Салишев Сергей Николаевич
аспирант
Кыргызский национальный университет им. Жусупа Баласагына
г. Бишкек, Республика Кыргызстан
Алияскарова Милана Урматбековна
аспирант
Кыргызско-Российский Славянский университет имени Б.Н. Ельцина
г. Бишкек, Республика Кыргызстан
Сеюбергенова Дидар Сламовна
докторант
Международный университет Кыргызстана
г. Бишкек, Республика Кыргызстан

АНАЛИЗ КЛЮЧЕВЫХ РИСКОВ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: *в статье раскрывается понятие информации с точки зрения юридической науки и ее классификация по различным критериям. Освещаются вопросы защиты информации, включая персональные данные, государственные и коммерческие тайны. Анализируются угрозы информационной безопасности, в том числе информационные атаки, вмешательство иностранных государств и использование информационных технологий террористическими и экстремистскими группами. Особое внимание уделяется регулированию информации в России и классификации информации на общедоступную и ограниченного доступа согласно Федеральному закону «Об информации, информационных технологиях и о защите информации». Рассматриваются ключевые факторы, которые приводят к разночтениям в научном понимании информационной безопасности.*

Ключевые слова: *информация, информационная безопасность, персональные данные, угрозы, законодательство, национальные интересы, кибербезопасность, информационные технологии.*

Для понимания информационной безопасности необходимо рассмотреть нормативно-правовые акты различных стран, которые содержат термины, такие как «цифровая информация», «электронная информация», «компьютерная информация» и «виртуальная информация». Эти документы также включают понятия, такие как «персональные данные», «личные данные», «дезинформация», «фейковая информация», «провокационная информация», «заведомо ложная информация», «компьютерные преступления» и «информационные войны». Эти термины применяются не только в научных исследованиях, но и в законодательных и политических документах, а также в рекомендациях и текстах, посвященных науке.

Юридическая наука предлагает несколько подходов к определению понятия «информация». В.Г. Семенова и Е А. Петриченко рассматривают информацию как способ передачи человеческого опыта и знаний, включая в это понятие различные объекты материального и нематериального мира [1, с. 23]. А Г. Волеводз выделяет юридический критерий информации, считая, что она должна быть записана на материальном электронном носителе и обладать идентификационными данными [2, с. 43].

В конституционном праве понятие «информация» охватывает все виды тайн, включая личную, семейную, коммерческую, государственную, медицинскую и др. В связи с этим информацию можно классифицировать по различным признакам: 1) по отношению к разным видам тайн; 2) по связи с персональными данными; 3) по юридической значимости; 4) по охране авторским или патентным правом. Также существует классификация информации по доступу к ее распространению: 1) информация, распространяемая свободно; 2) информация, распространение которой возможно только по договоренности между субъектами; 3) информация, распространение которой регулируется федеральными или региональными законами; 4) информация, распространение которой запрещено или ограничено. К последней категории относятся данные, составляющие различные виды тайн, а также информация, которая может быть признана социально опасной или незаконной.

Рассматривая информацию как объект уголовно-правовых отношений, важно подчеркнуть ее уникальные и значимые особенности. Во-первых, она нормативна: все действия с информацией, регулируемые законодательством, влекут юридическую ответственность. Во-вторых, информация должна быть достоверной, т.е. объективной и соответствующей действительности, особенно в правовых и общественных контекстах. Третьей важной характеристикой является конфиденциальность: доступ к информации должен быть ограничен, чтобы защитить права и интересы владельца или пользователя. Информация не только передает данные, но и формирует эмоциональное и психологическое состояние субъектов права, что может иметь как благоприятные, так и неблагоприятные последствия. Кроме того, государственные, медицинские и коммерческие тайны не подлежат публичному распространению и требуют особой защиты от несанкционированного доступа. Их нарушение влечет уголовную ответственность.

