|  |
| --- |
| министерство науки и высшего образования российской федерацииЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ |

****

**Юридический институт**

**Кафедра «Судебная и правоохранительная деятельность»**

**ОТЧЁТ**

**по учебной практике по получению первичных умений и навыков**

**научно-исследовательской деятельности**

Ф.И.О. студента: Сергеева Арина Николаевна

 (полностью)

Номер группы: 405

Наименование предприятия (организации) прохождения практики:

кафедра «Судебная и правоохранительная деятельность»

(полное наименование)

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 2](#_Toc166926834)

[ГЛАВА 1 ОБЩАЯ ХАРАКТЕРИСТИКА КРИПТОПРЕСТУПЛЕНИЙ 5](#_Toc166926835)

[1.1. Обзор истории развития криптографии и применения криптографических методов преступниками 5](#_Toc166926836)

[1.2. Роль криптопреступлений в современной цифровой эпохе, включая использование криптовалют и анонимных сетей 8](#_Toc166926837)

[ГЛАВА 2 АНАЛИЗ КРИПТОПРЕСТУПЛЕНИЙ В СОВРЕМЕННОМ МИРЕ 10](#_Toc166926838)

[2.1. Типы криптопреступлений: кибератаки, кибермошенничество, расследование виртуальных криминальных сообществ и т.д. 10](#_Toc166926839)

[2.2. Актуальные примеры криптопреступлений, произошедших за последние годы 13](#_Toc166926840)

[ЗАКЛЮЧЕНИЕ 17](#_Toc166926841)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 19](#_Toc166926842)

# ВВЕДЕНИЕ

Криптопреступления, как следствие цифровизации преступности, являются одним из наиболее актуальных и опасных видов преступлений в современном мире. Вместе с появлением новых технологий и развитием цифровой сферы, криминальные элементы стали активно использовать средства криптографии и криптовалют, чтобы осуществлять свои злодеяния. Это открыло новые возможности для преступников и представляет серьезную угрозу для национальной и международной безопасности.

Одной из основных причин роста криптопреступности является растущая зависимость нашего общества от цифровых технологий. Сейчас мы все больше времени проводим в интернете, делаем покупки онлайн, обмениваемся информацией через социальные сети и мессенджеры. Все это создает огромное количество данных, которые могут стать ценной добычей для киберпреступников.

Криптографические технологии, которые были созданы для защиты информации и обеспечения конфиденциальности, сегодня используются и против нас. Преступники перехватывают и шифруют информацию, позволяя им скрыть свои следы и избежать уголовной ответственности. Они используют технику стеганографии, чтобы скрыть свои сообщения внутри обычных файлов, и криптовалюты, чтобы получать и переводить деньги без отслеживания.

Наряду с этим, преступники активно используют взломы и хакерские атаки для получения доступа к защищенной информации. Они могут украсть личные данные, банковские реквизиты, пароли и другую чувствительную информацию, которая может быть использована в корыстных целях. Часто целью криптопреступников становятся крупные корпорации, государственные учреждения и даже индивидуальные граждане.

Борьба с криптопреступностью представляет собой сложную задачу как для правопорядка, так и для общества в целом. Власти ведут активные операции по выявлению преступников, сотрудничая с международными партнерами и разрабатывая новые методы и технологии для борьбы с киберугрозами. Однако, в связи с быстрым развитием криптовалют и криптографических систем, задача оказывается сложной и требует постоянного совершенствования.

Объект исследования - использование криптовалют для совершения преступлений в сети, а также использование новых технологий для создания новых видов преступлений.

 Предмет исследования - исторический анализ развития криптопреступлений в России, понятие и их роль в формировании социально-культурного опыта, ценностей и норм поведения в обществе.

Цель работы: изучение основных этапов развития криптопреступлений в России и их влияние на современное состояние общества, а также способы их предотвращения.

