Утечки конфиденциальных данных в цифровую эпоху: этико-правовые аспекты кибербезопасности

С. А. Ващенко

Санкт-Петербургский государственный университет

vashhenkosofia05@gmail.com

Аннотация

Статья посвящена анализу этико-правовых аспектов цифровой безопасности в контексте возрастающих киберугроз и трансформации общества под влиянием цифровых технологий. Рассматриваются этические принципы, лежащие в основе противодействия киберпреступности, в том числе вопросы ответственности за действия в киберпространстве. Особое внимание уделено изучению причин утечек конфиденциальных данных и анализу правовых механизмов, направленных на обеспечение кибербезопасности, с оценкой их эффективности. В работе рассматриваются ключевые вызовы, связанные с утечками конфиденциальных данных, включая технологические уязвимости, недостатки правового регулирования и этические дилеммы киберпространства. Особое внимание уделено изучению причин роста киберпреступности, среди которых выделяются усложнение кибернетических систем, отсутствие международных стандартов защиты данных и низкая осведомленность пользователей. На основе анализа статистики утечек и регуляторных практик демонстрируется: современные механизмы кибербезопасности зачастую не успевают адаптироваться к динамике угроз, что требует пересмотра существующих подходов к обеспечению кибербезопасности. Основным результатом исследования стало выявление системных противоречий между технологическим прогрессом, правовым регулированием и этическими нормами. На примере конкретных случаев утечек данных показано, что они обусловлены не только техническими факторами (уязвимости API, человеческий фактор), но и слабостью санкционных механизмов, особенно в сравнении с жесткими нормами General Data Protection Regulation. Анализ принципов киберэтики (конфиденциальность, прозрачность, подотчетность) подтвердил их декларативный характер в отсутствие эффективных инструментов реализации. При этом такие инициативы, как «Хартия цифровой этики РФ» и практика этичного хакинга, демонстрируют потенциал сочетания «мягкого» регулирования с технологическими решениями.

Ключевые слова: цифровая безопасность, кибербезопасность, киберэтика, утечки конфиденциальных данных, киберугрозы, киберпреступность

Библиографическая ссылка: Ващенко С. А. Утечки конфиденциальных данных в цифровую эпоху: этико-правовые аспекты кибербезопасности // Информационное общество: образование, наука, культура и технологии будущего. Выпуск 9 (Труды XXVIII Международной объединенной научной конференции «Интернет и современное общество», IMS-2025, Санкт-Петербург, 23 – 25 июня 2025 г. Сборник научных статей). — СПб: Университет ИТМО, 2025. С. 103-114. DOI: 10.17586/3033-5574-2025-9-103-114.

1. Введение

На сегодняшний день цифровая трансформация охватывает практически все сферы деятельности общества, следствием чего становится рост киберугроз и необходимость обеспечения кибербезопасности. По данным CyberSecurity Ventures за 2023 г., мировой ущерб от киберпреступлений, включая утечки конфиденциальных данных, превысил $ 8 трлн. В России, согласно данным Роскомнадзора, ежегодно устанавливается более 4 тыс. случаев утечек конфиденциальных данных пользователей.

Цель данного исследования — провести системный анализ причин утечек конфиденциальных данных, оценить эффективность современных мер защиты и выявить основные технологические, правовые и этические тенденции в сфере кибербезопасности.

Актуальность исследования обусловлена необходимостью изучения вопросов преодоления разрыва между стремительным развитием технологий и нормативно-этическим регулированием.

В последние годы государства все чаще позиционируют цифровизацию как один из ключевых приоритетов развития. Это обусловлено тем, что стремительный переход к системе электронного документооборота, внедрение цифровых процессов верификации юридических действий, а также реализация концепции цифровой экономики затрагивают не только профессиональную деятельность людей, но и общественные отношения в целом. В сфере государственного управления цифровизация трансформирует или замещает некоторые компетенции органов власти. Особое внимание в данном контексте следует уделить развитию электронного правительства, которое преобразует способы взаимодействия граждан с государственными услугами, обеспечивая оперативность, прозрачность, инклюзивность и надежность. Кроме того, оно расширяет возможности граждан в принятии политических решений. Тем не менее, регулирование данных процессов требует одновременной реализации как норм публичного права для обеспечения безопасности, гарантий прав и свобод человека, защиты персональных данных, так и частноправовых норм, направленных на защиту имущественных интересов [1].

