Российский экономический интернет-журнал №1/2022

Научная статья

Original article

УДК 338.2

Совершение мошеннических действий в сети Интернет и их влияние на экономическую безопасность

Микаева А.С., к.э.н., доцент

МИРЭА-Российский технологический университет, Москва, Россия

Пенчукова Т.А., к.э.н., доцент

МИРЭА-Российский технологический университет, Москва, Россия

Аннотация. В данной статье рассматривается влияние мошеннических действий в сети Интернет на экономическую безопасность личности, хозяйствующего субъекта и государства в целом. Авторами приводятся виды мошеннических действий, совершаемых в сети Интернет, обосновываются причины их стремительного развития и увеличения. Рассматриваются меры по предотвращению мошеннических действий и защите конфиденциальной информации в сети Интернет.

Ключевые слова: мошеннические действия, сеть Интернет, экономическая безопасность, мошенничество в сети Интернет, правонарушение, преступление, меры борьбы

Committing fraudulent activities on the Internet and their impact on economic security

Mikaeva A.S., Candidate of Economics, Associate Professor

MIREA-Russian Technological University, Moscow, Russia

Penchukova T.A., Candidate of Economics, Associate Professor

MIREA-Russian Technological University, Moscow, Russia

Annotation. This article discusses the impact of fraudulent activities on the Internet on the economic security of an individual, an economic entity and the state as a whole. The types of fraudulent activities committed on the Internet are given, the reasons for their rapid development and increase are substantiated. Measures are considered to prevent fraudulent activities and protect confidential information on the Internet.

Key words: fraudulent activities, Internet, economic security, Internet fraud, offense, crime, countermeasures

Активное развитие информационно-телекоммуникационных технологий и сетей, характеризуется ростом скорости и объема передаваемой информации, применением новых методов ее поиска и хранения, уникальными возможностями производства, новыми видами деятельности в сети Интернет, что приводит к появлению новых способов мошеннических.

Масштабы правонарушений в информационной сфере, можно проследить в различных источниках, например, статистические и аналитические материалы, а также отчеты Министерства внутренних дел РФ, Министерства экономического развития РФ, Федеральной службы безопасности, Федеральной службы технического и экспортного контроля и т.п. (табл. 1)

Таблица 1

Отчет по данным МВД России о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий

Базовый период	Количество преступлений
Январь-декабрь 2020 г.	510 396
Январь-декабрь 2019 г.	201 700
Январь-декабрь 2018 г.	121 247

Для более полного понимания динамики преступлений в данной сфере (на основании данных, рассмотренных в табл. 1), составлена столбчатая диаграмма (рис. 1).

Рис. 1 – Динамика роста количества преступлений, совершенных использованием информационно-телекоммуникационных технологий

В данных, предоставленных пресс-службой МВД, говорится, что в России в 2020 году зарегистрировано 510,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий. Это на 73,4% больше, чем в предыдущем году. 80% из них (410,5 тыс.) совершены путём кражи или мошенничества. В 2020-м злоумышленники при совершении преступлений чаще использовали банковские карты, сеть Интернет и телефон. В частности, за год количество деяний с применением пластиковых карт увеличилось на 453,1%, достигнув 190,2 тыс. С помощью сети Интернет было совершено 300,3 тыс. преступлений (+91,3%), средств мобильной связи – 218,7 тыс. (+88,3%). Зачастую одно и то же преступление может совершаться с применением одного или двух приведённых методов, уточнили в ведомстве [2].

На основании данных, представленных на рис. 2, отчетливо видно, что преступления, совершаемые с использованием информационно-коммуникационных технологий и в сфере компьютерной информации (большая часть из них, совершается в сети Интернет) занимают практически одну четвертую часть от всех преступлений.

Особое внимание хотелось бы обратить на область, связанную с экономикой. Действительно, ведь именно эта сфера больше всего подвергается кибератакам злоумышленников, которые порой несут значительные и непоправимые последствия не только для отдельного человека или группы людей, а для всего государства, а иногда и для целого мира. Экономическая

безопасность является частью экономической политики государства. Главным образом, она обеспечивает экономический суверенитет страны, единство ее экономического пространства, стабильное и бесперебойное функционирование, финансовую устойчивость государства. При дестабилизации экономики, как известно, происходит отток капитала за рубеж, либерализация цен и непродуманная приватизация, девальвация национальной валюты, рост инфляции, кризис финансовой системы, криминализация общественных отношений и т.д.