Для достижения поставленной цели необходимо выполнить ряд задач:

1.Проанализировать историю развития криптографии и применения криптографических методов преступниками;

2.Рассмотреть роль криптопреступлений в современной цифровой эпохе, включая использование криптовалют и анонимных сетей;

3.Выделить Типы криптопреступлений: кибератаки, кибермошенничество, расследование виртуальных криминальных сообществ и т.д.;

4. Проанализировать актуальные примеры криптопреступлений, произошедших за последние годы.

В основу исследования положены общенаучные, частнонаучные и специальные методы, среди которых анализ и синтез, абстрагирования, системно-структурный.

Практическая значимость состоит в том, что основные положения исследования могут быть использованы в учебном процессе юридических ВУЗов, а также в дальнейших исследованиях проблем по данной теме.

Работа состоит из введения, двух глав, в которых отражено основное содержание работы, заключения и списка использованной литературы.

# ГЛАВА 1 ОБЩАЯ ХАРАКТЕРИСТИКА КРИПТОПРЕСТУПЛЕНИЙ

# 1.1. Обзор истории развития криптографии и применения криптографических методов преступниками

История развития криптографии уходит своими корнями в самые древние времена. С самого начала человечества люди осознавали важность сохранения конфиденциальности информации и передачи её только нужным лицам. Однако первые методы шифрования были довольно простыми и легко взламываемыми.

Одним из первых известных примеров применения криптографии стал шифр Цезаря, который использовался в Древнем Риме. Суть его заключалась в замене каждой буквы алфавита на другую букву, находящуюся на несколько позиций вперед или назад. Это позволяло передавать сообщения, которые могли быть прочитаны только теми, кто знал ключ к шифру[[1]](#footnote-1).

С течением времени методы шифрования становились более сложными и надежными. В Средние века использовались различные шифры, такие как шифр Виженера, который был основан на использовании последовательности ключей, и шифр Плейфейра, который использовал замены и перестановки букв. Хотя эти методы были сравнительно надежными для своего времени, они все же подвергались взлому различными способами.

Однако настоящая революция в криптографии произошла в XX веке с появлением электронных компьютеров. Криптографические методы стали намного сложнее и надежнее. Во время Второй мировой войны Enigma, немецкая машина шифрования, оказалась краеугольным камнем ломки немецких шифров, и ее расшифровка стала важным вкладом в победу союзников.

В последующие годы криптография продолжала развиваться, появились новые методы, основанные на математических алгоритмах. Алгоритмы с открытым ключом, такие как RSA, позволили создать безопасные системы передачи данных и защитить информацию от несанкционированного доступа преступников. Однако по мере усовершенствования криптографических методов, преступники также улучшали свои навыки и технологии.

С развитием технологий и науки, криптография стала все более сложной и надежной. Одним из важнейших прорывов в этой области стала появление симметричных алгоритмов шифрования. Такие алгоритмы используют один и тот же ключ как для шифрования, так и для расшифровки сообщений. Но даже с появлением таких алгоритмов, применение криптографических методов стало популярным не только среди правопослушных граждан, но и среди преступников.

Применение криптографии преступниками стало серьезной проблемой для правоохранительных органов. Уязвимость информационных систем оказывает негативное влияние на безопасность общества. Преступники используют криптографические методы для сокрытия своих преступных действий, обмана правоохранительных органов и обеспечения анонимности при передаче информации[[2]](#footnote-2).

В ответ на рост криминального использования криптографии, правительства по всему миру разрабатывают специальные программы и законодательные акты, направленные на борьбу с этой проблемой. Они также ведут активное сотрудничество с криптографическими компаниями и специалистами, чтобы разработать эффективные методы обнаружения и расшифровки криптографически защищенной информации.

В современном мире столкновение интересов между преступниками, правоохранительными органами и специалистами по криптографии остается непрерывным. Преступники совершенствуют свои методы шифрования, а правоохранительные органы и специалисты по криптографии пытаются разработать средства для борьбы с этими методами.

