Канунникова Н.Г.,

кандидат юридических наук, доцент
Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России (г. Нальчик)

К вопросу о киберпреступности в контексте социологического понятия девиантности

Киберпреступность, являясь одной из форм девиантного поведения, представляет собой комплекс противоправных деяний, которые стали возможны благодаря широкому проникновению цифровых технологий в нашу жизнь. Это не только преступления, непосредственно связанные с компьютерами, но и любые правонарушения, совершаемые в киберпространстве, чему способствуют повсеместный доступ к интернету, использование умных устройств и развитие новых технологий. Спектр киберпреступлений весьма разнообразен и включает в себя такие деяния, как хищение персональных данных, мошенничество в сети, нарушение интеллектуальной собственности, несанкционированный взлом систем, распространение вредоносного ПО (включая вирусы и DDoS-атаки), массовую рассылку нежелательной почты (спам), фишинг, создание и распространение материалов с детской порнографией, а также преследование и травлю в интернете (кибersталкинг и кибербуллинг).

В рамках комплексного междисциплинарного подхода современные исследователи киберпреступности уделяют особое внимание новым и актуальным проблемам: от использования инновационных методов хранения данных для совершения преступлений в киберпространстве (включая кражу криптовалюты) до влияния социальных сетей на рост киберпреступности и использования сетевого фактора в кибертерроризме. Также изучается поведение жертв и преступников в цифровой среде, разрабатываются стратегии и инструменты для обеспечения кибербезопасности и защиты инфраструктуры от киберугроз[1].

Высокая прибыльность и низкий уровень риска делают киберпреступность привлекательным видом криминальной деятельности. Именно поэтому, на фоне общего снижения уличной и насильственной преступности в мире и России, криминал не исчез, а активно осваивает виртуальное пространство. Интернет стал для него благоприятной средой, где принцип неотвратимости наказания практически не работает. В

[1] Cybercrime: interdisciplinary approaches to cutting crime and victimisation in cyber space. URL: http://www.newworldencyclopedia.org/entry/Cybercrime (дата обращения: 23.08.2025 г.)

результате ущерб от киберпреступлений продолжает стремительно увеличиваться.

Признавая киберпреступность как один из наиболее критических глобальных рисков на Всемирном экономическом форуме в 2018 году, эксперты оценили ежегодные потери мировой экономики от нее в 500 миллиардов долларов. Эта сумма сопоставима с годовым ВВП Швейцарии (659 миллиардов долларов в 2017 году). В ответ на эту серьезную угрозу в Давосе было объявлено о создании Глобального центра кибербезопасности. Его ключевая цель – учредить первую международную платформу для совместной работы правительств, бизнеса, специалистов и правоохранительных органов, направленную на преодоление вызовов в сфере кибербезопасности[1].

За тридцать лет, прошедших с момента появления персональных компьютеров, мир столкнулся с новой глобальной угрозой – массовой киберпреступностью. Изучение российских и зарубежных данных позволяет выделить ключевые особенности современной кибердевиантности и преступности:

1. Информационная сфера все больше страдает от девиаций и преступлений. Легкость получения несанкционированного доступа к данным открывает широкие возможности для незаконного обогащения и недобросовестной конкуренции. Под угрозой оказываются патенты на инновационные продукты, секреты фармацевтических разработок, маркетинговые стратегии компаний и их финансовые ресурсы. Киберпреступность становится все более изощренной и трудноуловимой. Например, в Европе каждый десятый покупатель, желая сэкономить на лекарствах, обращается к онлайн-магазинам, где 90 % предлагаемых препаратов – подделки. Это напрямую связано с тем, что преступники получают доступ к конфиденциальной информации фармацевтических компаний.

2. Незаконное присвоение программных продуктов, достигаемое путем взлома систем защиты и получения несанкционированного доступа к базам данных и серверам разработчиков ПО и аппаратных устройств, представляет собой форму девиантного поведения и нелегального обогащения. Показательным примером является случай в Силиконовой долине, где сотрудник компании, занимающейся разработкой операционных систем, смог обойти систему безопасности, используя введенные телефонные номера. Украденная программа привела к многомиллионным убыткам для компании, а ее нелегальное распространение нанесло существенный ущерб как создателям, так и правообладателям.

[1] ВЭФ анонсировал создание Глобального центра кибербезопасности. URL: https://www.securitylab.ru/news/491033.php (дата обращения: 20.08.2025).

3. Утечка конфиденциальной информации. Благодаря передовым технологиям, разработанным для военных нужд, злоумышленники могут дистанционно сканировать и декодировать электромагнитное излучение компьютеров, получая доступ к цифровым данным. Этот метод активно используется технически продвинутыми преступниками.

4. Целью компьютерного хулиганства является порча или модификация частных или секретных корпоративных данных. Отдельные хакеры, демонстрируя девиантное поведение, намеренно уничтожают или изменяют информацию на персональных компьютерах, в корпоративных сетях или в сетях конкурирующих организаций. Массовое явление приобрело создание и распространение деструктивных компьютерных вирусов, включая червей, макровирусы и полиморфные вирусы.

5. Технологический прогресс и повсеместное распространение Интернета стали катализатором для расцвета компьютерных преступлений и хакерской деятельности. Злоумышленники, например, изучают социальные сети для организации краж, а кибersталкеры используют GPS-данные смартфонов для непрерывного отслеживания своих жертв. Сегодняшние киберпреступники обладают возможностью полностью опустошать банковские счета и безвозвратно удалять данные с компьютерных серверов. Важно понимать, что ни одна компьютерная система не является абсолютно неуязвимой.