Регулирование информации осуществляется различными отраслями права, включая уголовное, гражданское и административное. Для обеспечения эффективной защиты общественных отношений необходимо четко определить характеристики информации и смежных понятий, а также разработать эффективные механизмы защиты информационной безопасности. В этом контексте прогнозирование и анализ угроз в информационной сфере играют важнейшую роль в обеспечении национальной безопасности, которые требуют проведения тщательного политологического анализа их негативного влияния и разработки на этой основе результативных стратегий, подходов и инструментов для их устранения. Положение усугубляется еще и тем, что в современном мире информационные угрозы становятся все более трудно выявляемыми из-за быстрого развития технологий из-за стремительного развития технологий, которые позволяют скрывать информацию за нейтральными программами. Кроме того, теперь можно передавать информацию в любую точку мира с высокой скоростью и в больших объемах. Такие атаки часто анонимны, молниеносны и имеют тщательно спланированное прикрытие, что затрудняет их своевременное обнаружение и противодействие.

В научной литературе предлагаются различные классификации угроз информационной безопасности. Так, С.В. Вихорева предлагает деление угроз по источнику угроз: антропогенные, техногенные и стихийные [3]. А.А. Хореев классифицирует угрозы по цели воздействия на информацию: конфиденциальность, целостность, доступность, утечка и неправомерное вмешательство [4]. М.М. Кучерявый разработал классификацию угроз национальной безопасности в глобальном информационном пространстве и выделил несколько ключевых аспектов: 1) источник угрозы (внутренний или внешний); 2) компоненты информационной сферы (политические, технологические и психологические); 3) характер угрозы (деструктивный или скрытый) и 4) масштаб (локальный, региональный, национальный или глобальный) [5, с. 194].

А.А. Малюк выделяет угрозы по способу воздействия: информационные (несанкционированный доступ к информации для ее хищения, искажения или уничтожения) и программно-математические (установка скрытого оборудования или компонентов в программно-аппаратные системы) [6, с. 27].

Доктрина информационной безопасности России от 5 декабря 2016 года №646 рассматривает главные информационные угрозы через призму политики. В ней особо подчеркивается быстрое развитие технологий, способных влиять на информационную инфраструктуру, и использование иностранными государствами информационных операций для достижения своих военно-политических целей. Такие операции включают психологические воздействия на общественное сознание, что может привести к дестабилизации внутри страны, подрыву суверенитета и территориальной целостности [7].

Также в последние годы спецслужбы иностранных государств активизируют техническую разведку, направленную против органов власти, научных и оборонных учреждений. Для этого они применяют компьютерные закладки, программное обеспечение для доступа и сканеры сетей, чтобы извлекать секретные данные и перехватывать трафик. Традиционные задачи, такие как сбор информации об экономике, военной мощи и научных достижениях дополняются использованием глобальных систем для решения новых вызовов.

Еще одной угрозой для национальной безопасности государства становится расширение присутствия в информационном пространстве террористических и экстремистских групп. В последние годы они все более активно используют информационные технологии для продвижения своей разрушительной идеологии и разжигания межнациональной и социальной вражды. Это явление, известное в науке как «информационный терроризм» [8, с. 35] или «кибертерроризм» [9, с. 10], приобретает все более масштабный характер. Данный тип информационного оружия характеризуется высокой степенью управляемости, скрытности, универсальности, доступности и продолжительным эффектом воздействия [8, с. 35].

Одной из ключевых угроз национальной кибербезопасности является использование информационно-коммуникационных систем иностранного производства, что может привести к уязвимостям в программном и аппаратном обеспечении. Ошибки в коде, слабые места в оборудовании и недостатки в защите данных делают системы уязвимыми для несанкционированного доступа, кибератак и утечек информации. Такие риски также могут серьезно угрожать национальной безопасности и суверенитету государства.

Таким образом, основные угрозы информационной безопасности можно условно разделить на внутренние (низкая степень информатизации, ошибки персонала) и внешние (вмешательство иностранных государств, технические атаки). Внутренние и внешние угрозы обусловлены недостатками в управлении информацией и ее защите.

В юридической науке информация классифицируется по нескольким критериям. Во-первых, в зависимости от владельца: это могут быть частные лица, организации или государственные структуры. Во-вторых, по значению в правовой системе информация может быть ключевой для законов (нормативная) либо второстепенной (ненормативная). В-третьих, по форме хранения она может быть зафиксирована в документах (документированная) или существовать в устной или иной форме (недокументированная). Наконец, по степени доступности:

информация может быть открыта для всех (общедоступная) или доступна только ограниченному кругу лиц (ограниченного доступа).