Цифровизация социальной жизни и элементов государственного управления, активно развивающаяся под влиянием цифровых технологий, привела к трансформации общества. Этот процесс актуализирует необходимость усиленного контроля над этико-правовыми аспектами цифровой безопасности, что является ключевым условием для повышения её эффективности в новых реалиях. При этом цифровая безопасность представляет собой комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от вирусных атак и несанкционированного вмешательства [2]. Её задачи включают не только противодействие вирусным атакам, но и создание устойчивых систем для минимизации рисков в цифровой среде. Данная концепция тесно связана с более узкой областью — кибербезопасностью, которая представляет собой область деятельности, относящуюся к защите информационных систем (аппаратного и программного обеспечения и связанной с ними инфраструктуры), данных и ИТ-услуг от несанкционированного доступа, повреждения (преднамеренного или случайного) или некорректного использования [3]. Последние подразумевают специфику производства услуг в сфере информационных технологий, что требует отдельного внимания к их уязвимостям.

Стремительное развитие технологий способствует появлению новых вызовов в области кибербезопасности. К ним относятся не только традиционные угрозы, такие как преднамеренные атаки или случайные повреждения данных, но и риски, связанные с некорректным использованием цифровых сервисов. Это делает вопрос интеграции этических и правовых норм в технологические процессы особенно актуальным.

2. Основные проблемы в обеспечении цифровой безопасности

2.1. Усложнение кибернетических систем и модернизация методов кибератак

Современные кибернетические системы характеризуются беспрецедентной сложностью, обусловленной интеграцией распределения сетей, интернета вещей (Internet of Things) и облачных технологий. Это создает новые возможности для киберпреступников, которые применяют как традиционные методы, например, фишинг или блокировку данных, так и инновационные подходы. Среди последних можно выделить: долгосрочные скрытые атаки, которые остаются незамеченными, использование искусственного интеллекта для автоматизации поиска уязвимостей, целенаправленные атаки на критическую инфраструктуру.

Главная проблема заключается в том, что системы защиты не успевают адаптироваться к скорости появления новых угроз. Например, многие организации до сих пор полагаются на устаревшие антивирусные программы, в то время как злоумышленники применяют алгоритмы машинного обучения для обхода защиты.

2.2. Правовые противоречия на международном уровне

Отсутствие единых стандартов регулирования киберпространства осложняет борьбу с цифровой преступностью. Каждое государство самостоятельно разрабатывает правовые режимы, связанные с обеспечением кибербезопасности, что приводит к сложности расследования трансграничных атак и мешает обмену информацией о новых угрозах и методах их нейтрализации между государствами. В результате киберпреступники используют правовые пробелы, что повышает риски атак в странах со слабым законодательством.

2.3. Уязвимости в облачных сервисах и недостаточное финансирование кибербезопасности

Переход на облачные сервисы, несмотря на их удобство, повышает уязвимости данных. Исследования показывают, что большинство утечек происходит из-за ошибок в настройке доступа или использования устаревших версий программ. Однако, не менее важной проблемой остается человеческий фактор, выраженный в неосознанном распространении личной информации через мессенджеры, социальные сети и в несоблюдении установленных организацией правил, в том числе: использование слабых паролей, пренебрежение двухфакторной аутентификацией и постоянным обновлением программного обеспечения. Особенно уязвим малый и средний бизнес: многие компании пренебрегают качественной защитой, а крупные организации внедряют в систему защиты более сложные технологии только после утечки данных [4].

Несмотря на декларируемую цифровизацию, государственные учреждения продолжают демонстрировать отставание в переходе на электронный документооборот. Этот системный пробел создает благоприятную среду для эксплуатации уязвимостей, поскольку гибридные модели работы (сочетание бумажных и цифровых процессов) повышают риски несанкционированного доступа и потери данных. Статистические данные подтверждают прямую корреляцию между технологической незрелостью инфраструктур и уровнем киберпреступности. Так, в 2020 г. МВД России зафиксировало свыше 500 тыс. преступлений, связанных с использованием телекоммуникационных технологий, включая мошенничества с банковскими картами и фишинговые атаки через интернет-каналы.

