# ОСОБЕННОСТИ КИБЕРПРЕСТУПНОСТИ

**Евгений Владимирович С.**

слушатель Санкт-Петербургского Университета МВД России, РФ, г. Санкт-Петербург

**Аннотация.** В статье рассматривается состав и методы киберпреступности, особенности противостояния киберпреступности, подчеркиваются опасность использования сети Интернет для распространения наркотиков и сложности борьбы с таким распространением из-за существования DarkNet, Telegram и криптовалют.

**Ключевые слова:** киберпреступность, фишинг, хакинг, распространение наркотиков через сеть Интернет, DarkNet, Telegram, криптовалюты.

Киберпреступность - это незаконная деятельность, которая происходит в киберпространстве, то есть в сети Интернет. Киберпреступность объединяет различные виды преступлений, такие как: кража, мошенничество, вымогательство, посягательства на авторские права и личную безопасность (особо опасны лица, склоняющие других лиц к преступлениям или суициду), распространение порнографических материалов, сбыт наркотических и психотропных средств, оружия, нарушение функционирования компьютерных сетей и оборудования, вовлечение несовершеннолетних в преступную деятельность, экстремизм и т.д.

К наиболее часто встречающимся проявлениям киберпреступности относятся:

- кража личных данных - преступник получает доступ к личной информации, такой как номера социального страхования, номера кредитных карт или пароли, и использует эту информацию для своих целей.

- распространение вредоносных программ - злоумышленник создает и распространяет программы, которые могут нанести вред компьютеру или сети. Это может привести к потере данных, нарушению работы системы или даже к ее уничтожению.

- мошенничество с электронными платежами - преступник использует украденные данные кредитных карт или другие методы для совершения незаконных платежей.

- нарушение авторских прав - злоумышленник копирует, распространяет или использует без разрешения материалы, защищенные авторским правом, такие как музыка, фильмы, книги или программное обеспечение.

Противостоять киберпреступности сложно вследствие того, что технические и программные средств постоянно развиваются, повышается уровень знаний, умений и навыков киберпреступников и все это требует особой подготовки сотрудников правоохранительных органов, которые также должны постоянно повышать свою техническую квалификацию. Для киберпреступности характерна высокая общественная опасность (поскольку через сеть Интернет сбываются наркотики и оружие), латентность, высочайший уровень оперативности, удаленность преступников (нахождение многих из них за рубежом), высокая анонимность.

Нужно отметить, что глава 28 УК РФ, которая направлена на противодействие

киберпреступности охватывает узкий диапазон подобного рода преступлений:

- неправомерный доступ к компьютерной информации – преступление небольшой или средней тяжести;

- создание, использование и распространение вирусов – преступление небольшой или средней тяжести;

- нарушение правил эксплуатации компьютерных сетей - преступление небольшой тяжести или средней тяжести;

- неправомерное воздействие на критическую инфраструктуру - преступление небольшой тяжести или средней тяжести;

- технические нарушения, описанные в статье 274.2 УК РФ - преступление небольшой тяжести [1].

Незначительные наказания за подобного рода киберпреступления не могут сдерживать желающих нарушить закон. Наказание следует ужесточить путем перевода такого рода преступлений в категорию тяжких.

Киберпреступники используют различные методы для достижения своих целей. Например, они могут создавать фишинговые сайты, которые выглядят как настоящие, чтобы получить доступ к личным данным пользователей. Они также могут использовать вредоносные программы, чтобы получить доступ к компьютерам и украсть конфиденциальную информацию.

Существенная проблема для правоохранительных органов заключается в том, что киберпреступники могут нарушать закон из любой точки мира, кроме того, они часто используют анонимные сети и другие методы, чтобы скрыть свою личность. Есть еще один фактор, затрудняющий противодействие киберпреступности – криптовалюты, которые не позволяют проследить транзакции и выявить заказчика.

Одной из наиболее значимых проблем для общества в связи с киберпрестпуностью является сбыт наркотических средств (в 2022 году из 177,7 тысячи зарегистрированных наркопреступлений 82,7 тысячи (46,5 процента) были совершены с использованием IT-технологий [2]):

- посредством мессенджера Telegram;

- в магазинах DarkNet, попасть в которые можно через специальный браузер TOR. Сеть DarkNet - это часть интернета, которая не индексируется поисковыми системами и часто используется для анонимного обмена информацией, торговли товарами и услугами, которые могут быть незаконными или контролируемыми. В DarkNet часто используется шифрование и анонимизация, что делает пользователей трудноидентифицируемыми.

