Гайфуллин Азамат Салаватович,
Магистр
Институт права УУНиТ
Российская Федерация, город Уфа

ИНФОРМАЦИОННЫЕ УГРОЗЫ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *статья посвящена анализу правовой природы информационных угроз в условиях цифровизации общественных отношений. Рассматриваются основные подходы к определению информационных угроз, их классификация по объекту воздействия, происхождению и способу реализации, а также особенности правовой охраны персональных данных как наиболее уязвимого сегмента информационной безопасности. Отдельное внимание уделяется информационной войне, информационному противоборству и правовым последствиям использования сети «Интернет» в качестве среды реализации противоправных действий.*

Ключевые слова: *информационная безопасность, информационные угрозы, персональные данные, информационное право, сеть «Интернет», правовое регулирование, частная жизнь, кибербезопасность.*

Abstract: *This article analyzes the legal nature of information threats in the context of the digitalization of social relations. It examines the main approaches to defining information threats, classifying them by target, origin, and method of implementation, as well as the legal protection of personal data as the most vulnerable segment of information security. Particular attention is paid to information warfare, information confrontation, and the legal consequences of using the internet as a medium for illegal activities.*

Keywords: *information security, information threats, personal data, information law, internet, legal regulation, privacy, cybersecurity.*

В условиях цифровизации общественных отношений проблематика информационных угроз перешла из узкопрофессиональной сферы в круг общих вопросов правовой политики государства. Сегодня информационная среда выступает не только технической оболочкой хранения и передачи сведений. Она стала пространством реализации публичной власти, частной автономии, предпринимательской активности и юридически значимых действий. По этой причине защита информации рассматривается уже не как вспомогательное направление, а как одно из условий устойчивости правопорядка. В научной литературе обоснованно отмечается, что эффективное противодействие угрозам возможно лишь при точном определении их содержания, выявлении каналов утечки сведений и установлении способов неправомерного доступа к охраняемой информации [1].

Правовая характеристика информационных угроз предполагает обращение к их сущности как к совокупности факторов, обстоятельств и действий, создающих риск нарушения режима обращения информации, нормального функционирования информационных систем и реализации прав субъектов информационных отношений. С этой точки зрения информационные угрозы следует рассматривать не только как технические сбои или противоправные действия в цифровой среде, но и как юридически значимые явления, способные причинить вред личности, организации, обществу и государству. В основе их правовой оценки лежит посягательство на конфиденциальность, целостность, достоверность и доступность информации. Нарушение конфиденциальности ведет к разглашению сведений ограниченного доступа. Нарушение целостности способно исказить содержание данных и сделать невозможным их правомерное использование. Утрата достоверности отражается на юридической силе информации, а ограничение доступности парализует работу систем, органов и пользователей [2].

Современная доктрина предлагает несколько оснований классификации информационных угроз. Наиболее продуктивным представляется их разграничение по объекту воздействия. Для государства особую опасность представляют информационные войны, кибершпионаж, несанкционированное получение сведений, составляющих государственную или иную охраняемую законом тайну, а также воздействия, затрагивающие устойчивость инфраструктуры и систему публичного управления. Для организаций угрозы выражаются в утечке служебной и коммерческой информации, незаконном доступе к корпоративным ресурсам, подмене данных и ином вмешательстве, которое способно повлечь имущественный вред либо нарушить нормальную хозяйственную деятельность. Для личности основными рисками являются дистанционное мошенничество, незаконное наблюдение, неправомерное распространение персональных данных, вмешательство в частную жизнь и причинение репутационного вреда с использованием цифровых средств. Подобная классификация показывает, что единый технический механизм может влечь различные правовые последствия в зависимости от объекта посягательства и круга затронутых интересов [3].

Не менее важным является деление угроз по их происхождению. Естественные угрозы обусловлены авариями, стихийными явлениями и иными факторами, не зависящими от поведения конкретного субъекта, но способными причинить вред информационной системе или массиву данных. Искусственные угрозы, напротив, связаны с поведением участников информационных отношений. Внутри этой группы обычно выделяются случайные и умышленные формы. Случайные угрозы возникают вследствие ошибок персонала, нарушения правил эксплуатации, программных сбоев и технических дефектов. Умышленные связаны с целенаправленным противоправным воздействием, включая взлом, внедрение вредоносного программного обеспечения, незаконное копирование сведений, их подмену, блокирование или распространение. В юридическом плане это разграничение

важно потому, что в каждом случае различаются основания ответственности, характер предупредительных мер и объем обязанностей владельца системы по обеспечению режима безопасности [4].