Рис. 2 – Преступления, совершенные с использованием информационно-телекоммуникационных технологий (данные МВД России за январь – сентябрь 2020 г.)

Особую популярность в современном обществе приобретает такой вид правонарушения в сети Интернет как мошенничество. В соответствии со ст. 159 Уголовного кодекса РФ мошенничество – «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» [1].

Преимущественно в связи с повсеместным распространением COVID-19 и введением всеобъемлющих мер социального дистанционирования, увеличилось применение онлайн-коммуникаций государственными органами, предприятиями и частными лицами. Следует отметить тот факт, что большинство пользователей сети Интернет мало знакомы с онлайн-технологиями и принципами их работы, что является существенным

преимуществом для злоумышленников; а так же факт того, что в настоящее время в сети Интернет осуществляется огромное количество различных мошеннических действий, которые можно классифицировать по следующим группам:

1) интернет-попрошайничество как один из наиболее распространенных видов мошеннических действий в сети Интернет, выражаемых в просьбе пожертвовать какую-либо сумму денежных средств, что является определенной угрозой экономической безопасности личности;

2) сайты-подделки, другими словами, сайты-клоны — внешне (дизайн, интерфейс, оформление) не отличаются от оригинальных сайтов. Создаются такие сайты на подобие популярных социальных сетей, с целью выманивания денежных средств или взлома аккаунтов;

3) программы-блокеры – созданы для проникновения в систему и блокирования доступа к ней;

4) фишинг является также одним из наиболее распространенных видов мошеннических действий в сети Интернет, его целью является получение доступа к конфиденциальным данным пользователей. Например, отправление личного сообщения на электронный адрес пользователя от имени банка [3]. Он подразделяется на следующие типы (рис. 3).

Приведем следующий перечень причин, которые порождают столь большое количество мошеннических действий в сети Интернет:

- инкогнито, другими словами, анонимность пользователей, данная особенность очень заманчива для пользователей Сети, так как можно скрыть свое имя, место положение, возраст, в общем все личные данные, что при совершении правонарушения является несомненным плюсом для мошенника.
- доступная цена (низкая цена за услуги, кроме того, существует и бесплатный доступ выхода в сеть Интернет, практически из любого места).
- масштабность (возможность охвата достаточно большой аудитории, причем из разных уголков мира, что также является огромным преимуществом для преступника).

- бесконтактность – это свойство позволяет выполнять те или иные действия на большом расстоянии, без личного присутствия на месте преступления.
- скорость совершаемых действий (информация между пользователями, компаниями, государствами распространяется достаточно быстро, не взирая на расстояния и какие-либо границы).