К концу 2023 г. наблюдается устойчивая негативная динамика: объем подобных правонарушений вырос на 28,7 %, что свидетельствует о недостаточной эффективности текущих мер защиты. При этом рост криминальной активности сопровождается прогрессом в раскрываемости преступлений — например, внедрение алгоритмов анализа Big Data позволило идентифицировать 15 % сложных многоэтапных атак, которые ранее оставались

незамеченными. Однако данная положительная тенденция не компенсирует системных проблем: замедление цифровой трансформации госсектора продолжает ограничивать возможности для противодействия угрозам, поскольку устаревшие ИТ-системы не поддерживают современные протоколы шифрования и методы аутентификации.

Помимо всех вышеперечисленных проблем в обеспечении цифровой безопасности, немаловажную роль играют этические и социальные проблемы, которые включают в себя споры о публичных и частных аспектах личной информации, которая становится все более доступной в Интернете [5].

3. Основные этические принципы в киберпространстве

Стремительная цифровая трансформация, сопровождаемая внедрением нейросетевых алгоритмов, генеративного ИИ и децентрализованных систем, актуализирует вопросы этического регулирования киберпространства. Несмотря на растущий объем исследований в области киберэтики, сохраняется критический разрыв между технологическими инновациями и их нормативно-ценностным осмыслением.

Под киберэтикой обычно понимаются правила нравственного (справедливого, честного, правильного) поведения в сфере Интернета. Она распространяется далеко за рамки «сетевого этикета» — правил, которые были выработаны в ранний период начала функционирования Интернета [5].

Помимо этого, современная киберэтика требует междисциплинарного подхода, интегрирующего философию технологии, антропологию данных и машинную этику (machine ethics). Критическим ограничением текущих исследований остаётся недостаточная проработка методологии анализа ценностных императивов, что проявляется в фрагментарности теоретических моделей и их слабой адаптации к вызовам нейросетевых алгоритмов.

Стоит отметить, что ключевая задача киберэтики заключается не только в повышении цифровой грамотности, но и в формировании системных механизмов для разрешения нормативных вопросов, возникающих на стыке человеко-машинного взаимодействия. При этом регулятивный потенциал киберэтики ограничен за счет отсутствия единых решений в вопросах экзистенциальных рисков искусственного интеллекта, этической верификации алгоритмических решений, пересмотра концепции ответственности в условиях делегирования полномочий искусственному интеллекту.

В применении этических принципов основной целью является повышение компетентности в использовании современных технологий и осведомленности об обязанностях и полномочиях субъектов информационных отношений. При этом необходимо учесть, что киберэтика призвана регулировать поведение человека в информационном мире [6].

Киберэтику также называют интернет-этикой, то есть областью прикладной этики, изучающей этические вопросы и моральные дилеммы, связанные с появлением цифровых технологий и глобальной виртуальной среды, в частности: проблемы конфиденциальности, точности и доступности информации, защиты интеллектуальной собственности, безопасности данных и цифрового неравенства [7].

Особую остроту приобретают вопросы киберпреступности, поскольку традиционные этические парадигмы не учитывают специфику криптоанонимности и децентрализованных систем. Так, распространение смарт-контрактов и децентрализованных автономных организаций требует разработки новых критериев справедливости, выходящих за рамки антропоцентричных моделей.

Помимо вышеперечисленного к сфере киберэтики и изучаемым ею вопросам, можно отнести вопросы киберпреступности глобальной сети, ставящие под угрозу основные принципы кибербезопасности, этические и нравственные особенности общения в сети, социальные последствия внедрения цифровых технологий, вопросы доступа и цензуры

информации, проблемы цифрового неравенства. Из этого следует, что современная кибербезопасность основывается на системе этических принципов, формирующих базу осознанного взаимодействия в цифровом мире.

В данном контексте стоит отметить, что к ключевыми и наиболее значимыми принципами киберэтики в цифровой среде относятся:

- конфиденциальность — защита персональных данных от несанкционированного доступа, обеспечивает доверие к цифровым системам у пользователей и включает в себя методы шифрования и аутентификацию, позволяющие минимизировать сбор личных данных. Нарушение конфиденциальности приводит к фишинга, утечкам данных и кибермошенничеству;
- прозрачность (открытость процессов и алгоритмов обработки информации), обеспечивает осведомленность пользователей об использовании их данных и помогает обнаруживать скрытые угрозы в киберпространстве;
- подотчетность (ответственность субъектов за кибербезопасность среди конкретных организаций и разработчиков). Благодаря подотчетности организации обязуются брать ответственность за утечки данных пользователей, в связи с чем внедряют наиболее эффективные и продвинутые меры защиты.

