вило, преступники совершают деяния, находясь на территории другого государства, с которым отсутствует международное соглашение в сфере оказания правовой помощи в их выявлении и раскрытии.

Как видим, с одной стороны, широкое распространение рассматриваемого хищения обусловлено тем, что благодаря сети Интернет преступники обладают возможностью доступа к значительному числу потенциальных потерпевших, а также доступа к информационным ресурсам организаций, а также финансовых учреждений.

В связи с чем законодателями при введении специальной нормы, предусмотренной ст. 212 УК, соблюден принцип системности, справедливости уголовного закона, так как преступления, совершаемые в сфере информационных технологий, являются более общественно опасными по сравнению с традиционными преступлениями в сфере собственности, предусмотренными ст. 205 «Кража», ст. 209 «Мошенничество» УК.

Обобщая вышеизложенное, следует констатировать тот факт, что необходимость установления уголовной ответственности за хищение имущества путем модификации компьютерной информации связана со спецификой способов и средств совершения таких преступных посягательств против собственности. Кроме того, о повышенной общественной опасности рассматриваемой разновидности хищений свидетельствуют следующие факторы: высокая латентность данных преступлений, транснациональный характер их совершения и объективная сложность доказывания. В связи с чем указанные факты свидетельствуют о необходимости дальнейшего конструирования диспозиции, квалифицирующих и особо квалифицирующих признаков рассматриваемой уголовно-правовой нормы с целью эффективного противодействия преступлениям, совершаемым в данной сфере.

1. Гриб, Д.В. Социальная обусловленность норм уголовного законодательства Российской Федерации и Республики Беларусь, предусматривающих ответственность за хищения, совершаемые с использованием информационных технологий / Д.В. Гриб // Евраз. адвокатура. – 2019. – № 2 (39). – С. 74–78.

2. Лопашенко, Н.А. Уголовная политика : монография / Н.А. Лопашенко. – М. : Волтерс Клувер, 2009. – С. 579.

3. Епифанова, Е.В. Общественная опасность как научная категория, законодательная дефиниция: история и современность : монография / Е.В. Епифанова. – М. : Юрлитинформ, 2012. – С. 189.

4. Дмитренко, А.П. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий / А.П. Дмитренко, Е.А. Русскевич // Вестн. Акад. Генер. прокуратуры Рос. Федерации. – 2017. – № 5 (61). – С. 18–22.

УДК 343.985

Н.С. Делов

ПРОБЛЕМЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Интернет активно используется каждым пользователем. Данная среда служит для обеспечения доступа к различным информационным ресурсам и системам. С каждым годом интернет все больше проникает в жизнь обычных людей, и это неудивительно. Ведь с помощью него можно обмениваться сообщениями с людьми, которые находятся на дальнем расстоянии от вас, можно найти необходимую информацию, решать производственные вопросы и приобретать необходимые товары и услуги.

Но есть и обратная сторона. Чем больше интернет проникает в нашу жизнь, тем больше появляется интернет-мошенничества, способов их совершения, и тем больше они становятся разносторонними. Стоит также отметить, что данный вид мошенничества является латентным, т. е. скрытым. Ведь он исключает непосредственный контакт с жертвой, данные о преступнике неизвестны, его место расположения, ник-нейм. Учитывая эти факторы, мошенники создают свой бизнес, основанный на обмане, и получают в дальнейшем огромные доходы с доверчивых граждан [1, с. 55].

В ходе раскрытия и расследования уголовных дел, которые связаны с использованием сети Интернет, возникают различные трудности, а именно:

установление личности преступника;

неизвестность его местонахождения;

использование скрытых айпи-адресов;

использование данных другого человека, непричастного к совершению преступления.

Исходя из этого, анализ правоприменительной практики показывает, что чаще всего совершаются следующие преступления:

хищение информации путем использования вирусов, которые ломают систему и позволяют изъять необходимую для преступника информацию;

неправомерный доступ к охраняемой законом компьютерной информации, в том числе базы данных правоохранительных органов;

использование внушения и злоупотребления доверием со стороны граждан и получение от них необходимой информации о банковских счетах, денежных средствах, и даже личной информации.

Как видим, преступники используют различные способы мошенничества и схемы обмана, что приводит к внесению корректировок в уголовный закон. Так, Федеральный закон Российской Федерации от 23 апреля 2018 г. № 111 «О внесении изменений в Уголовный кодекс Российской Федерации» внесены изменения в ст. 159.3 и 159.6, связанные с противоправными действиями преступников с электронными денежными средствами граждан [2].

