотиве. В связи с развитием сети интернет, развивается кибермошенничество, как разновидность киберпреступлений. Можно стать не только жертвой преступных посягательств, но и не подозревая, участником или соучастником преступления. К основным условиям и причинам, толкающим людей на совершения преступления в данной сфере, являются:

- легкий способ совершения. Например, когда мошенники предлагают оплатить какую-либо услугу, но получив деньги заносят людей в черный список. В данном случае, сама жертва заинтересована в оказании услуги, однако в поисках источника реализации необходимой услуги попадают на мошенника;

- получение большой прибыли. Как известно, банковские карты являются одним из наиболее безопасных способов хранения денежных средств. И за один звонок мошенники могут получить даже миллион рублей, злоупотребляя доверием жертвы;

- сложность в поиске преступника. Банковские переводы могут осуществляться между разными странами. И найти мошенника из другой страны составляет большие трудности для правоохранительных органов на территории того государства, где жертвами стали её граждане;

- латентность. Люди, столкнувшиеся с мошенниками, нередко умалчивают о произошедшем в силу определенных факторов, например: чувствуют свою вину, отсутствие времени, малозначительность ущерба;

- популярность, слава. Некоторые киберпреступники обходят защиту сайтов государственного значения. Это производит резонанс. На поиск преступника бросают все силы правоохранительных органов. Это хорошая возможность прославится, как минимум, на всю страну.

Цели киберпреступлений также различны, но в большинстве своем на практике встречаются цели незаконного обогащения, а также дестабилизации каких-либо, в том числе, государственных структур [5].

Выводы. Таким образом, установление и анализ субъективной стороны совершения преступлений в сфере экономики с использованием компьютерных технологий расширяет круг превентивной деятельности правоохранительных органов по профилактике и недопущению киберпреступлений. Предотвратить совершение преступлений в сфере экономики реально. На основании вышеизложенного авторы статьи предлагают следующие способы:

- ввести в школьную программу уроки финансовой грамотности;

- сделать СМС рассылку со сведениями о том, как не стать жертвой и как отличить мошенников от работников банка. Граждане должны понять, что называть данные карт по мобильной связи они могут лишь в том случае, когда самостоятельно звонят на официальный номер банковского учреждения;

- прекратить установку файлов с подозрительных и неизвестных источников в сети интернет, ведь, кроме полезных файлов можно установить вирус, который передаст вашу конфиденциальную информацию киберпреступникам;

- проверять местонахождение своих близких, в случае шантажа;

- не пренебрегать установлением всех этапов безопасности страницы в социальных сетях;

- блокировать банковскую карту в случае потери, это можно сделать даже в телефонном режиме.

В заключении хотелось бы добавить, что обязанность каждого гражданина обезопасить свои финансы, свою конфиденциальную информацию. Соблюдая простые правила, можно предотвратить совершение IT-преступлений.

Список литературы

1. Волеводз А. Г. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Сборник документов. Москва: Юрлитинформ, 2001. 496 с.

2. Краткая характеристика состояния преступности в Российской Федерации за январь-июнь 2021 года [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/item/25094008/ (дата обращения 12.11.2022)

3. Леонов А. П. и др. под общ. Ред. А. П. Леонова. Компьютерная преступность и информационная безопасность. Минск: АРИЛ, 2000. с. 552.

4. Российская Федерация. Законы. Уголовный кодекс Российской Федерации (УК РФ) от 13.06.1996 N 63-ФЗ (ред. от 24.03.2022) [Электронный ресурс] – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 12.11.2022)

5. Ощепкова, Е. В. Особенности мотива и цели киберпреступлений / Е. В. Ощепкова. — Текст : непосредственный // Молодой ученый. — 2021. — № 47 (389). — С. 258-259. — URL: https://moluch.ru/archive/389/85749/ (дата обращения: 22.11.2022).