Информация ограниченного доступа может быть защищена (например, государственные тайны или международные секреты) или представлять угрозу для определенных лиц. Ограничение доступа к такой информации направлено на защиту страны, прав граждан или безопасности государства. Однако существуют сведения, которые должны быть доступны для всех, например, законы или данные о состоянии окружающей среды.

Зафиксированная информация обладает определенными характеристиками, которые позволяют ее идентифицировать, в то время как информация, существующая лишь в устной форме, может быть утрачена или искажена, что затрудняет ее идентификацию и последующее использование. В юридической сфере часто применяется термин «электронный документ», который обозначает информацию, представленную в цифровом формате и предназначенную для восприятия человеком через компьютеры, а также для передачи по сетям и обработки в информационных системах. Важно различать электронный документ и электронное сообщение, которое представляет собой информацию, передаваемую или получаемую пользователем через информационно-телекоммуникационные сети.

Разнообразие носителей информации затрудняет ее классификацию. В частности, человек как носитель информации может потребовать дополнительных критериев классификации в зависимости от его статуса.

Согласно статье 5 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ [10], информация подразделяется на общедоступную и информацию ограниченного доступа. Общедоступная информация включает общеизвестные сведения и информацию, доступ к которой не ограничен, и может использоваться любыми лицами с учетом установленных ограничений. Ограничение доступа к информации устанавливается федеральными законами для защиты конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства при соблюдении конфиденциальности.

Доступ к определенной информации не может быть ограничен, включая нормативные правовые акты, затрагивающие права и обязанности граждан, информацию о состоянии окружающей среды, деятельности государственных органов, использовании бюджетных средств (кроме сведений, составляющих государственную или служебную тайну), а также информацию из открытых фондов библиотек, музеев, архивов и других информационных систем.

С.Ю. Трофимцева и А.В. Линьков классифицируют информацию с ограниченным доступом на защищаемую информацию, включающую информацию, содержащую тайну, и информацию, не содержащую тайну, а также на «негативную для субъектов информацию», требующую защиты психики субъектов информационных отношений [11, с. 111]. И.И. Салихов выделяет три группы информации с ограниченным доступом: государственную тайну, межгосударственные секреты и конфиденциальную информацию [12, с. 10]. Государственная тайна определяется в соответствии с Федеральным законом «О государственной тайне» от 21 июля 1993 года №5485-1 [13] и включает сведения о стратегических и оперативных планах, разработке и производстве ядерных боеприпасов, тактико-технических характеристиках вооружения и военной техники, а также сведения в области экономики, науки, техники, внешнеполитической и внешнеэкономической деятельности, которые могут нанести ущерб безопасности государства.

Закон устанавливает, что к государственной тайне не относятся сведения о чрезвычайных происшествиях и катастрофах, угрозах безопасности и здоровью граждан, стихийных бедствиях и их прогнозах, состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, преступности, привилегиях, компенсациях и льготах, предоставляемых государством, фактах нарушения прав и свобод, размерах золотого запаса и государственных резервах, состоянии здоровья высших должностных лиц и фактах нарушения законности органами власти.

Конфиденциальная информация включает сведения, доступ к которым ограничен, но которые не обладают признаками государственной тайны или межгосударственных секретов. К такой информации относятся персональные данные,

тайна следствия и судопроизводства, служебная тайна, профессиональная тайна (врачебная, нотариальная, адвокатская), коммерческая тайна, сведения о сущности изобретений до официальной публикации, а также сведения из личных дел осужденных и о принудительном исполнении судебных актов.

Вопрос о соотношении понятий «тайна» и «конфиденциальная информация» остается дискуссионным. Одни авторы считают их равнозначными [14], другие – что тайна является разновидностью конфиденциальной информации с дополнительным признаком обеспеченности государственной защитой [15, с. 36]. Представляется, что тайна – это информация, доступ к которой ограничен ее владельцем, и нарушение которой влечет негативные последствия. Тайна характеризуется следующими признаками: это информация, известная ограниченному кругу лиц, доступ к которой возможен только с разрешения обладателя, и несанкционированное разглашение которой приводит к утрате ее ценности и значимости.

В уголовном праве понятие тайны охватывает информацию, доступ к которой регулируется законодательством. Нарушение этой конфиденциальности квалифицируется как уголовное преступление, подчеркивая ее особую правовую значимость. Компьютерная информация, имеющая специфическую природу, характеризуется тесной интеграцией с носителем и существует в двух формах: программное обеспечение и данные. Виртуальная природа и отсутствие физических границ компьютерной информации требуют применения специализированных устройств для доступа и обработки, что обусловливает необходимость особого подхода к правовому регулированию и защите.

Глава 28 Уголовного кодекса Российской Федерации регулирует вопросы защиты информации, обрабатываемой с использованием компьютерных технологий. Исторически термины «компьютер» и «электронно-вычислительная машина» (ЭВМ) считались взаимозаменяемыми, но в современной юридической и технической практике понятие «компьютер» значительно расширилось. В настоящее время оно включает широкий спектр устройств, таких как смартфоны и планшеты, что требует актуализации правового регулирования. Для более

точного и универсального описания этих устройств предлагается использовать термин «средства вычислительной техники», охватывающий аппаратные и программные компоненты систем обработки данных. Этот термин позволяет гибко квалифицировать различные аспекты обработки информации, обеспечивая эффективное правоприменение.

Защита компьютерной информации регулируется не только Уголовным кодексом РФ, но и другими законодательными актами – Гражданским кодексом, Федеральными законами: «О связи» от 7 июля 2003 года №126-ФЗ, «О персональных данных» 27 июля 2006 года №152-ФЗ и «Об информации, информационных технологиях и о защите информации» 27 июля 2006 года №49-ФЗ. Однако на текущий момент в российском законодательстве отсутствует специализированный акт, комплексно регулирующий защиту информации в цифровом пространстве. Также до сих пор в отечественной юриспруденции остается дискуссионным понятие информационной безопасности из-за сложной природы информации. Безопасность определяется рядом исследователей как состояние защищенности информационных систем и ресурсов от угроз. Опасность же рассматривается как вероятность наступления неблагоприятных событий, способных нанести ущерб [16, с. 149]. Отсутствие устоявшегося понятия информационной безопасности в отечественной юридической науке объясняется сложностью и многогранностью самого феномена. Информационная безопасность – это не просто защита данных от несанкционированного доступа, но и обеспечение их целостности, конфиденциальности и доступности. Она включает в себя широкий спектр вопросов, связанных с защитой информации в различных сферах: государственной, коммерческой, личной и других. Кроме того, информационная безопасность является динамичной областью, которая постоянно развивается вместе с технологическим прогрессом. Появление новых технологий (искусственный интеллект, блокчейн, беспилотная доставка) создают новые вызовы и угрозы, которые требуют постоянного обновления и адаптации подходов к обеспечению информационной безопасности.

Таким образом, отсутствие единого понимания информационной безопасности в юридической науке отражает сложность и многогранность этого явления, а также необходимость постоянного обновления и адаптации правовых норм и механизмов защиты информации в условиях быстро меняющегося цифрового мира.

Выводы.

1. Для информации характерны угрозы, которые классифицируются на антропогенные, техногенные, стихийные, внутренние и внешние. Среди основных угроз выделяются кибератаки, вмешательство иностранных государств и информационный терроризм. Угрозы информационной безопасности классифицируются по источнику (антропогенные, техногенные, стихийные), цели воздействия (конфиденциальность, целостность, доступность), способу воздействия (информационные, программно-математические), масштабу и характеру проявления

2. Проблема информационной безопасности в российской юриспруденции сохраняет свою актуальность и сложность из-за многоаспектности и динамичности информации. Основные задачи в этой области включают защиту данных от несанкционированного доступа, обеспечение их целостности, конфиденциальности и доступности. Быстрое развитие информационных технологий предъявляет новые требования к правовому регулированию, создавая дополнительные вызовы и угрозы, на которые необходимо адекватно реагировать.