Отдельного внимания заслуживает деление угроз по способу воздействия на информационную систему. Пассивные формы не предполагают прямого вмешательства в ее функционирование, но позволяют получить доступ к охраняемым сведениям либо использовать их вне установленного режима. К таким формам относятся перехват данных, наблюдение, прослушивание, копирование информации без изменения ее содержания. Активные угрозы выражаются в модификации информации, внедрении вредоносных компонентов, разрушении информационных ресурсов, нарушении алгоритмов работы и блокировании доступа к данным. Такое деление имеет значение для юридической квалификации посягательств и оценки их общественной опасности. Не всякое неправомерное получение информации тождественно ее уничтожению или искажению, а потому правовая реакция на данные формы воздействия должна различаться [5].

В рамках анализа информационных угроз нельзя обойти вниманием явления, связанные с воздействием на общественные и государственные процессы через информационную среду. К ним относится информационная война, под которой в науке понимается целенаправленное воздействие на информационную среду другой стороны в политических, экономических или военных целях. В таком понимании она представляет собой не разовую акцию, а устойчивую систему действий, направленных на изменение восприятия событий, ослабление доверия к государственным институтам, дестабилизацию общественных отношений и получение стратегических преимуществ. Информационная война находится на стыке информационного права, права национальной безопасности, международного права и правового регулирования противодействия деструктивному воздействию в публичной сфере [4].

С более широких позиций следует рассматривать и информационное противоборство, которое охватывает политические, экономические, дипломатические и иные формы воздействия посредством информационных средств. Его правовая значимость состоит в том, что вред в таком случае может наступать не только в результате прямого нарушения режима охраны информации, но и через системное влияние на поведение граждан, институтов власти и механизмов принятия решений. Для правовой системы это означает необходимость учитывать не только завершенные правонарушения, но и те действия, которые формируют условия для дестабилизации общественных процессов и подрыва устойчивости информационной среды [5].

Динамика цифровых отношений показывает, что одной лишь констатации наличия угроз недостаточно. Возникает задача постоянного мониторинга, оценки рисков и обновления правовых механизмов защиты. В литературе обоснованно отмечается, что управление в сфере информационной безопасности строится через оценку ситуации, постановку целей, выбор решений и разработку вариантов их реализации [2]. С правовой точки зрения это означает необходимость сочетать нормативное регулирование, организационный контроль и меры юридической ответственности. Чем быстрее меняется цифровая среда, тем меньшую ценность имеет разовое нормативное решение, если оно не сопровождается процедурами актуализации и надзора.

Одной из наиболее сложных форм негативного воздействия выступает так называемое информационное оружие. Под ним понимается совокупность способов и средств, направленных на нарушение конфиденциальности, целостности и доступности информации, а также на дестабилизацию систем управления. Его особенность состоит в скрытом характере применения, трансграничности и возможности причинения вреда далеко за пределами цифровой среды. Результатом такого воздействия могут стать сбои управления, ограничение доступа к государственным и частным сервисам,

имущественные потери и массовое распространение искаженной информации. Именно поэтому правовая оценка информационного оружия должна учитывать не только техническую сторону его применения, но и цели воздействия, объект посягательства, правовой режим затронутых сведений и последствия для охраняемых законом интересов [6].

Значительная часть информационных угроз реализуется через сеть «Интернет», которая выступает основной средой обращения информации, хранения данных, совершения сделок и реализации коммуникационных прав. Расширение цифрового пространства усилило риски мошенничества, вирусных атак, незаконного использования персональных данных, подмены сведений и вмешательства в работу информационных систем. В Российской Федерации ответом на эти вызовы стало принятие специальных правовых актов, направленных на обеспечение устойчивости национального сегмента сети. К ним относится Указ Президента Российской Федерации от 22 мая 2015 года № 260 «О некоторых вопросах информационной безопасности Российской Федерации», которым утвержден порядок подключения информационных систем и сетей к сети «Интернет» и размещения информации через российский государственный сегмент сети. Сам факт существования такого акта показывает, что безопасность сетевой среды рассматривается государством как самостоятельный предмет правового регулирования, связанный с суверенитетом и национальной безопасностью [7].

