



УДК 342

**КИБЕРПРЕСТУПЛЕНИЯ И ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:
ПРОБЛЕМЫ РАССЛЕДОВАНИЯ**

Лукашова София Леонидовна

студент

Аленевская Анна Сергеевна

преподаватель

Колледж права имени Н.С. Киселевой,

Россия, г. Москва

Аннотация. В последние годы резко возросло число преступлений в цифровой сфере, особенно в экономике, а также мошеннических схем с использованием мобильной связи. Ущерб от таких деяний колоссален, что свидетельствует о серьезной угрозе личным правам граждан и экономике страны. Однако раскрываемость остается крайне низкой из-за специфических особенностей: анонимности, трансграничности и автоматизированности. Статья посвящена классификации киберпреступлений, анализу статистики, проблемам расследования и мерам профилактики.

Ключевые слова: киберпреступность, фишинг, социальная инженерия, цифровые доказательства, кибертерроризм.

CYBERCRIME AND TELEPHONE FRAUD: INVESTIGATION CHALLENGES

Lukashova Sofia Leonidovna

student

Alenevskaya Anna Sergeyevna

lecturer

N.S. Kiseleva College of Law,

Moscow, Russia

Abstract. In recent years, there has been a sharp increase in crimes within the digital sphere—particularly in the economic sector—as well as in fraudulent schemes involving mobile communications. The financial losses resulting from such acts are immense, indicating a serious threat to citizens' personal rights and the national economy. However, case clearance rates remain extremely low due to specific characteristics of these crimes: anonymity, their cross-border nature, and automation. This article addresses the classification of cybercrimes, statistical analysis, investigation challenges, and preventive measures.

Keywords: cybercrime, phishing, social engineering, digital evidence, cyberterrorism.



ВВЕДЕНИЕ

Стремительная цифровизация изменила структуру общества, создав не только новые возможности, но и новые угрозы. Преступники действуют дистанционно, атакуя граждан, корпорации и государства. Многие традиционные преступления перешли в интернет, где их расследование значительно сложнее. Яркий пример глобальной угрозы - атака вируса WanaCrypt0r 2.0 в мае 2017 года, заразившая более 75 тысяч устройств в 99 странах.

Понятие и особенности киберпреступлений

Киберпреступление - это деяние в электронной сфере, направленное на несанкционированное проникновение в компьютерные сети, программы и устройства с целью хищения, модификации или подмены данных. Объектом посягательства выступают общественные отношения в сфере безопасного создания, хранения и передачи компьютерной информации.

Ключевые особенности:

- скрытность - использование шифрования и анонимных сетей;
- трансграничность - преступник и жертва в разных странах, что мешает юрисдикции;
- нестандартность методов - крупные атаки уникальны;
- автоматизация - многие процессы автоматизированы.

Эти свойства делают киберпреступления одними из наименее раскрываемых. Ситуацию осложняет кадровый дефицит: 95% следователей имеют только юридическое образование, лишь 5% - дополнительное ИТ.

Классификация

По цели и способу совершения выделяют четыре группы:

1. Против собственности - несанкционированный доступ к данным.
2. Нарушение авторских и смежных прав в РФ уголовно наказуемо.
3. Манипуляции с данными - подлог, хищение, блокировка.
4. Тяжкие деяния - кибертерроризм, распространение наркотиков, порнография, теневые рынки.

Статистика и способы совершения

В России число киберпреступлений растет на 10% ежегодно. По данным Генпрокуратуры, в 2018 году ущерб достиг 400 млрд рублей, а число зарегистрированных преступлений выросло на 44% по сравнению с 2017 годом. За 2015–2016 годы со счетов банков похищено 348,6 млн рублей - в пять раз больше, чем годом ранее.

Наиболее распространен метод социальной инженерии - психологического манипулирования людьми. Он не требует высоких технических навыков и включает:



- Фишинг - массовые рассылки от имени банков с переходом на поддельные сайты.
- Фарминг - перенаправление пользователей на ложные IP-адреса для имитации надежных сайтов.
- Кибероружие - вредоносное ПО для вывода из строя инфраструктуры.

Кроме того, активно действуют киберпорнография, наркоторговля, кибертерроризм и теневые рынки, где продаются похищенные данные и паспорта.

Преступления по телефону

Отдельную группу составляют мошенничества через звонки, СМС и мессенджеры. Их цель - хищение денег. Злоумышленники подменяют номера (например, «900» Сбербанка) и используют социальную инженерию. Типичные сценарии: сообщения о «выигрыше», просьбы о помощи от «родственников в беде», шантаж. Жертвами чаще становятся люди старше 40 лет, плохо ориентирующиеся в новых схемах. Характерна серийность - редко ограничиваются одним эпизодом.

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ

В 53% случаев проверка сообщений начинается спустя 10 дней после инцидента. Главные препятствия:

- анонимность в сети (VPN, прокси, неперсонифицированные карты);
- сложность обыска и выемки цифровых устройств - требуются узкопрофильные специалисты;
- нехватка квалифицированных кадров - привлечение неэкспертов ведет к потере следов.

В России организованы курсы повышения квалификации следователей, специализирующихся на киберпреступлениях, перенимается международный опыт.

ВЫВОДЫ

Киберпреступность прогрессирует вместе с технологиями. Основные препятствия на пути правосудия - анонимность, техническая сложность и дефицит специалистов. Для эффективного противодействия необходимы: постоянный мониторинг, совершенствование законодательства, повышение цифровой грамотности населения и подготовка кадров. Дальнейшие исследования крайне актуальны, так как методы преступников постоянно эволюционируют.

Список литературы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.07.2016)
2. Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. – 2018. – № 1. – С. 135-137.
3. Арзамасцев М.В. К вопросу об уголовно-правовой классификации киберпреступлений // Актуальные вопросы права и отраслевых наук. – 2017. – № 1 (3). – С. 11-16.



4. Кочкина Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3 (17). – С. 162-169.
5. Захаров Д.Н., Щерба В.В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. – 2017. – № 2(20). – С. 72-76.