Криптография является ключевой областью в сфере информационной безопасности. Её развитие и применение имеют важное значение для защиты информации и обеспечения безопасности общества. Однако необходимо учесть, что криптографические методы могут быть использованы не только в целях защиты, но и для сокрытия преступных действий. Поэтому постоянное совершенствование и сотрудничество не только в области разработки криптографических методов, но и в борьбе с их злоупотреблением являются критически важными задачами для обеспечения безопасности и порядка.

# 1.2. Роль криптопреступлений в современной цифровой эпохе, включая использование криптовалют и анонимных сетей

Криптопреступления в современной цифровой эпохе играют значительную роль, поскольку преступники все чаще используют криптографические технологии для совершения различных преступлений в онлайн-среде. Особое внимание уделяется использованию криптовалют и анонимных сетей, которые позволяют преступникам скрывать свои действия и обходить системы защиты.

Так, В.А. Номоконов и Т.Л. Тропина киберпреступностью называют совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, сетей и данных[[3]](#footnote-3).

С.В. Скляров и К.В. Евдокимов указывают, что компьютерная преступность в широком смысле по объему и содержанию больше таких понятий, как киберпреступность, интернет-преступность, преступность в сфере компьютерной информации и преступность в сфере информационных технологий[[4]](#footnote-4).

Вместе с тем некоторые современные авторы сходятся во мнении, что все преступления в сфере компьютерной информации совершаются в сети Интернет[[5]](#footnote-5).

Криптовалюты, такие как Биткойн, являются одним из наиболее распространенных инструментов для осуществления финансовых манипуляций и совершения преступлений. Используя криптовалюту, преступники могут обмениваться нелегальными товарами и услугами, а также легко перемещать деньги по всему миру, минуя банки и контролирующие органы.

Для обеспечения анонимности преступники часто обращаются к использованию анонимных сетей, таких как Тор. Эти сети маскируют IP-адрес и защищают идентичность пользователей, делая их практически нераспознаваемыми. Благодаря этому, преступники могут свободно коммуницировать, планировать и совершать преступления, не подвергаясь риску быть выследженными и пойманными правоохранительными органами.

Важно отметить, что криптопреступления включают в себя не только финансовые махинации и мошенничество, но и распространение незаконного контента, кибершантаж, кибератаки и шпионаж. Преступники с использованием криптографии могут захватывать персональные данные, пароли, банковские реквизиты и другую конфиденциальную информацию, что создает значительную угрозу для безопасности и конфиденциальности в онлайн-мире.

Для борьбы с криптопреступлениями необходимо постоянное совершенствование технологий и законодательства, а также улучшение навыков и знаний правоохранительных органов и специалистов в области кибербезопасности. Только совместными усилиями и эффективной координацией можно эффективно противостоять растущей угрозе криптопреступности и обеспечить безопасность в цифровой эпохе.

# ГЛАВА 2 АНАЛИЗ КРИПТОПРЕСТУПЛЕНИЙ В СОВРЕМЕННОМ МИРЕ

# 2.1. Типы криптопреступлений: кибератаки, кибермошенничество, расследование виртуальных криминальных сообществ и т.д.

Использование современных технологий в криминальных целях долгое время являлось элитным, прибыльным и достаточно безопасным делом. Не зря подкомитет ООН по преступности поставил эту проблему в один ряд с терроризмом и наркотическим бизнесом.

До 2004 года, несмотря на многомиллиардные потери в 90% случаев правоохранительным органам даже не удаывалось выйти на след преступников, что связано с тщательной маскировкой следов преступлений. А в начале компьютерной эры, даже при поимке преступника ему часто удавалось уйти от ответственности в связи с отсутствием соответствующей статьи в законодательстве[[6]](#footnote-6).

В настоящее время уголовный кодекс РФ в главе 28 определяет следующие всеобъемлющие виды возможных преступлений в сфере компьютерной информации:

Статья 272. Неправомерный доступ к компьютерной информации 1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети[[7]](#footnote-7).

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ 1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

 Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети 1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред[[8]](#footnote-8).