Анализ информационных угроз неизбежно выводит к категории информации как объекту права. В юридической литературе она обычно понимается как совокупность сведений о лицах, предметах, фактах, событиях и процессах, которые могут быть объектом хранения, передачи, обработки и защиты. Внутри этой категории особое место занимают персональные данные. Их правовой режим сегодня образует самостоятельный институт информационного законодательства, обладающий собственным предметом

регулирования, режимом защиты и системой ограничений. Это имеет прямое значение для оценки информационных угроз, поскольку посягательства на персональные данные затрагивают не только техническую безопасность системы, но и конституционно охраняемую сферу частной жизни [8].

Вопрос о содержании понятия персональных данных остается одним из наиболее обсуждаемых в юридической науке. Под ними следует понимать не произвольный набор сведений о лице, а юридически значимую информацию, которая позволяет идентифицировать субъекта либо составить о нем достаточно полное представление. В современных условиях именно такая информация становится наиболее уязвимым объектом. Угроза в данном случае выражается не только в прямой утечке данных, но и в возможности их объединения, сопоставления и дальнейшего использования вне согласия субъекта и вне предусмотренных законом целей. В научной литературе справедливо подчеркивается, что защита персональных данных выступает одной из гарантий неприкосновенности частной жизни и требует особого правового режима [9].

Серьезной проблемой остается и неопределенность ряда нормативных положений, регулирующих обработку персональных данных. Отдельные исследователи связывают эту проблему с недостаточной конкретизацией требований к операторам и необходимостью разработки локальных актов, детализирующих порядок хранения, обработки и защиты информации. С позиций темы информационных угроз это имеет прямое значение. Если обязанности оператора сформулированы расплывчато, если порядок допуска к данным не урегулирован, а внутренний контроль носит формальный характер, то правовой режим охраны неизбежно ослабевает. В подобных условиях риск злоупотребления возникает не только извне, но и внутри самой системы законной обработки данных [10].

Современные исследования обращают внимание и на необходимость пересмотра самих критериев допуска к персональным данным. Рост числа

субъектов, участвующих в их обработке, расширение числа цифровых платформ и многослойный характер оборота данных делают прежние модели охраны недостаточными. На практике угроза формируется не только вследствие противоправного внешнего вмешательства, но и в результате чрезмерного объема полномочий у законных участников обработки, использования сведений вне первоначально заявленных целей, отсутствия надлежащего разграничения доступа и слабого контроля за дальнейшим оборотом информации [11].

Расширительное понимание персональных данных характерно и для международно-правовых актов. В частности, Конвенция Африканского союза «О кибербезопасности и защите личных данных», заключенная в г. Малабо 27 июня 2014 года, распространяет режим защиты на сведения, характеризующие физические, физиологические, психические, экономические, культурные и социальные признаки личности. Такой подход демонстрирует отход от узкого перечневого понимания персональных данных и показывает, что правовая охрана должна распространяться и на те сведения, которые лишь в совокупности позволяют индивидуализировать лицо и вторгнуться в сферу его частной жизни [12].

Эта логика поддерживается и в отечественной науке, посвященной защите конституционного права на неприкосновенность частной жизни. Автоматизированная обработка персональных данных рассматривается как сфера повышенного риска, поскольку современный цифровой оборот позволяет собирать, сопоставлять и использовать огромные массивы сведений о человеке. Чем проще объединить разрозненные данные, тем выше вероятность вмешательства в частную сферу. По этой причине правовая охрана должна учитывать не только тип сведений, но и способ их обработки, объем, цели использования и последствия для субъекта [13].

