

Сапченко А.С.  
студент магистратуры  
2 курс, Юридический институт  
Севастопольский государственный университет  
Россия, г. Севастополь

## СПОСОБЫ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ ПРИМЕНИТЕЛЬНО К ИХ ВИДАМ

***Аннотация:** автором статьи приведено понятие киберпреступности, рассмотрены виды преступлений в сфере информационных технологий и способы совершения преступлений в рамках каждого вида. Изучены способы сокрытия следов преступником, затрудняющие его идентификацию. Проанализирован ущерб, причиняемый компьютерными преступлениями, и даны рекомендации по борьбе с изучаемым видом преступности.*

***Ключевые слова:** киберпреступления; компьютерные атаки; конфиденциальные данные; кибермошенничество; кибервымогательство; вредоносные программы; кибертерроризм.*

***Abstract:** The author of the article gives a concept of cybercrime, considers types of crimes in the sphere of information technology and ways of committing crimes within each type. The ways of concealing traces by the criminal, making it difficult to identify him, are studied. The damage caused by computer crimes is analyzed and recommendations are given for combating the type of crime under study.*

***Keywords:** cybercrime; computer attacks; confidential data; cyber fraud; cyber extortion; malware; cyber terrorism.*

Активное развитие информационных технологий и внедрение их в повседневную жизнь людей неизбежно привело к формированию нового вида преступности: киберпреступность [1, с. 227]. Под киберпреступностью можно понимать совокупность противоправных действий, совершаемых в киберпространстве, где информационные ресурсы и техника могут выступать либо как предмет преступного посягательства, либо как средство реализации преступного умысла, либо как область, в которой совершаются противозаконные деяния [2, с. 47].

Рассматриваемая форма преступности с течением времени начинает представлять все большую угрозу, поскольку арсенал действий сотрудников правоохранительных органов по идентификации личности преступника значительно ограничен, ведь грамотное использование специалистом компьютерных технологий обеспечивает практически полную анонимность в информационной сфере. Таким образом, преступления, совершаемые с применением телекоммуникационных сетей, обладают высокой латентностью, так как не оставляют практически никаких следов.

Интерес представляют виды компьютерных преступлений, поскольку каждый из этих них может использовать уникальные способы реализации, требующие творческого подхода. Так, можно выделить:

- компьютерные атаки – взлом компьютерных систем и сетей, влекущий неправомерное получение доступа к чужим базам данных и нарушение конфиденциальности и целостности содержащейся в них информации. К способам проведения таких атак можно отнести взлом пароля, когда злоумышленник пытается угадать или восстановить пароль путем использования подбора возможных комбинаций или обмана пользователя; фишинг – обманное электронное письмо, целью которого является получение личной информации адресата; DDOS-атаки, которые искусственно перезагружают сервер огромным потоком запросов, что влечет его

недоступность; инъектирование SQL-кода – то есть внедрение SQL-запросов в формы приложения для получения доступа к базе данных;

- кража конфиденциальных данных – незаконное завладение чужими логинами, паролями, номерами банковских счетов и иной персональной информацией, которая в дальнейшем может использоваться для мошенничества или быть продана на «черном рынке». Осуществляется, как правило, посредством компьютерной атаки. Объектом преступного посягательства являются личные данные пользователей или конфиденциальная информация компаний;

- кибермошенничество – обман пользователей сети «Интернет» с целью хищения личных и финансовых данных жертв. Сюда относятся фишинг, поддельные платежные системы, мошенничество с банковскими картами и т.д. Активно применяется социальная инженерия [3, с. 134]. Как правило, основной целью кибермошенничества выступает получение финансовой выгоды. Достаточно интересной особенностью является то, что данный вид компьютерных преступлений чаще всего осуществляется именно группой людей, а не одним человеком, и в качестве жертв обычно выступают представители малого бизнеса. Для распространения мошеннических схем используются электронная почта и социальные сети;

- кибервымогательство – требование выплатить определенную сумму денег или совершить то или иное действие под угрозой совершения компьютерной атаки или распространения порочащих сведений о жертве в случае отказа [4, с. 294]. Можно выделить несколько видов угроз в рамках кибервымогательства: шифрование или уничтожение данных, разглашение конфиденциальной информации, отключение компьютерных систем и ресурсов. Для реализации угрозы злоумышленник использует, как правило, вредоносное ПО, заражающее компьютер жертвы. Свои требования преступник передает либо через электронную почту, либо через социальные сети, а сумма, запрашиваемая в качестве выкупа, может быть очень велика;

- распространение вредоносных программ – создание и распространение программного обеспечения, предназначенного для нанесения ущерба зараженной компьютерной системе или перехвата контроля над ней. К таким программам относятся вирусы, трояны, черви, шпионское ПО и т.д. [5, с. 93-94]. Распространяются они через электронную почту, USB-накопители, загрузки с торрентов и другие источники. Нередко используются не только с целью получения финансовой выгоды, но и для самосовершенствования и развития своих способностей в использовании информационных технологий;

- кибертерроризм – использование информационных и коммуникационных технологий для распространения страха с политической, религиозной или идеологической целью. В качестве цели может выступать нанесение ущерба критической инфраструктуре. Для осуществления используются DoS- и DDoS-атаки, взломы сайтов, заражение систем вирусами и червями, фишинговые атаки и кража данных.