 И при совершении любого из упомянутых в УК правонарушений может использоваться криптографические приемы. Вид и цель преступного деяния во многом определяется личностью преступника.  К первой категории таковых отнесем хакеров. К хакерам относят увлеченных компьютерной техникой лиц. Они имеют свой жаргон, кодекс хакерской чести, конференции, на которых обмениваются методиками взлома систем защиты.

Особенность хакеров- сочетание профессионализма в компьютерной технике с элементами фанатизма и изобретательности. Взлом ими обычно осуществляется ради самого взлома, основная цель- преодоление все усложняющихся средств защиты. Другая разновидность хакеров- кракеры.  Это лица, имеющие необходимый опыт и нашедшие материальный интерес в приложении своих знаний. Наибольшее число хищений информации совершается именно кракерами. Разновидность кракеров- информационные маклеры и мета-хакеры. Первые нанимают хакеров и платят им деньги за произведенную работу. Вторые-контролируют и используют группы хакеров как инетеллектуальные средства взлома.

 Основные направления деятельности этой категории – взлом защит разного вида, в основном криптографических. Это, например, крекинг программного обеспечения (по заказу и из интереса), взлом систем спутниково телевиденья, перехват и расшифровка банковских транзакций с целью использования банковских реквизитов клиентов, прослушка разговоров по сетям передачи данных, в т.ч. спутниковой и сотовой связи, клонирование СИМ карт и электронных проездных документов и прочее[[9]](#footnote-9).

Среди хакеров имеется своя элита- «белые воротнички». Они характеризуются организованностью совершения преступлений с обязательным сокрытием произведенных действий,и обладающими устойчивыми и ярко выраженными преступными навыками. Направление их деятельности – взлом систем электронных транзакций, защищенных стойкой и сверхстойкой криптографией каналов связи, промышленный шпионаж и крекинг систем сотовой связи.

Связь с соратниками по ремеслу поддерживают постоянно, но на чрезвычайно конфиденциальном и персональном уровне, крайне редко лично, в основном через сетевые средства общения, защищенные стойкой криптографией. Именно на долю таких преступников приходится 79% хищений средств в крупных и особо крупных размерах.

# 2.2. Актуальные примеры криптопреступлений, произошедших за последние годы

Мировая статистика компьютерных атак демонстрирует тенденцию к росту. В этом году наряду с увеличением числа преступлений, возрастает и сложность самих несанкционированных проникновений. При этом неизменными остаются цели мошенников, которые чаще всего руководствуются политическими мотивами. Подробнее о статистике киберпреступлений в России и причинах утечек расскажем в этой статье.

За первые 5 месяцев года произошла 261 тысяча успешных атак, что почти на треть (27,5%) превысило показатели прошлого года. Чаще всего для реализации преступлений используется интернет, а в текущем году с целью незаконного проникновения всё чаще применяются мобильной сети.

Положительная тенденция в области киберзащищённости наблюдается в банковском секторе: снижается число мошеннических действий с электронными деньгами (на 27% по сравнению с предыдущим годом). По данным Центрального банка в первом квартале 2023 года было отражено 2,7 миллиона атак, благодаря чему были предотвращены хищения более 700 миллионов рублей. Успешными стали 252100 операций, которые злоумышленникам удалось провести без разрешения владельцев счетов.

Согласно данным компании Kaspersky, в текущем году наиболее подверженными кибернападениям оказались крупные предприятия и объекты инфраструктуры. Наибольший урон понесли ИТ-предприятия, розничная торговля и компании финансового сектора.

Наибольший прирост числа компьютерных атак отмечен в Ингушетии (+217%) и Ненецком автономном округе (+215%). Кроме того, значительный рост продемонстрировали 8 других регионов Российской Федерации. Есть в статистике и успешные результаты борьбы с кибератаками. Наибольшее сокращение числа проникновений отмечено в Дагестане и Чеченской Республике ‒ по 23%, кроме того небольшое уменьшение продемонстрировала Московская область ‒ 0,3%.