6. Современный кибersталкинг приобрел форму кибербуллинга, который особенно опасен для детей и социально незащищенных групп. Это явление заключается в систематической травле, оскорблениях или угрозах, распространяемых через цифровые каналы, такие как социальные сети, электронная почта и SMS. Любое унизительное или угрожающее сообщение, отправленное в электронном виде, считается кибербуллингом. Кибербуллинг является одним из наиболее разрушительных видов онлайн-атак. В условиях повсеместного распространения смартфонов и социальных сетей среди молодежи, этот вид высокотехнологичного социального насилия стремительно набирает обороты. В детской среде кибербуллинг часто выражается в угрозах публикации унизительных фотографий или видео, а также в создании поддельных веб-ресурсов, призванных опозорить жертву. Анонимность, которую предоставляют информационные технологии, позволяет кибербуллерам избегать ответственности. Дети, становясь жертвами, не могут идентифицировать своих обидчиков и опасаются мести с их стороны, если обратятся за помощью. Последствия кибербуллинга могут быть трагическими, приводя к серьезным психологическим проблемам и даже к суициду.

7. Современная киберпреступность трансформировалась: теперь ее движущей силой являются вредоносные программы, созданные для

автоматизации незаконных действий. Эти программы могут принимать форму вымогателей, шифрующих личные данные и требующих выкуп. Они также представляют серьезную угрозу для современных автомобилей, которые, будучи оснащенными сотнями микрочипов и сложным программным обеспечением, контролирующим все системы – от навигации до безопасности – могут быть взломаны хакерами с преступными целями. Бот-сети, объединяющие тысячи зараженных компьютеров, становятся мощным инструментом для атак на банки, компании и государственные учреждения. Прошли времена, когда киберпреступления совершались лишь высококвалифицированными одиночками. Сегодня вредоносное ПО доступно любому, кто имеет злой умысел – будь то преследователь, недовольный сотрудник или начинающий террорист, – позволяя им взламывать компьютеры, смартфоны и банковские счета. Эта угроза экспоненциально растет в современном мире, давая возможность даже заключенным совершать киберпреступления без последствий.

8. На протяжении десятилетий телефонный фрикинг представляет собой незаконное вторжение в сферу сотовой связи. С развитием мобильных технологий эта форма девиантного поведения приобрела массовый характер, охватывая кражу или нелегальное использование SIM-карт, номеров вызываемых абонентов и кодов доступа для получения незаконной прибыли. В настоящее время особую актуальность приобрел взлом голосовой почты, где частные голосовые ящики, предназначенные для хранения сообщений, становятся мишенью для телефонных мошенников. В современной России фрикинг, особенно в контексте широкого распространения Android-смартфонов, стал острой проблемой. Злоумышленники заражают устройства вредоносными программами, что позволяет им получать доступ к банковским счетам жертв, поскольку смартфоны хранят огромное количество личных данных, от информации о балансе карты до паролей и логинов.

9. Киберпреступность в банковской сфере: основные схемы мошенничества через интернет-банкинг

Злоумышленники прибегают к трем ключевым методам кражи средств, используя системы интернет-банкинга.

Первый метод: манипуляции через СМС-банкинг. В этом случае мошенники используют вредоносное ПО, способное перехватывать все СМС-сообщения, поступающие на мобильный телефон жертвы. Затем, с помощью приложения «Мобильный банк», преступник переводит деньги на свой счет. Важно отметить, что владелец смартфона не получает никаких уведомлений о списании средств. Как правило, такие хищения носят характер мелких или средних сумм.

Второй метод: фишинговые сайты. Кибермошенники создают поддельные веб-сайты, имитирующие официальные страницы банков. Эти «фишинговые» ресурсы практически неотличимы от настоящих и предназначены для выманивания у клиентов конфиденциальных данных, таких как логины и пароли. Эти данные затем используются для получения доступа к банковским счетам и финансовым активам. Один из наиболее опасных сценариев такого мошенничества выглядит следующим образом: злоумышленник, используя общедоступные списки веб-адресов, рассылает сообщения. В этих сообщениях под предлогом необходимости подтверждения личной информации, клиенту банка предлагается ввести свои данные.

В третьем варианте атаки фрикеры внедряют поддельные интерфейсы в Google Play. Эти интерфейсы перехватывают данные банковских карт пользователей, когда те пытаются совершить покупку внутри приложения. Эффективность этих атак обусловлена тем, что злоумышленники часто остаются вне досягаемости правосудия.

10. В киберпространстве все чаще совершаются масштабные электронные платежи с использованием цифровых валют, которые существуют в виде данных на банковских серверах. Взломав системы безопасности, хакеры получают доступ к информации, позволяющей им мгновенно и без труда переводить крупные суммы денег в любую точку планеты. Хотя ежедневно в деловом мире проводятся многомиллиардные электронные сделки, точные данные об убытках, понесенных компаниями и частными лицами в результате таких операций, отсутствуют. Причина в том, что уровень технической оснащенности преступников настолько высок, что не позволяет даже зафиксировать момент хищения значительных денежных средств.

Все вышесказанное подводит автора к мысли о том, что в эпоху постмодерна, с ее high-tech технологиями, культурой потребления и гламурным капитализмом, девиантное и криминальное поведение трансформируется: его носители изощренно используют все новые технологические возможности. Современные девианты и преступники активно применяют не только традиционные инструменты, такие как оружие, телефоны, лекарства и транспорт, но и активно интегрируют в свою деятельность компьютеры, сотовую связь и Интернет. Незаконная деятельность, построенная на основе современных технологий, столь же многообразна, как и сами эти технологии.