С этим связан и дискуссионный вопрос о соотношении персональных данных и информации о частной жизни. В науке обоснованно отмечается, что

часть персональных данных непосредственно относится к частной жизни и требует особых правовых механизмов защиты. Вместе с тем режим охраны частной жизни и режим охраны персональных данных не совпадают полностью, поскольку основаны на различных правовых конструкциях и используют разные отраслевые средства воздействия. Такой подход представляется оправданным. Не всякая информация о лице затрагивает его частную жизнь, но значительная часть персональных данных способна вторгаться в нее, особенно если речь идет о здоровье, семейном положении, месте проживания, биометрических характеристиках и иных чувствительных сведениях [14].

В литературе встречается и позиция, согласно которой персональные данные и информация о частной жизни пересекаются, но не совпадают полностью. В качестве примера нередко приводятся анкетные сведения - имя, место рождения, адрес, данные об образовании и профессиональной квалификации. Эти сведения могут выполнять служебную, кадровую или идентификационную функцию и не всегда затрагивают интимную сферу личности. Однако на практике один и тот же массив сведений в зависимости от контекста способен приобрести характер информации о частной жизни. Именно в этом состоит одна из главных трудностей правового регулирования: закон оперирует категориями, границы которых нередко меняются в зависимости от обстоятельств конкретного дела [15].

Критическую оценку узкого разграничения персональных данных и частной жизни предлагает современная доктрина, указывая на то, что сведения об образовании, месте работы, фамилии, адресе или контактных данных не перестают быть связанными с частной сферой лишь потому, что используются в официальном документообороте или встречаются в материалах производства. В условиях цифрового оборота даже внешне нейтральные сведения в совокупности позволяют создать подробный профиль личности, установить ее связи, маршруты перемещения, имущественные особенности и

иные элементы частной жизни. Отсюда вытекает необходимость более осторожного и широкого подхода к определению пределов правовой охраны [16].

При характеристике информационных угроз нельзя игнорировать и тот факт, что сведения собираются и распространяются через различные каналы: письменные документы, устные сообщения, аудио- и видеосвязь, цифровые платформы, сетевые публикации и средства массовой информации. Исторически сбор и систематизация сведений воспринимались как обычная функция государства и общества, однако в цифровую эпоху объем данных, скорость их оборота и способы обработки изменили саму природу риска. Информация может быть официальной и неофициальной, достоверной и недостоверной, проверенной и непроверенной. В ряде случаев она используется как средство целенаправленного воздействия на честь, достоинство и деловую репутацию. В этом контексте важное место занимает Закон Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», который формирует правовую рамку распространения сообщений и материалов в публичной сфере и определяет пределы ответственности за злоупотребление свободой массовой информации [17].

Современные проблемы правового регулирования информационных угроз проявляются прежде всего в неравномерности нормативной детализации. Российское законодательство уже содержит большое количество предписаний, направленных на защиту информации, персональных данных и устойчивости цифровой инфраструктуры, однако в практике сохраняются вопросы, связанные с разграничением видов информационных угроз, единообразием терминологии и пределами обязанностей операторов данных. Серьезной проблемой остается и фрагментарность регулирования в тех случаях, когда одна и та же ситуация затрагивает сразу несколько правовых режимов: неприкосновенность частной жизни, защиту персональных данных,

тайну коммуникаций, режим сведений ограниченного доступа и правила распространения информации в сети «Интернет». В результате правоприменитель нередко вынужден одновременно обращаться к разным нормативным актам, которые не всегда согласованы между собой [18].

Еще одна проблема связана с быстрым изменением способов совершения правонарушений в цифровой среде. Законодательная конструкция, которая в момент принятия выглядела достаточной, через сравнительно короткий срок может перестать отвечать новым формам вмешательства в информационные системы, незаконной обработки данных или скрытого цифрового воздействия. Это особенно заметно в сфере кибербезопасности, где правовая система должна реагировать на угрозы, но одновременно не создавать избыточных ограничений для законного оборота информации и цифровых сервисов. В этой связи одним из направлений решения следует признать развитие более гибких механизмов правового регулирования, основанных на сочетании общих требований закона и специальных подзаконных правил, обновляемых с учетом практики и технологических изменений.