Кроме общего роста числа кибератак отмечается и возрастание количества проникновений, которые не относятся к DDoS-атакам. Стратегия проникновений меняется во всём мире. Причина тому ‒ новые технологии и рост профессионализма хакеров. Например, взломщики активно используют ChatGPT, с помощью которого создают грамотные вызывающие доверие фишинговые письма. Вместе с этим растёт популярность киберразведки, которая особенно необходима на публичных сервисах.

Первое место среди компьютерных атак занимают кражи персональных данных. Согласно данным Роскомнадзора, количество взломов за прошедшие месяцы 2023 года превышает статистику аналогичного периода прошлого года в 4 раза. Этот вид проникновений привлекает хакеров той информацией, которую позволяет получить. Используя её, можно распознать личность и получить несанкционированный доступ к учётным записям и персональным данным. Украденные базы реализуются через специальные площадки, для распространения информации о которых используются каналы Telegram[[10]](#footnote-10).

Согласно статистике этого года, уже было обнаружено 76 фактов утечки конфиденциальной информации. Для сравнения, за такой же период предыдущего года было зафиксировано всего 19 случаев. Как сообщает Роскомнадзор, за 7 месяцев текущего года в интернет было выложено более 200 миллионов записей с личными данными граждан России. Масштаб проблемы действительно велик, ведь число украденных записей превышает численность населения нашей страны (146,4 миллиона человек).

Персональные данные попадают в сеть практически ежемесячно. Эта информация в большей части связана с регистрацией на маркетплейсах и интернет-порталах, а также с картами лояльности.

Согласно данным Центрального Банка в 2023 году ущерб россиян от кибермошенников составил 15,8 млрд рублей, а количество успешных операций составляет 1,17 млн. По сравнению с прошлым годом, последняя цифра возросла на 33%. Почему она растет? Эксперты предполагают, что мошенники стали чаще использовать адресные атаки по телефону и качественнее к ним готовиться[[11]](#footnote-11).

Только за 2023 год из финансовых организаций утекло 170,3 млн записей персональных данных клиентов. Это в 3,2 раза, больше прошедшего 2022 года. А если взять во внимание 2021 год, то этот показатель вырос в 57 раз. Рост таких инцидентов, в первую очередь, связан с организацией групп хакеров на фоне проведения СВО. Также в 2023 году произошло 168 утечек персональных данных из российских компаний, а в открытый доступ попало 300 млн записей.

За последние полгода-год с телефонными мошенниками сталкивались 67% россиян, и чаще всего, это были жители Москвы и Санкт-Петербурга (85%). По данным социологического агентства «Вебер», всего с телефонными мошенниками сталкивались 88% жителей России, а 10% теряли средства в результате этого общения. Вовсе не сталкивались с мошенниками – 76% россиян.

Только за прошлый год в Сеть утекли 240 млн уникальных телефонных номеров россиян. В эту статистику входят не только банки и финансовые организации, но и сегмент электронной коммерции, компании здравоохранения, досуга и так далее. При этом эксперты отмечают, что количество мошенничеств с использованием электронных средств платежа уменьшилось более чем на треть.

В России создан специальный сервис DLBI, который специализируется на мониторинге даркнета и расследовании утечек информации. Расскажем о тех, которые стали наиболее громкими в этом году (источники утечки могут носить предположительный характер, основываясь на предоставленной взломщиками информации).