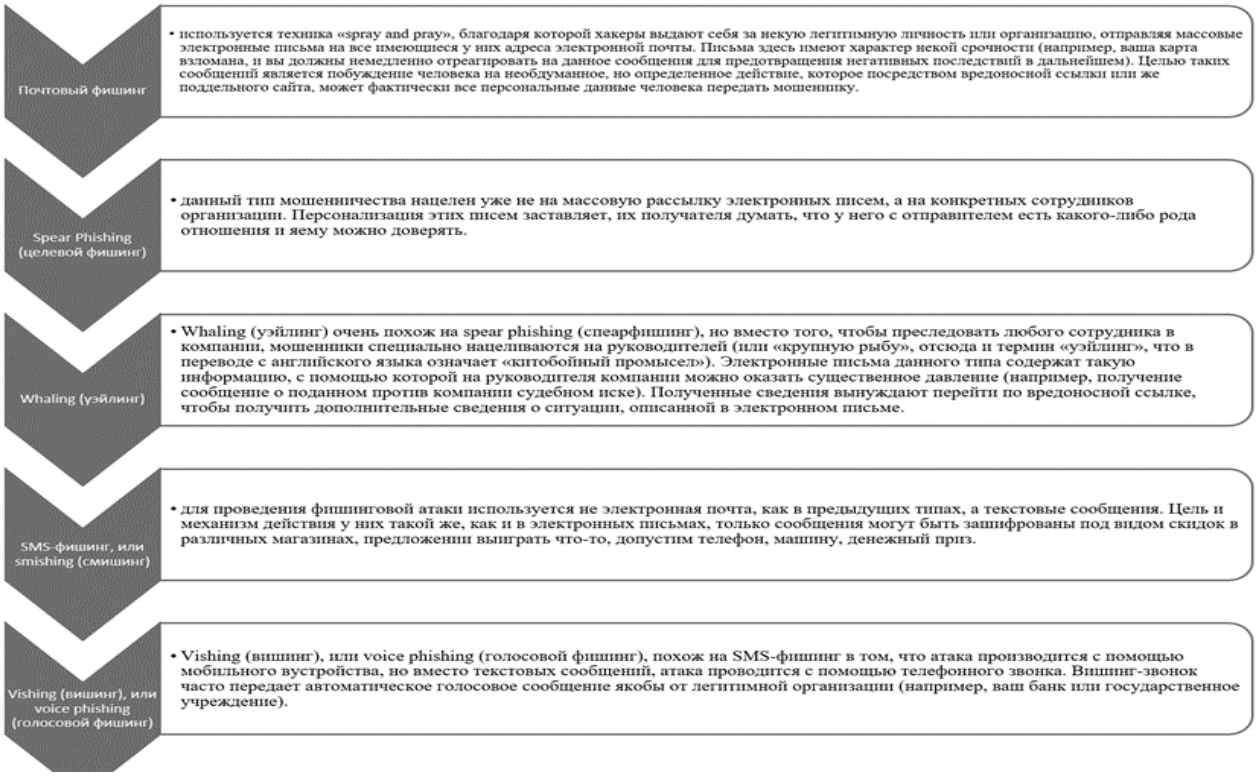

Рис. 3 – Разновидности фишинга

Из всего вышеперечисленного можно сделать вывод, что сеть Интернет является идеальной площадкой для совершения мошеннических действий. Анонимность, бесконтактность, масштабность, наивность людей и многое другое –подталкивает на совершение все большего количества преступлений в данной сфере.

Если рассматривать совершение мошеннических действий в сети Интернет как угрозу экономической безопасности, то, несомненно, все рассмотренные выше виды мошеннических действий несут множество негативных последствий как для личности, хозяйствующих субъектов, так и государства в целом (табл. 2).

Таблица 2

Влияние мошенничества в сети Интернет на личность, хозяйствующий субъект, государство

Субъект экономической безопасности	Личность	Хозяйствующий субъект	Государство
Последствия от мошеннических действий в сети Интернет	1) Манипулирование сознанием и поведением человека, приводит к растлению нравственного сознания людей. 2) Финансовые убытки. 3) Появление недоверия к различным благотворительным фондам, фондам помощи, интернет-магазинам и сайтам, банкам. 4) Потеря имущества. 5) Нарушение гражданских прав и свобод человека и т.д.	1) Раскрытие конфиденциальной информации, получение информации конкурентами. 2) Финансовые потери. 3) Банкротство. 4) Уменьшение объемов производства, а тем самым невыполнение договорных условий в срок. 5) Уменьшение доли рынка, т.е. потеря позиции на рынке. 6) Потеря репутации. 7) Снижение доверия клиентов и инвесторов. 8) Нарушение бизнес-процессов и т.д.	1) Искажение информации, приводит к нарушению международных отношений, обостряет обстановку как внутри страны, так и между странами, что в худшем случае влечет за собой начало военных действий, а также оказывает влияние на политическую жизнь общества. 2) Дефицит бюджета. 3) Инфляция. 4) Увеличение теневого сектора. 5) Нарушение функционирования экономической деятельности страны. 6) Увеличение криминализации экономики (например, легализация денежных средств или иного имущества, приобретенных приступным путем) и т.д.

Совершение мошеннических действий приводит к нарушению множества процессов, которые способствуют эффективному развитию личности, стабильному функционированию хозяйствующего субъекта и других. Кроме того, происходит подрыв национальной безопасности, так как экономическая безопасность является одной из ее составляющих.

