УДК 343.72

Аксенов А.А.,
студент 2МЗЮ курса факультета права и управления
Владимирского юридического института
Федеральной службы исполнения наказаний
Россия, г. Владимир
Научный руководитель: Зыков Д.А.,
заведующий кафедрой публично-правовых дисциплин
факультета права и управления Владимирского юридического
института Федеральной службы исполнения наказаний
Россия, г. Владимир

КИБЕРМОШЕННИЧЕСТВО: ПОНЯТИЕ И ПУТИ ПРОТИВОДЕЙСТВИЯ

Аннотация: *Мошенничество – это крайне актуальная проблема, которая требует уточнения и разрешения. Мошенничество в сети Интернет развивается с течением времени и органы противодействия не должны стоять на месте. В данной статье отмечены основные причины совершения мошенничеств в сети Интернет, а также предложены основные пути противодействия кибермошенничеству.*

Ключевые слова: *мошенничество, информационная безопасность, обман, злоупотребление доверием, Интернет, кибермошенничество, киберпреступность, пандемия COVID-19.*

CYBERFRAUD: CONCEPT AND WAYS OF COUNTERACTION

Annotation: *Fraud is an extremely urgent problem that requires clarification and resolution. Fraud on the Internet develops over time and counteraction agencies*

should not stand still. This article highlights the main reasons for committing fraud on the Internet, as well as the main ways to counteract cyber fraud.

Key words: *fraud, information security, deceit, breach of trust, Internet, cyberfraud, cyber crime, COVID-19 pandemic.*

Современный мир меняется необычайно быстрыми темпами, и процессы цифровизации порождают новые угрозы в области кибербезопасности.

В 2020 г., с началом пандемии COVID-19, эти тенденции лишь усилились. Одним из новых явлений в мировом масштабе являются конфликты в киберпространстве и кибератаки на критическую инфраструктуру государств, информационные (гибридные) войны [2, с. 196].

Информационная технология проникает практически во все сферы деятельности общества, что регулярно усугубляет положение информационной безопасности. Обмен информации стал быстрым и эффективным, за счет внедрение новых технологий в нашу жизнь, но из-за этого преступность в информационной сфере становится доступна каждому, что даже переросла за рамки тех понятий, которые обычно существуют для определения преступности.

Об актуальности правового обеспечения информационной безопасности говорят и международные документы. Так, в докладе Европола за 2020 г. киберпреступления обозначены как особо опасные преступления. К ним отнесены:

- разработка вредоносных компьютерных программ.

- кибератаки, в особенности на объекты жизненно важной инфраструктуры тех или иных государств.

- интернет-контент, который касается сексуальной эксплуатации женщин и детей.

- террористические сайты в интернете, в том числе в Даркнете.

- незаконная торговля людьми, оружием, наркотиками, иными запрещенными товарами через сеть интернет.

- отмывания незаконных денежных средств через сеть Интернет.

- шифрование данных преступниками через сеть Интернет.

- кибермошенничества и киберкражи [1, с. 249].

Сегодня мошенничество является одним из самых распространенных видом преступления, оно представляет собой хищение чужого имущества обманом. К сожалению, жертвами мошенников становятся не тысячи, а сотни тысяч людей. Человека цифровые технологии окружают со всех сторон: на работе, дома, в больнице, школе и т.д. Уже сегодня цифровые технологии используют в научных исследованиях, в робототехнике или области медицины и многом другом. Кроме того, они не останавливаются в развитии и охватывают весь мир. Однако есть и «обратная сторона медали».

Мошенничество в сфере электронной коммерции с онлайн-платежами – одно из наиболее распространенных видов мошенничества, которое обозначает любые незаконные онлайн-транзакции, совершаемые киберпреступниками. Жертва, как правило, – онлайн-пользователь, который испытывает следующие типы убытков: потеря денег, процентов, конфиденциальной информации или личного имущества через онлайн-средства.

С увеличением количества онлайн транзакций и неограниченного доступа к интернет-технологиям онлайн-клиенты сталкиваются с множеством рисков для своей личной информации и нарушением политик безопасности.

Процессы цифровизации движутся вперед, электронная коммерция становится неотделимой частью нашей обыденной жизни. При этом так называемая e-commerce все более популяризируется, растут обороты денежных сумм, увеличивается количество операций, что влечет за собой рост киберпреступлений. Эта угроза является огромны препятствием для развития бизнеса еще и в интернет-пространстве.

Повышенное использование криптовалюты также способствует перемещению и отмыванию средств, добытых преступным путем. Растущее использование интернета по всему миру, недостаточная осведомленность пользователей и повышающаяся зависимость от онлайн-коммуникаций снижают возможности по борьбе с кибермошенничеством.

На сегодняшний день среди основных причин кибермошенничества можно выделить следующие [3, с. 74]:

1) недостаточно совершенная законодательная база в области правового регулирования киберпреступности;

2) отсутствие специалистов и специально подготовленных людей, занимающихся расследованием кибермошенничеств;

3) сложность раскрытия преступлений в информационной среде, отсутствие доказательств и улик;

4) отсутствие практического опыта ведения дел по расследованию кибермошенничеств.

Кибермошенничества имеют специфические характеристики, которые осложняют процесс их обнаружения и предотвращения. К таким можно отнести:

• высокую латентность – кибер-мошенники успешно скрывают следы преступлений и долгое время остаются неустановленными;

• преимущественную неосведомленность потерпевших о факте преступного воздействия;

• трансграничность – преступник, потерпевший и объект преступления (например, база данных, банковский счет) могут быть расположены на территориях как разных субъектов страны, так и разных государств;

• автоматизированность преступлений – совершение преступлений возможно в автоматизированном режиме;

• особую подготовленность преступников, интеллектуальный характер преступной деятельности (правонарушители являются экспертами

в IT-технологиях и пользуются слабыми местами в информационных системах, в программном обеспечении);

• невозможность предотвращения и пресечения кибермошенничеств традиционными средствами.

Полагаем, на сегодняшний день необходимо постоянное комплексное правовое воздействие на сферу информационной безопасности, путем ее совершенствования на теоретической и практической основах. В связи с чем считаем необходимым повысить уровень специальных знаний в области информационных технологий следователей. Для этого необходимо создать отдельный отдел по расследованию кибермошенничеств, состоящий из специалистов, которые прошли дополнительные курсы по «Методики расследования компьютерных преступлений». Также в ВУЗах можно ввести обучение такой профессии, как «следователь-программист», чтобы выпускать молодых специалистов узкого профиля, которые бы занимались непосредственно расследованием кибермошенничеств.

В рамках оперативно-розыскной работы в процессе раскрытия и расследования мошенничеств в сети Интернет следует обеспечить:

- приобретение и использование широкого спектра надежных источников информации;

- подбор квалифицированного кадрового состава аналитических подразделений;

- обновление знаний и повышение квалификации аналитиков;

- применение ими самых продуктивных средств и технологий;

- организация надежного сотрудничества с зарубежными правоохранительными органами, поскольку значительное число преступлений совершается с использованием интернет-ресурсов с серверов, физически расположенных на территории иных государств.

Таким образом, как видим, наступление XXI века ознаменовало активное развитие современных информационных технологий,

пронизывающих практически все сферы жизнедеятельности человека. С каждым годом увеличивается число людей, занятых в сфере информационных услуг и коммуникаций, что приводит к использованию информационных технологий в негативном аспекте, а именно для совершения разного рода хищений и иных противоправных действий. Иными словами, цифровизация в широком смысле вызвала активное развитие кибермошенничеств как в Российской Федерации, так и по всему миру.

Подводя итог, отметим, что только совместная и слаженная деятельность правоохранительных органов, а также иных участников информационного пространства в борьбе с кибермошенничеством в настоящее время обеспечит положительный результат в сфере борьбы с указанном видом преступлений. При этом стоит отметить, что данная деятельность должна носить комплексный и регулярный характер, а также взаимодействовать на постоянной основе со специалистами по расследованию кибермошенничеств.

Полагаем, эффективным методом является повышение медиа-грамотности населения, поддержка со стороны государства проектов по развитию самосознания граждан в области потребления информационных данных, а также распространение повесток в медиа-пространстве среди целевой аудитории, особенно молодых людей, потребляющих большее количество контента.

Использованные источники:

1. Ишмухаметов, Я.М. Международное сотрудничество в борьбе с транснациональной киберпреступностью / Я.М. Ишмухаметов, Д.Р. Янмурзин // Право и государство: теория и практика. – 2021. – № 6 (198). – С. 249-251.

2. Касторский, Г.Л. Киберпреступность в период пандемии коронавируса COVID-19 / Г.Л. Касторский, А.Г. Форкош // Молодой ученый. – 2020. – № 52 (342). – С. 196-198.

3. Стеценко, Ю.А. Мошенничество в сети интернет / Ю.А. Стеценко, Н.С. Холодковская // Вестник Таганрогского института имени А.П. Чехова. – 2021. – № 2. – С. 74-79.