* В январе в сеть попали данные зарегистрированных на одном из сервисов mail.ru, покупателей «Спортмастер», коды сервиса «Газпромбанк инвестиции» и некоторые базы данных страховой компании «СОГАЗ-ЖИЗНЬ».
* В феврале незаконный доступ получила информация аптечного сервиса «Здравсити», данные сотрудников компаний «Дикси» и «Бристоль», массив данных сайта asi.ru.
* В марте хакеры взломали сайт юридических услуг «СберПраво» и приложение «Сберспасибо».
* В апреле был открыт доступ к информации компании «BI.Zone» и портала kassy.ru.
* В мае было зафиксировано проникновение на сайт фонда «Сколково», а также слиты данные компании ИнфоТеКС и сети клинико-диагностических лабораторий «СИТИЛАБ»

Этот пугающий список ‒ лишь часть того, что было слито в первые 5 месяцев 2023 года. Постоянно обнаруживаются новые утечки. В частности, в API «Росреестр» нашли уязвимость, благодаря которой можно было получить информацию об объекте недвижимости без авторизации.

Учредитель сервиса DLBI Ашот Оганесян отмечает, что основную массу сливов информации (свыше 90%) составляют дампы баз данных. Взлом и выгрузка этой информации происходит благодаря наличию слабых мест в компонентах системы создания и управления сайтом[[12]](#footnote-12).

Понятие ИТ-безопасности в настоящее время затрагивает как компании, так и физических лиц. Доступ к новым технологиям наряду с преимуществами несёт и ряд опасностей, в том числе связанных с утечкой конфиденциальных данных. Предотвратить кражу информации практически невозможно, но в наших силах обеспечить качественный мониторинг уязвимостей и предоставить населению доступ к знаниям, которые позволяют избежать ошибок и финансовых потерь.

# ЗАКЛЮЧЕНИЕ

Криптография играет важную роль в нашей истории, начиная с появления самых ранних форм шифрования в древних цивилизациях. Она развивалась параллельно с развитием человечества, и в настоящее время имеет ключевое значение в цифровой эпохе. Однако, криптографические методы, которые должны обеспечивать безопасность наших данных, также используются преступниками для выполнения своих злонамеренных целей.

Роль криптопреступлений в современной цифровой эпохе нельзя недооценивать. Преступники все чаще обращаются к криптовалютам и анонимным сетям для сокрытия своих активностей и финансовых операций. Криптовалюты, такие как Биткойн, предоставляют преступникам возможность проводить транзакции без раскрытия своей личности, что затрудняет расследование и привлечение их к ответственности.

Существует несколько типов криптопреступлений, которые представляют серьезную угрозу в цифровой среде. Кибератаки являются одним из наиболее распространенных примеров криптопреступлений. Преступники могут использовать различные методы, такие как фишинг, вредоносное программное обеспечение и взлом, для получения несанкционированного доступа к конфиденциальной информации или системам. Кибермошенничество - еще одна распространенная форма преступлений, где преступники используют криптографию для обмана и мошенничества с целью получить незаконную финансовую выгоду.

Очень важно, чтобы силовые органы и кибербезопасность оставались в тренде и адаптировали свои навыки для борьбы с криптопреступлениями. Ведь технологии и методы, используемые преступниками, также продолжают развиваться. Расследование виртуальных криминальных сообществ, сбор и анализ данных и разработка новых методов противодействия - все это крайне необходимо для эффективной борьбы с криптопреступлениями.

Необходимость в защите от криптопреступлений становится все более актуальной в нашем современном обществе. Актуальные примеры криптопреступлений за последние годы, такие как атака на крупные компании, утечка конфиденциальных данных и мошеннические операции с использованием криптовалют, говорят о необходимости постоянного внимания к этой проблеме и принятии мер для ее решения.

В заключение, криптография является неотъемлемой частью нашей цифровой эпохи, и использование криптографических методов преступниками вызывает серьезные опасения для безопасности информации и финансов в нашем обществе. Разработка эффективных методов противодействия криптопреступлениям и сотрудничество силовых органов, регуляторных органов и кибербезопасности являются неотъемлемыми шагами для обеспечения безопасности и защиты интересов общества в цифровую эпоху.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

РАЗДЕЛ 1 НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ

 ОФИЦИАЛЬНЫЕ АКТЫ

Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (ред. от 19.02.2018) // Собрание законодательства Российской Федерации, 17.06.1996, № 25, ст. 2954.