Расцвет торговли наркотиками в сети Интернет возник после начала использования криптовалют, чаще всего, биткоинов. Криптовалюты позволяют скрыть как плательщика, так и получателя платежа.

Торговля в Telegram осуществляется посредством специализированных каналов и ботов. В каналах может распространяться информация о ботах, которые настроены на выдачу информации о платеже, а затем выдачи информации о месте нахождения закладки.

Рекламируют такие каналы часто так называемые наркоблогеры. Наркоблогеры, как правило, действующие наркоманы, которые делятся информацией о наркотиках на своих каналах.

Трудности в установлении интернет-магазинов и площадок, предлагающих незаконные услуги в сфере незаконного оборота наркотиков, и их закрытии заключаются в том, что интернет-хостинги зачастую находятся за границей, и, даже если сотрудники правоохранительных

органов предпринимают меры для их закрытия, через некоторое время открываются новые интернет-магазины. Если их блокирует Роскомнадзор, на следующий день они открываются по новому адресу и продолжают заниматься преступной деятельностью.

Расследование преступлений, связанных с незаконным оборотом наркотиков с использованием информационных технологий затруднено сложностью этих технологий, невозможностью освоить эти технологии большей частью следователей, поскольку фактически, это инженерная специальность, и постоянным усовершенствованием этих технологий.

Кроме того, современные информационные технологии постоянно повышают требования к своему освоению, в первую очередь, временные - современные технологии требуют значительного времени для их изучения.

Т.О. Чистанов предлагает: «в качестве обеспечения эффективного расследования преступлений указанной группы следует создать подразделение киберпатрулирования», обеспечивающих мониторинг подозрительных сайтов, сетей, интернет-магазинов, изучение отзывов и иных сообщений граждан в сети интернет [3].

А.М. Ишин отмечает: «интернет—мониторинг является одним из перспективных направлений оперативного поиска в сети интернет» [4].

Чтобы отследить деятельность киберпреступников в целом, и наркопреступников в частности, используется интернет-мониторинг социальных сетей, мессенджеров и пр. и затем пользуются традиционными методами, например, наблюдением, когда устанавливается, например, отсутствие в сети конкретного человека, потому что он, куда-либо вышел: его выход фиксирует наружная служба наблюдения, а затем просто сопоставляется время сессии человека в сети.

Иногда преступники могут быть обнаружены, если участвуют в деятельности сторонних сайтов, например, общаются на форумах или в социальных сетях. Из сетевой беседы можно получить какую-либо ценную информацию.

Также практикуется и работа под прикрытием, когда полицейские агенты на время становятся участниками незаконного рынка и входят в доверие к преступникам, что в итоге приводит к арестам последних.

Кроме аналитики, существует эффективность работы СОРМ (система техсредств для оперативно-розыскных мероприятий), относящихся к деятельности спецслужб. На сегодня в России уже есть разработки, позволяющие выделять и расшифровывать интернет-трафик мессенджера Telegram. При соединении систем фиксации интернет-трафика, входящих в СОРМ, с возможностью выделения и расшифровки сообщений Telegram задача борьбы с анонимностью мессенджера будет решена в принципе.

В целом существует общая проблема в расследовании преступлений с использованием информационных технологий: техническая неготовность работников ОВД к работе в сети Интернет, фактически, требуются в настоящее время в ОВД именно технические специалисты для противодействия преступникам, подготовить же большое количество технических специалистов для ОВД проблематично, кроме того, существуют и ограничения по численности сотрудников.

**Список литературы:**

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 23.03.2024) (с изм. и доп., вступ. в силу с 01.04.2024) — Текст: электронный // КонсультантПлюс [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 24.03.2024).

2. Генерал МВД рассказал о победе над «Гидрой» из даркнета  — Текст : электронный //

Lenta.ru [сайт]. — URL: https://lenta.ru/news/2023/08/22/narco/ (дата обращения: 24.03.2024).

3. Ишин А.М. Современные проблемы использования сети Интернет в расследовании преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки. – 2013. – № 9. С. 121.

4. Чистанов Т.О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств // Международный научно-исследовательский журнал. – 2016. – № 11. С.88.