Данные принципы ясно отражены как в международных нормативных актах, например: General Data Protection Regulation (GDPR) — общий регламент по защите данных и Cybersecurity Act — представляющий единую систему сертификации кибербезопасности для продуктов и услуг, так и в российском законодательстве: Федеральный закон № 152–ФЗ «О персональных данных», Федеральный закон № 149–ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон № 187–ФЗ «О безопасности критической информационной инфраструктуры (КИИ)».

Однако, применение этих принципов на практике приводит к конфликту между требованиями цифровизации и необходимостью защиты данных. Этический конфликт безопасности и свободного распространения информации приводит к вопросу о разработке новых правовых механизмов и этических кодексов поведения в киберпространстве.

4. Киберэтика как новая область регулирования цифрового пространства

Развитие и постоянная модернизация киберэтики демонстрируют потребность в нормативно-этическом регулировании взаимодействий в условиях цифровой трансформации.

Одним из ключевых примеров институционализации этических норм в цифровом пространстве является разработанная в 2021 г. «Хартия цифровой этики РФ» — документ, созданный Альянсом по защите детей в цифровой среде совместно с крупнейшими российскими IT-компаниями. В отличие от жёстких правовых механизмов GDPR, Хартия носит рекомендательный характер, что отражает переходный этап от декларации абстрактных принципов к их системному законодательному закреплению в цифровой этике.

Важно отметить, что нормативное регулирование не исчерпывает всех аспектов регулирования цифровой среды. В этой связи приоритетной задачей становится не только формальное принятие этических кодексов, но и обеспечение их осознанного усвоения на индивидуальном уровне. Данный аспект зафиксирован в тексте Хартии, где подчеркивается необходимость формирования цифровой культуры, основанной на ответственности всех участников взаимодействия.

Деятельность «Хартии цифровой этики РФ» позволяет сделать вывод о постепенной эволюции регулятивных механизмов — от рекомендательных норм к комплексным правовым решениям. Однако эффективность подобных инициатив напрямую коррелирует с синхронизацией нормативных требований с образовательными и просветительскими практиками, направленными на повышение цифровой грамотности общества. Данный

пример актуализирует проблему низкой осведомленности о последствиях киберпреступности, которая остается ключевым вызовом в сфере киберэтики.

Считая низкую осведомленность о последствиях киберпреступности одной из проблем в области киберэтики, необходимо разграничивать группы киберпреступников по уровню их компетентности и сфере интересов. особое внимание следует уделить наименее квалифицированным из них, в частности новичкам, которые зачастую являются молодыми людьми, действующими из личного интереса. Можно предположить, что огромное количество актов хакерства со стороны молодежи обусловлено незнанием этических принципов и установленных нормативных актов, которые на законодательном уровне предполагают последствия за незаконные, неэтичные поступки.

Сочетание нормативных инициатив с образовательными мерами могло бы сократить число киберпреступлений, совершаемых некомпетентными в вопросах киберэтики хакерами, формируя наиболее ответственное и осознанное отношение к поведению в цифровой среде.

5. Этичный хакинг

Если говорить о более масштабном и профессиональном противодействии киберугрозам, то особое внимание следует уделить этичному (белому) хакингу. Этичный хакинг, также известный как белый хакинг, представляет собой практику легального и разрешенного проникновения в компьютерные системы и сети с целью выявления и устранения уязвимостей.

Этические хакеры используют те же методы, что и злоумышленники, однако их действия согласованы с владельцами систем и направлены на повышение уровня кибербезопасности. История этичного хакинга берет свое начало в 1970-х годах, когда корпорация IBM начала применять хакеров для тестирования своих систем. С тех пор этичный хакинг стал важным инструментом в арсенале средств защиты информационных технологий, получив признание и поддержку на международном уровне [8].

Данный подход демонстрирует как навыки, связанные с киберпреступностью, могут быть направленны на защиту цифровой инфраструктуры. Необходимо иметь в виду, что развитие киберпространства и борьба с киберпреступностью требует комплексного подхода, включая в себя нормативное регулирование, повышение осведомленности общества о последствиях незаконных действий и возможности изменения направленности навыков с деструктивных целей на развитие цифровой этики.