Как же бороться с таким типом преступлений? Какие меры нужно предпринять для предотвращения противозаконных действий злоумышленников? Ответим на данные вопросы.

Во-первых, совершенствование нормативно-правовой базы. Из-за недостаточной разработанности теории права сети Интернет отношения, возникающие в Сети, трактуются российскими исследователями достаточно неопределенно, что отрицательно сказывается на формулировании общей

концепции права в сети Интернет и его специфики на современном этапе развития общества [4].

Во-вторых, создание специальных подразделений или улучшение действия уже существующих. Целью, которых является перехват сообщений, звонков от мошенников; предупреждение о противоправной деятельности хакеров, защита гражданских прав и свобод человека; быстрое реагирование на факт, случившегося преступления и выявление личности преступника.

В России расследованием и раскрытием преступлений такого характера занимается МВД и его следующие подразделения:

- Управление «К» (кибербезопасность) – особое подразделение МВД РФ, в пределах своей компетенции занимается выявлением, предупреждением, пресечением и раскрытием преступлений в сфере компьютерной информации; преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и направленных против здоровья несовершеннолетних и общественной нравственности; преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации [2].
- Главное управление экономической безопасности и противодействия коррупции (ГУЭБиПК МВД России), обеспечивающее и осуществляющее в пределах своей компетенции:

– правоприменительные полномочия в области обеспечения экономической безопасности государства;

– противодействия преступлениям экономической и коррупционной направленности.

В-третьих, осведомление пользователей о видах мошеннических действий, возможных схемах действий злоумышленников, названиях компаний-мошенников, а также о мерах предосторожности и защиты.

В нашей стране уже делаются попытки по созданию программного обеспечения, которое смогло бы бороться с данным видом правонарушений или вовсе предотвращать возникновение самого факта преступления.

В-четвертых, обеспечить дополнительную защиту счетов и банковских карт, обучить людей финансовой грамотности. Одним из примеров повышения финансовой грамотности общества, является «Стратегия повышения финансовой грамотности в Российской Федерации на 2017-2023 годы», утвержденная Правительством Российской Федерации от 25.09.2017 г.

Таким образом, можно сделать вывод, что решение проблем, связанных с мошеннической деятельностью в сети Интернет, должно быть одной из первостепенных и неотложных задач на повестке современного аппарата управления государством. Требуется не только совершенствование существующей нормативно-правовой базы, регулирующей отношения, возникающие в сети Интернет, но и наращивание технических мощностей, а также привлечение высококвалифицированных специалистов для поиска новых возможностей, решений и путей нивелирования угроз, выступающих перед государством в связи с возрастающим количеством преступлений, совершаемых при помощи информационно-телекоммуникационных технологий и сетей. Требуется выстроить полноценное взаимодействие специалистов в области юриспруденции, управления и технологического обеспечения, путем формирования площадок для их совместной работы.

Библиографический список:

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ
2. Сайт Министерства внутренних дел РФ. URL: https://xn--b1aew.xn--p1ai/ (дата обращения: 09.03.2021)
3. Микаева А.С. Проблемы правового регулирования в сети Интернет и их причины // Актуальные проблемы российского права. – 2016. – № 9. – С. 67-75.
4. Микаева А.С., Рутковская О.А. Правовая природа отношений в сети Интернет и их специфика // Научное обозрение. Серия 1: Экономика и право. – 2016. – № 3. – С. 136 – 142.

References:

1. Criminal Code of the Russian Federation dated June 13, 1996 № 63-FZ

2. Website of the Ministry of Internal Affairs of the Russian Federation. URL: https://xn--b1aew.xn--p1ai/ (date of access: 03/09/2021)

3. Mikaeva A.S. Problems of legal regulation on the Internet and their causes // Actual problems of Russian law. – 2016. - № 9. – P. 67-75.

4. Mikaeva A.S., Rutkovskaya O.A. Legal nature of relations on the Internet and their specifics // Scientific Review. Series 1: Economics and Law. – 2016. – №3. – P. 136 - 142.

Для цитирования: Микаева А.С., Пенчукова Т.А., Совершение мошеннических действий в сети Интернет и их влияние на экономическую безопасность / Российский экономический интернет-журнал. – 2022. – № 1. URL: