

Корчагин Павел Владимирович

Студент 1 курса

Башкирский государственный университет

Научный руководитель: Сакаева Эльвира Зинуровна

Кандидат экономических наук, доцент

Башкирский государственный университет

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В СЕТИ ИНТЕРНЕТ

***Аннотация.** Стремительное внедрение цифровых технологий во все сферы человеческой жизни предопределило возникновение новых общественных отношений. Наибольшую значимость и распространенность имеет технология Интернет, которая сделала коммуникации дешевыми и беспрепятственными, открыла новые горизонты для всего мирового сообщества и дала человеку безграничные возможности в области распространения информации.*

Всего несколько лет назад, интернет-преступления совершались в России, ввиду своей привилегированности, крайне редко, а интернет-преступность как негативное социальное явление, представляло реальную угрозу лишь в обозримом будущем. Но уже сейчас доля сетевой преступности в структуре общероссийской, существенно увеличилась. С появлением современных средств компьютерных технологий и телекоммуникаций, традиционные преступления - воровство, мошенничество, шпионаж, вымогательство трансформировались в новые формы. В статье рассмотрены экономические преступления в сети Интернет.

***Ключевые слова:** преступление, экономические преступления, интернет, киберпространство, мировая экономика.*

Korchagin Pavel Vladimirovich

Student 1 term

Bashkir State University

Scientific adviser

Sakaeva Elvira Zinurovna

Candidate of Economic Sciences, Associate Professor

Bashkir State University

ECONOMIC CRIMES ON THE INTERNET

Annotation. *The rapid introduction of digital technologies into all spheres of human life has predetermined the emergence of new social relations. The Internet technology is of the greatest importance and prevalence, which has made communications cheap and unhindered, opened new horizons for the entire world community and gave people unlimited opportunities in the field of information dissemination. Just a few years ago, Internet crimes were committed in Russia, due to their privilege, extremely rarely, and Internet crime as a negative social phenomenon posed a real threat only in the foreseeable future. But already now the share of network crime in the structure of the all-Russian has increased significantly. With the advent of modern means of computer technology and telecommunications, traditional crimes - theft, fraud, espionage, extortion have transformed into new forms. The article deals with economic crimes on the Internet.*

Keywords: *crime, economic crimes, Internet, cyberspace, world economy.*

За последние несколько десятилетий человечество сделало значительный прорыв в развитии науки и технологий, в особенности в тех отраслях, которые связаны со способами хранения и передачи информации, автоматизации технологических процессов, цифровизации государственной, политической, экономической, общественной и иных сфер жизнедеятельности. Глобальная

цифровизация благоприятно отражается на мировой экономике, производя существенные положительные изменения, связанные со значительным расширением рынков сбыта продукции, работ, услуг. Вместе с тем, виртуальное пространство, благодаря которому мы сегодня имеем возможность реализовывать многочисленные возможности, является также инструментом, позволяющим дистанционно получать доступ к любым данным, хранящимся в виде машинного кода. В результате складывается ситуация, когда рост возможностей, предоставляемых глобальной цифровизацией, пропорционально увеличивает потенциал кибератак, которым могут быть подвержены различные объекты, наиболее значимые в сфере государственной или общественной жизни [5, с. 225].

Сегодня в повседневной жизни используется много разных высокотехнологичных устройств - пластиковые карты, мобильные телефоны, планшеты, компьютеры. Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь определенно лучше, но требует достаточных навыков и знаний. Однако наряду с развитием высоких технологий появляются новые виды мошенничества, что, в свою очередь, ставит задачу борьбы с такими преступлениями перед обществом и правоохранительными органами. Особенно это касается глобальной сети Интернет, который не знает границ, поэтому позволяет мошенникам осуществлять свои преступные намерения на расстоянии.

Стремительное развитие рынков товаров, работ и услуг, сопровождающееся возможностью осуществления мгновенных безналичных платежей, повлекло за собой появление нового вида преступности – киберпреступности.

Массовое распространение экономической киберпреступности, ставящее безопасность тысяч пользователей в зависимость от компьютерных мошенников - кибермошенников, началось сравнительно недавно. Однако на сегодняшний день можно сказать, что усложнение и видоизменение

преступной деятельности, связанной с использованием глобальных компьютерных сетей, происходит постоянно, и нет никаких оснований считать, что в ближайшее время ситуация может измениться в лучшую сторону. Положение усугубляется еще и тем, что происходит вытеснение примитивного уголовного типа преступников интеллектуальными и предприимчивыми, с более изощренными способами ведения преступной деятельности. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей.

Анализируя возможные риски в экономической сфере, связанные с переходом на цифровые информационные технологии, к числу современных экономических киберугроз можно отнести атаки на банки, атаки на брокера, атаки на расчетную систему, хищения через интернет-банкинг, неправомерное использование бренда, применение программы-вымогателя и некоторые другие действия, совершаемые посредством использования вредоносных программ [2, с.29].

Главными факторами, которые оказывают влияние на совершение экономических преступлений в киберпространстве, являются:

- экономический кризис;
- повышение цен на товары первой необходимости;
- снижение уровня жизни;
- повышение уровня безработицы и т.д.

Использование возможностей киберпространства облегчает процесс совершения преступления на каждом этапе, позволяет оставаться анонимным и снижает риск быть пойманным.