3. Отсутствие единого определения информационной безопасности в российском законодательстве подчеркивает необходимость дальнейшего совершенствования нормативно-правовой базы. Для решения этой проблемы требуется провести всесторонний анализ существующих правовых норм и разработать комплексные меры, направленные на гармонизацию правового регулирования в сфере информационной безопасности, что позволит создать более устойчивую и гибкую правовую систему, способную эффективно адаптироваться к современным вызовам и угрозам.

Список литературы

1. Семенова В.Г. Информация: история понятия, его настоящее и будущее / В.Г. Семенова, Е.А. Петриченко // Известия вузов. Северо-Кавказский регион.

Серия: Общественные науки. – 2022. – №1 (213). – С. 16–26. DOI 10.18522/2687-0770-2022-1-16-26. EDN SZPHYR

2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 485 с. EDN QIONLH

3. Вихорев С.В. Классификация угроз информационной безопасности / С.В. Вихорев. – URL: http://elvis.ru/upload...7250c71c2a138fe9ecc.pdf (дата обращения: 20.05.2025).

4. Хорев А.А. Угрозы безопасности информации / А.А. Хорев // Техника для спецслужб. – URL: http://www.bnti.ru/showart.asp?aid=955&lvl=04.03 (дата обращения: 19.05.2025).

5. Кучерявый М.М. Информационное измерение политики национальной безопасности России в условиях современного глобального мира: дис. ... д-ра полит. наук: 23.00.04 / М.М. Кучерявый. – СПб., 2014. – 381 с. EDN IIPVEP

6. Малюк А.А. Защита информации в информационном обществе : учебное пособие для вузов / А.А. Малюк. – М.: Гор. линия-Телеком, 2015. – 280 с. EDN UOLMUR

7. Доктрина информационной безопасности Российской Федерации : утв. Указом Президента Российской Федерации от 5 декабря 2016 г. №646. – URL: https://www.mid.ru/ru/foreign_policy/official_documents/1539546/ (дата обращения: 25.05.2025).

8. Шеховцев Н.П. Информационное оружие: теория и практика применения в информационном противоборстве / Н.П. Шеховцев, Ю.П. Кулешов // Вестник Академии военных наук. – 2012. – №1 (38). – С. 35–40. EDN RSYNUR

9. Услинский Ф.А. Кибертерроризм в России: его свойства и особенности / Ф.А. Услинский // Право и кибербезопасность. – 2014. – №1. – С. 6–11. EDN SGYCSV

10. Об информации, информационных технологиях и о защите информации : Федеральный закон №149-ФЗ: принят 27 июля 2006 года. – URL:

https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 22.05.2025).

11. Трофимцева С.Ю. Проблема классификации информации по доступу и видам тайны в российском информационном праве и теории информационной безопасности / С.Ю. Трофимцева, А.В. Линьков // Информационная безопасность регионов. – 2012. – №2. – С. 108–116. EDN PGXAZZ

12. Салихов И.И. Информация с ограниченным доступом как объект гражданско-правовых правоотношений: автореф. дис. ... канд. юрид. наук: 12.00.03 / И.И. Салихов; Казан. гос. ун-т им. В.И. Ульянова-Ленина. – Казань, 2004. – 38 с. EDN NHMVGP

13. О государственной тайне: Федеральный закон №5485-1: принят 21 июля 1993 года. – URL: https://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 26.05.2025).

14. Ефремов А.А. Понятие и виды конфиденциальной информации / А.А. Ефремов. – URL: http://www.russianlaw.net/law/doc/a90.htm (дата обращения: 20.05.2025).

15. Паршин С.М. Тайна в уголовном законодательстве (теоретико-прикладное исследование): дис. ... канд. юрид. наук: 12.00.08 / С.М. Паршин. – Н. Новгород, 2006. – 207 с. EDN NNZWAL

16. Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы / Т.Л. Тропина, В.А. Номоконов // Библиотека криминалиста. – 2013. – №5 (10). – С. 148–160.