Пути решения обозначенных проблем могут быть связаны с несколькими направлениями. Прежде всего требуется более четкое нормативное разграничение категорий информации, персональных данных и сведений, относящихся к частной жизни, что позволит снизить уровень неопределенности в правоприменении. Не менее важным представляется усиление внутреннего контроля у операторов данных, установление более ясных требований к целям обработки, объему собираемой информации и порядку допуска к ней. Нуждается в развитии и система правового мониторинга, позволяющая своевременно выявлять новые формы информационных угроз и отражать их в нормативных предписаниях без длительного запаздывания. Перспективным направлением остается совершенствование правового обеспечения кибербезопасности в части

взаимодействия государства, организаций и пользователей цифровой среды, поскольку эффективная защита информации сегодня возможна только при сочетании публичных мер, внутреннего комплаенса и правовой культуры субъектов информационных отношений.

По итогу данного параграфа, мы можем сделать следующие выводы: информационные угрозы представляют собой сложное и многослойное правовое явление, которое охватывает разные по происхождению, форме реализации и последствиям виды негативного воздействия на информацию, информационные системы и охраняемые законом интересы личности, общества и государства. Наиболее уязвимой сферой остается оборот персональных данных, поскольку он напрямую связан с реализацией конституционного права на неприкосновенность частной жизни и в условиях цифрового оборота сопряжен с высоким риском неправомерного вмешательства. Эффективное противодействие информационным угрозам возможно лишь при дальнейшем развитии согласованного правового регулирования, точном определении содержания обязанностей субъектов, укреплении механизмов контроля и формировании такого режима защиты, который обеспечивает баланс интересов личности, общества, бизнеса и государства.

Список использованных источников и литературы:

1. Сидельникова Н.В., Беседина Т.В. Информационная безопасность // Образование. Карьера. Общество. 2018. № 1 (56). С. 71.

2. Грачева Е.А. Информационная безопасность // The Newman in Foreign Policy. 2020. Т. 3. № 54 (98). С. 57.

3. Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. Т. 11. № 4. С. 70-81.

4. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 58-74.

5. Панарин И.Н. Метод и методика оценки эффективности системы и защиты территориально-распределенных информационных систем // Информатизация и связь. 2020. № 3. С. 74.

6. Грачева Е.А. Информационная безопасность // The Newman in Foreign Policy. 2020. Т. 3. № 54 (98). С. 57.

7. Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/ (дата обращения: 15.04.2026).

8. Рузанова В.Д. Законодательство в области персональных данных как институт информационного законодательства // Юридический вестник Самарского университета. 2022. № 2. С. 15.

9. Степанова М.Н. Информационная безопасность в правовом поле: стратегии правового регулирования и защиты киберпространства // Правопорядок: история, теория, практика. 2024. № 1 (40). С. 48-52.

10. Михеева И.В., Нахман Ф.Г. Законодательство о защите персональных данных: неопределенность vs конкретности // Теоретическая и прикладная юриспруденция. 2023. № 2. С. 161.

11. Мхитарян А.С. Защита персональных данных в России: современное состояние и перспективы развития // Вестник Прикамского социального института. 2024. № 6. С. 202.

12. Конвенция Африканского Союза «О кибербезопасности и защите личных данных». Заключена в г. Малабо 27 июня 2014 г. // Официальный сайт Африканского Союза [Электронный ресурс]. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-dataprotection (дата обращения: 15.04.2026).

13. Федосин А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в РФ: автореф. дис. ... канд. юрид. наук. Саранск, 2009. С. 14.

14. Жирнова Н.А., Солдаткина О.Л. К вопросу о правовом режиме обезличенных персональных данных // Вестник Воронежского государственного университета. Серия: Право. 2024. № 4 (59). С. 44-51.

15. Дубень А.К. Правовые аспекты информационной безопасности государства: теоретические проблемы и перспективы развития // Правовая политика и правовая жизнь. 2024. № 3. С. 123-129.

16. Ересько П.В. Правовые проблемы обеспечения информационной безопасности личности в цифровом пространстве // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2025. Т. 25. Вып. 4. С. 424-436.

17. Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (с посл. изм. и доп. от 23 ноября 2024 г. № 411-ФЗ) // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru/ (дата обращения: 15.04.2026).

18. Смушкин А.Б. Кибербезопасность: понятие, структура, механизм правового обеспечения // Правоприменение. 2025. Т. 9. № 3. С. 114-123.