У данных противоправных действий также есть свои распространенные способы, такие как:

рассылка различных спам-SMS, таких как о выигрыше автомобиля, от банковских служб, якобы о противоправно взятом кредите на имя лица, также использование социальных сетей. Взламывая аккаунты, начинают писать от имени друзей, что произошла тяжелая жизненная ситуация и необходимы срочно денежные средства;

создание интернет-сайтов, интернет-магазинов. При осуществлении заказа и после оплаты сайт блокируется и уже нельзя обнаружить его или написать в службу поддержки, банковский счет, на который были отправлены денежные средства, уже не существует, либо был использован интернет-кошелек. Примером такого рода мошенничества служит продажа товара через сайты «Авито», «Юла»;

звонки и представление от лица сотрудников банка, которые под предлогом проверки или убеждения лица, что на него был взят кредит мошенниками, далее просят перевести денежные средства таким способом, что лицо самостоятельно диктует данные своего банковского счета, говорит ключевые фразы «ДА», «СОГЛАСЕН» и переводит денежные средства под предлогом закрытия кредита и после возврата этих же денежных средств.

Мошенничество в глобальной компьютерной сети Интернет может производиться и другими способами. Так, мошенники могут создавать интернет-банки или же специальные мнимые вклады, затем обещают, что при минимальном взносе и за короткий срок вам удастся удвоить, или даже утроить вносимую сумму. Услуга интернет-казино может также предоставляться. За минимальную сумму вам могут предоставить большой шанс выигрыша, но в итоге вы вовсе останетесь без денежных средств [3, с. 156].

Процесс сокрытия следов в данном случае проявляется в том, что мошенники изначально не оставляют никаких данных о себе, ни номер технической поддержки, ни факс, ни адреса электронной почты. Все сделки совершаются исключительно по предварительной оплате, если мошеннический сайт получает большую сумму денег, он и вовсе перестает существовать.

Данные способы совершения преступления в сети Интернет имеют свои особенности механизма следообразования. Этот механизм проявляется в том, что при совершении мошенничества в сети Интернет почти отсутствуют следы идеального характера. Это обусловлено тем, что потерпевший не контактирует со злоумышленником в реале, а весь процесс обмена информацией происходит через интернет. Исключением может служить только заказ какой-либо продукции через мошеннические интернет-магазины, в этом случае потерпевший может запомнить внешний вид курьера и сможет описать его внешность. Будет также объект преступления – посылка. Можно увидеть кем она отправлялась, адрес отправки, дату [4, с. 54–62].

Исходя из перечисленной выше информации, можно сделать вывод, что из-за постоянного развития интернет-ресурсов будут появляться различные способы интернет-мошенничеств. Но, несмотря на это, ведется и активное изучение данной проблемы с правоприменительной стороны. Создаются дополнительные ресурсы для изобличения лиц, совершающих подобного рода преступления, вносятся корректировки в законодательство. Именно поэтому представители закона, как и сеть Интернет, делают все возможное для изобличения преступников.

1. Харламов, Д.Д. Уголовная ответственность за компьютерное мошенничество по УК Российской Федерации и ФРГ / Д.Д. Харламов // Бизнес в законе. – 2021. – С. 55–59.

2. О внесении изменений в Уголовный кодекс Российской Федерации [Электронный ресурс] : Федер. закон Рос. Федерации, 23 апр. 2018 г., № 111-ФЗ. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_296451/. – Дата доступа: 14.10.2022.

3. Журавлева, Г.В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики / Г.В. Журавлева, Н.А. Карпова // Вестн. Моск. ун-та МВД России. – 2017. – № 5. – С. 153–158.

4. Александрова, И.А. Новое уголовное законодательство о мошенничестве / И.А. Александрова // Юрид. наука и практика. Вестн. Нижегор. акад. МВД России. – 2013. – № 21. – С. 54–62.

УДК 343.98

Е.Г. Котова

ОСОБЕННОСТИ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ В ХОДЕ БОЕВЫХ ДЕЙСТВИЙ

Актуальность данной темы вызвана прежде всего тем, что за последние 35 лет участились случаи вооруженных конфликтов в непосредственной близости от территориальных границ Российской Федерации, а в