Основой киберпреступлений, совершаемых в сфере экономической деятельности, являются незаконные предпринимательская и банковская деятельности, а также организация и проведение азартных игр, что, в свою очередь, приводит к созданию теневой экономики и черного рынка товаров и услуг. Однако если еще несколько десятилетий назад все операции

осуществлялись банками, то сегодня международный перевод денежных средств можно совершить в киберпространстве. Благодаря своей анонимности и «безграничности» киберпространство даёт почти любые возможности по приданию легальной формы преступному доходу. Интернет является местом осуществления всей мировой торговли, где возникают предпосылки для «отмывания денег», что является новым способом легализации. Данное обстоятельство образует множество трудностей в вопросах квалификации деяний, поиска и привлечения к ответственности виновных лиц, усложняет доказывание совершенных преступлений, а также создаёт условия для укрепления организованной киберпреступности [3, с.27].

Сотрудники правоохранительных органов неизбежно сталкиваются с большими трудностями в раскрытии и расследовании преступлений, поскольку преступления, совершаемые при помощи компьютерных технологий, характеризуются высокой секретностью, трудностями в сборе доказательств, для установления фактов их совершения и трудностями доказывания в суде [4, с.328].

Компьютерные преступления все чаще носят трансграничный характер. К этому приводит отсутствие как таковых границ в киберпространстве, что позволяет преступникам уйти от ответственности за границу, особенно туда, где не развита соответствующая служба, несовершенна нормативная база, не налажены методики расследований. В связи с этим приходится находить новые способы расследования киберпреступлений.

Необходимо отметить, что глобализация мировой экономики является безусловно важным фактором ее дальнейшего развития. Фактическая денонсация государственных границ при формировании новых (глобальных) рынков сбыта на сегодняшний день уже воспринимается как естественное явление. Однако нормальное функционирование экономики в новых условиях станет возможным только тогда, когда большинство государств объединят свои усилия в деятельности по противодействию компьютерной

преступности. Сегодня же многие компании все еще остаются уязвимыми для вновь возникающих киберугроз, что обусловлено использованием устаревших механизмов и технологий, недостаточной технической подготовленностью персонала, а также банальной халатностью, допускаемой работниками компании, так или иначе осуществляющими свою деятельность во всемирной глобальной сети, и отсутствием «цифровой культуры».

Характеризуя усилия, направленные на борьбу с проявлениями киберпреступности, следует отметить, что на сегодняшний день большинство мировых держав понимают опасность этого явления и предпринимают определенные шаги к тому, чтобы противостоять ей. Вместе с тем, нельзя не отметить, что, во-первых, вплоть до настоящего времени не было разработано единого международного документа, посвященного данной проблеме – все существующие международные соглашения в этой области носят лишь региональный характер. Во-вторых, даже имеющиеся дву- и многосторонние соглашения, распространяющие свое действие на определенный регион, как правило, существенно отстают в своем правовом регулировании от стремительно развивающегося технического прогресса [1, с.252].

Таким образом, для успешной борьбы с преступлениями, совершаемыми в сети Интернет, в том числе экономическими, требуется, во-первых, унификация подходов к пониманию самой сущности этого явления, во-вторых, активизация усилий всех без исключения государств, направленных на оперативную модернизацию внутреннего законодательства и разработку глобального международного соглашения, нормы которого регулировали бы складывающиеся отношения в рассматриваемой сфере, в-третьих, государственное финансирование программ, направленных на выявление киберпреступлений и изобличение киберпреступников, в-четвертых, повышение уровня осведомленности в области кибербезопасности как государственных органов и компаний, так и граждан.

Киберпространство нельзя оставить вне рамок правового поля. Информационные технологии уже проникли во все жизненно важные сферы общества и стали неотъемлемой их частью. Игнорирование кибер-угрозы может привести лишь к краху современного общества. Необходима оперативная реализация мер противодействия киберпреступности [6, с.192].

Список литературы:

1. Головенчик М.Г. экономический аспект киберпреступности: современное состояние и тенденции развития // Тенденции экономического развития в XXI веке. Материалы III Международной научной конференции. Минск, 2021. С. 251-254.
2. Грачева Ю. В. Цифровизация: некоторые уголовно-правовые риски в сфере экономики // Уголовное право. 2019. № 5. С. 28-30.
3. Киданова Н.Л. Актуальные проблемы современности – экономические преступления, совершаемые в киберпространстве // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2018. № 1. С. 26-29.
4. Никитина И.А. Совершенствование уголовного законодательства РФ по противодействию преступлениям в сфере экономической деятельности, совершаемым в сети Интернет // Проблемы современного законодательства России и зарубежных стран. Материалы VIII Международной научно-практической конференции. 2019. С. 327-332.
5. Шахбулатов М.М. Экономические преступления, совершаемые в киберпространстве // Право и правосудие в современном мире: актуальные проблемы уголовного, уголовно процессуального, международного и экологического права. Сборник научных статей молодых исследователей. Санкт-Петербург, 2020. С. 224-227.
6. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им / М.А. Простосердов //

Судебные известия. Информационный бюллетень Управления судебного департамента в Тамбовской области. – 2017. – №15(2) – С. 192.

© Корчагин П.В., Сакаева Э.З., 2021.