6. Развитие сферы безопасности и правовые механизмы защиты данных в России и мире

Основную проблему в обеспечении информационной безопасности составляет защита самой информации. Государство обеспечивает защиту информации на законодательном уровне, но оно не может оградить нас от человеческого фактора [9]. Современные системы правового регулирования в области защиты данных демонстрируют существенные различия в подходах к обеспечению кибербезопасности. Эти различия обусловлены как спецификой национальных законодательств, так и глобальными вызовами, связанными с ростом киберугроз.

Согласно Global Cybersecurity Index (GCI) — глобальному индексу кибербезопасности за 2020 г., ключевые государственные инициативы в области обеспечения конфиденциальности персональных данных граждан и формирования безопасной цифровой среды должны начинаться с модернизации нормативно-правовой базы [10].

По данным российской компании «Группа компаний InfoWatch», специализирующейся на информационной безопасности в корпоративном секторе и контролирующей около 50 % отечественного рынка систем защиты конфиденциальных данных, количество утечек

информации в мире за 2023 г. увеличилось более чем на 60 %, а объем скомпрометированных персональных данных — более чем в два раза. При этом доля России в мировом распределении утечек сократилась почти вдвое — с 10,8 % до 5,7 %.

А сектор аналитических исследований Университета Иннополис утверждает, что сегмент кибербезопасности в России развивается ускоренными темпами. Это подтверждается ростом глобального индекса киберготовности страны: если в 2019 г. РФ занимала 28 место, то к 2020 г. поднялась на 8 позицию.

Государство постоянно принимает меры по укреплению технологического суверенитета страны, что выражается в увеличении числа нормативных актов. Так, в 2022 г. было принято 257 нормативных правовых актов, касающихся регулирования сфер информационной безопасности, информационных технологий и цифровой экономики в целом, что на 25 % больше по сравнению с 2021 г.

В России основным нормативным актом в области защиты персональных данных выступает Федеральный закон № 152-ФЗ. Он устанавливает требования к операторам, однако характеризуется относительно мягкими санкциями. Например, в случае незаконной передачи информации о людях в количестве от 1 тыс. до 10 тыс. человек, должностным лицам государственного или муниципального органа либо некоммерческой организации назначается штраф от 200 тыс. до 400 тыс. рублей. Индивидуальным предпринимателям и компаниям — от 3 млн до 5 млн рублей.

Более строгие меры предусмотрены Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры», направленным на защиту объектов жизнеобеспечения государства. Однако его действие не распространяется на большинство коммерческих организаций, что создает пробелы в регулировании.

В отличие от российской практики, General Data Protection Regulation (GDPR) Европейского союза устанавливает пропорциональные штрафы до 4 % глобального оборота компании. Яркий пример — штраф Meta* в размере 1,2 млрд евро, наложенный в 2023 г. за нарушение правил трансграничной передачи данных. Подобные санкции стимулируют компании к соблюдению стандартов безопасности, тогда как в РФ меры остаются менее репрессивными.

Несмотря на прогресс в области кибербезопасности, российское законодательство требует дальнейшей гармонизации с международными нормами. Усиление санкций, расширение охвата регуляторных механизмов и внедрение риск-ориентированного подхода могут стать ключевыми направлениями для реформирования отрасли.

7. Анализ утечек данных: причины и последствия

Главной проблемой в киберпространстве остается компрометация персональных данных (PII — Personally Identifiable Information), становясь системным вызовом для глобальной кибербезопасности. Киберпреступники, специализирующиеся на фишинге и целевых атаках, активно эксплуатируют уязвимости инфраструктур компаний, превращая конфиденциальную информацию в товар теневого рынка. К наиболее распространенным факторам утечек относятся: недостаточная защита API-интерфейсов, внутренние угрозы и слабость регуляторного надзора. Иллюстрацией указанных проблем служат следующие примеры утечек.

7.1. Утечка данных в Facebook* (2019)

В 2021 г. произошла наиболее масштабная утечка данных пользователей. По сообщению Business Insider на одной из хакерских цифровых площадок были бесплатно опубликованы личные данные 533 млн пользователей этой социальной сети.