Компьютерные атаки в данном случае используются как более обобщающий термин, включающий в себя различные способы взлома компьютерных систем и получения несанкционированного доступа. Кибермошенничество – более узкая категория, ориентированная исключительно на извлечение прибыли. Кража конфиденциальных данных предполагает получение доступа к конкретному типу информации, а целью может выступать не только получение денежной выгоды, но и нанесение репутационного ущерба. Кибервымогательство схоже с кибермошенничеством в том плане, что преследует корыстную цель, однако различается способ достижения этой цели – использование угроз в отношении жертвы, а не введение ее в заблуждение. Распространение вредоносных программ как вид часто может иметь нейтральную цель: хакерские эксперименты. Кибертерроризм же может быть направлен против критической инфраструктуры. Все перечисленные виды используют схожие методы и нередко переплетаются между собой, поэтому в основе

разграничения лежит направленность преступного умысла. Важно отметить, что существуют и другие виды компьютерных преступлений.

Область преступлений в сфере компьютерной информации интересна своей новизной и творческим подходом со стороны преступников. Так, например, этому виду преступлений присуща инновационность, поскольку непрекращающееся совершенствование систем безопасности заставляет киберпреступников придумывать новые способы обмана и взлома, что нередко требует смекалки и нестандартное мышление. Помимо этого, можно выделить технологичность как один из аспектов киберпреступлений, ведь для реализации всех вышеописанных способов на практике необходимы глубокие знания в области информационных технологий, программирования и сетевой безопасности. Ну и, разумеется, преступлениям в сфере компьютерной информации присуща уникальность, ведь каждое компьютерное преступление имеет свою оригинальную составляющую, позволяющую обмануть системы защиты, – используются нестандартные техники и уловки.

Также преступниками используется ряд средств для сокрытия совершенных противозаконных действий. Среди них выделяются следующие:

1. Использование анонимных средств. Действия киберпреступников сложно отследить во многом из-за того, что они скрывают свой IP-адрес и настоящую личность с помощью VPN, прокси-серверов, анонимных сетей Tor и I2P [6, с. 12];

2. Удаление журналов системы и программ. Злоумышленники, как правило, чистят записи в системных журналах, журналах приложений, базах данных и других местах хранения следов своей деятельности. Также возможна фальсификация журналов и программного обеспечения систем безопасности путем внесения в них ложных данных;

3. Использование вредоносного ПО. Область применения вредоносных программ достаточно широка, что позволяет их использовать не только для реализации преступного умысла, но и для сокрытия следов;

4. Шифрование и стенография. Преступники могут шифровать перехваченные и скачанные данные, применять стенографию для их сокрытия в изображениях, аудио- и видеофайлах;

5. Применение криптовалют. Использование криптовалют позволяет маскировать незаконные финансовые потоки и средства, полученные преступным путем, так как отслеживание таких транзакций крайне затруднительно;

6. Уничтожение и повреждение носителей информации. Цифровые носители, которые содержат информацию, способную помочь в идентификации преступников, могут быть уничтожены или повреждены, что влечет утрату записанной на них информации.

Из такого разнообразия методов сокрытия следов преступного деяния и вытекает высокая латентность преступлений в сфере компьютерной информации. Усугубляет ситуацию то, что опасность этих преступлений происходит не только из их латентности. В первую очередь, они имеют огромный масштаб, поскольку кибератаки могут затрагивать миллионы пользователей, компаний и даже критическую инфраструктуру государств. Утечки данных, кибервымогательство и нарушение стабильной работы предприятий могут повлечь значительный экономический ущерб. Вместе с тем успешные атаки неизбежно приводят к подрыву доверия населения, в данном случае – к цифровым сервисам и электронной коммерции. Также возможно манипулирование общественным мнением путем грамотного использования преступником социальных сетей и мессенджеров для распространения ложной информации. И самое главное, компьютерные преступления несут угрозу национальной безопасности, ведь серьезные кибератаки способны подорвать работу энергетики, транспорта, финансовых институтов и военных систем [7, с. 449].

В целом, для снижения процента совершаемых компьютерных преступлений на уровне всего государства рекомендуется следующее:

повышать киберосведомленность граждан; инвестировать в киберразведку; использовать новейшие технологии; улучшить механизмы обмена информацией [8, с. 216]; актуализировать уголовное и административное законодательство; усовершенствовать системы международного взаимодействия.

Таким образом, проблематика преступлений в сфере компьютерной информации остра и актуальна, а глубокое изучение способов совершения этих преступлений способствует выработке эффективных методов борьбы с ними. Тем самым, для обеспечения надлежащего уровня кибербезопасности необходимо в полной мере осознавать угрозу, которую представляет инструментарий современного киберпреступника.

#### **Список литературы:**

1. Крайнова Н.А. Проблема кибербезопасности общества в криминологическом осмыслении // Право и государство: теория и практика. – 2023. – № 2 (218). – С. 227-229.
2. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – №1(24). – С. 45-55.
3. Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве // Вестник Удмуртского университета. Социология. Политология. Международные отношения. – 2022. – №1(6). – С. 133-138.
4. Чурсина А.Д. Кибервымогательство и угрозы в социальных сетях // Вестник Московского университета МВД России. – 2022. – № 5. – С. 294-296.
5. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. – 2019. – № 3(148). – С. 87-99.

6. Назаров Л.Н., Низаева С.Р. Способы совершения преступлений в сфере компьютерных технологий // Актуальные проблемы права и государства в XXI веке. – 2020. – № 1(12). – С. 11-15.
7. Запорожец С.А., Крайнова Н.А. К вопросу о противодействии киберпреступности в условиях новой геополитической реальности // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2023. – Т. 9 (75). – С. 448-456.
8. Крайнова Н.А. Некоторые аспекты противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 210-216.