Федеральный закон от 31 июля 2020 г. N 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" (с изменениями и дополнениями) – Электронный ресурс. – Режим доступа: <http://www.consultant.ru/document/cons_doc_LAW_115625/>

Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы: утв. указом Президента РФ от 09.05.2017 № 203. URL: <http://www.kremlin.ru/acts/bank/41919>  (дата обращения: 10.05.2024).

РАЗДЕЛ 2 ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Долгиева М. М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. № 10. С. 109-115.
2. Евдокимов К.Н. Политические факторы компьютерной преступности в России // Информационное право. 2015. № 1. С. 41—47.
3. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45—52.
4. Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10. № 2. C. 322—330.
5. Солдатова Ю. А. Использование криптовалюты в преступной деятельности // Перспективы развития институтов права и государства: сборник научных трудов 4-й Международной научной конференции. Курск, 2021. С. 47-49.
6. Ташло Т. А. Особенности преступлений, связанных с криптовалютой // Актуальные проблемы правоприменения и управления на современном этапе развития общества: сборник статей по материалам II Национальной заочной научно-практической конференции. 2020. С. 243-247.

 РАЗДЕЛ 3 ЭЛЕКТРОННЫЕ РЕСУРСЫ

К вопросу об использовании «криптовалюты». URL: <http://old.prokurat-so.ru/main.php?id=3004> (дата обращения: 10.05.2024).

Противодействие нелегальной деятельности на финансовом рынке // Банк России – Электронный ресурс. – Режим доступа: <https://cbr.ru/analytics/inside/2022_1/>

Финансовые пирамиды в крипте: признаки и громкие случаи / // Moscow Digital School – Электронный ресурс. – Режим доступа: <https://mosdigitals.ru/media/finansovye-piramidy-v-kripte-priznaki-i-gromkiesluchai>

1. Ташло Т. А. Особенности преступлений, связанных с криптовалютой // Актуальные проблемы правоприменения и управления на современном этапе развития общества : сборник статей по материалам II Национальной заочной научно-практической конференции. 2020. С. 243-247. [↑](#footnote-ref-1)
2. Солдатова Ю. А. Использование криптовалюты в преступной деятельности // Перспективы развития институтов права и государства: сборник научных трудов 4-й Международной научной конференции. Курск, 2021. С. 47-49. [↑](#footnote-ref-2)
3. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45—52. [↑](#footnote-ref-3)
4. Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10. № 2. C. 322—330. [↑](#footnote-ref-4)
5. Евдокимов К.Н. Политические факторы компьютерной преступности в России // Информационное право. 2015. № 1. С. 41—47. [↑](#footnote-ref-5)
6. Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы: утв. указом Президента РФ от 09.05.2017 № 203. URL: <http://www.kremlin.ru/acts/bank/41919>  (дата обращения: 10.05.2024). [↑](#footnote-ref-6)
7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (ред. от 19.02.2018) // Собрание законодательства Российской Федерации, 17.06.1996, № 25, ст. 2954. [↑](#footnote-ref-7)
8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (ред. от 19.02.2018) // Собрание законодательства Российской Федерации, 17.06.1996, № 25, ст. 2954. [↑](#footnote-ref-8)
9. Долгиева М. М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. № 10. С. 109-115. [↑](#footnote-ref-9)
10. К вопросу об использовании «криптовалюты». URL: <http://old.prokurat-so.ru/main.php?id=3004> (дата обращения: 10.05.2024). [↑](#footnote-ref-10)
11. Противодействие нелегальной деятельности на финансовом рынке // Банк России – Электронный ресурс. – Режим доступа: <https://cbr.ru/analytics/inside/2022_1/> [↑](#footnote-ref-11)
12. Финансовые пирамиды в крипте: признаки и громкие случаи / // Moscow Digital School – Электронный ресурс. – Режим доступа: <https://mosdigitals.ru/media/finansovye-piramidy-v-kripte-priznaki-i-gromkiesluchai> [↑](#footnote-ref-12)