---

* *Организация Meta, а также её продукты Instagram и Facebook, признаны экстремистскими на территории РФ.*

Утечка также была вызвана недостаточным контролем и качеством API платформы и повлекла за собой серьезные последствия: появление автоматизированного Telegram-бота, с помощью которого можно было получить доступ к данным конкретного человека. В последствии компания столкнулась с многочисленными судебными исками, ударом по репутации социальной сети и штрафом в размер € 265 млн, согласно системе штрафов GDPR.

Помимо этого, после расследования, установившее в 2021 г. факты противоправного получения контроля над чужими учетными записями с помощью внутренней функции восстановления доступа к учетным записям «Oops» (online operations), несколько десятков специалистов, в том числе из службы безопасности компании были уволены.

7.2. Утечка данных «Сбербанка» (2022)

В 2022 г. произошла крупнейшая утечка данных «Сбербанка», вызванная уязвимостью API-интерфейсов. По словам заместителя председателя правления Сбербанка, в течение всего года хакеры украли данные более 65 млн россиян, среди которых 13 млн данных банковских карт. Однако Роскомнадзор сопоставил нанесённый организацией ущерб пользователям в 300 тыс. рублей штрафа.

Ключевыми проблемами инцидента стали: недостаточная защита API, то есть отсутствие строгой аутентификации и слабость регуляторных мер. Ущерб от перевыпуска карт составил не менее 4,5 млрд руб.

Данный инцидент повлиял на всю сферу финансов и заставил задуматься о внедрении обязательных стандартов защиты API и межбанковском сотрудничестве, направленном на противодействие подобным кибератакам в будущем.

7.3. Утечка конфиденциальной информации клиентов сервиса «Яндекс.Еда» (2022)

В 2022 г. наиболее значимым стал инцидент одного из сервисов Яндекса, связанный с безопасностью личных данных пользователей. Конфиденциальная информация, в том числе контактные телефоны, данные о составе и времени заказов, адресах доставок оказались в открытом доступе, согласно официальному заявлению компании — из-за нарушения политики информационной безопасности одним из сотрудников.

В последствии данного инцидента компания усилила меры безопасности полностью исключив «ручную» обработку информации о заказах, а также усилив внутренние системы контроля доступа к личным данным пользователей.

Для киберпреступников особую значимость подобных утечек представляет не только компрометация личных данных пользователей цифровых площадок, но и способ заработать на этом с помощью теневых рынков. Конфиденциальные данные становятся товаром в Даркнете и, имея большой спрос, используются в дальнейшем для реализации целевых атак.

В 2021 г. в Даркнете появилась возможность купить персональные данные почти 100 млн подписчиков индийского платежного приложения MobiKwik. За 70 тыс. долларов киберпреступники предлагали доступ более чем к 8 ТБ данных, включая номера телефонов, учетные данные, истории транзакций и реквизиты банковских карт.

Еще более масштабная утечка 2021 г. произошла в китайской компании Alibaba Group. По сообщению The Wall Street Journal один из официальных разработчиков ПО в течение восьми месяцев копировал данные более 1 млрд пользователей торговой интернет-платформы Taobao, пока администрация Alibaba не заметила подозрительную активность в своей сети.

Из этого можно сделать вывод, что скомпрометированные данные становятся товаром, достигающим стоимости в десятки тысяч долларов, и, на сегодняшний день, внутренние угрозы остаются наиболее значимым вызовом в обеспечении информационной безопасности, так как даже лидеры внедрения и применения новых технологий не застрахованы от скрытых кибератак.

Также данные случаи позволяют выделить три стратегических направления для реформирования кибербезопасности: унификация стандартов защиты API на международном уровне, ужесточение контроля за внутренними угрозами через внедрение систем мониторинга и повышение ответственности компаний за утечки через адекватные штрафные санкции. Реализация этих мер требует не только технологических инвестиций, но и активного диалога между государством, бизнесом и международным экспертным сообществом.

8. Системы защиты от утечек

Внутренние киберугрозы представляют собой наиболее значительную опасность не только для персональных данных пользователей, но и для компаний. В данном контексте особую актуальность приобретают комплексные системы предотвращения утечек информации, которые являются один из наиболее важных факторов в безопасности организации. В данном контексте, стоит отметить, что к ключевыми и наиболее значимыми принципами киберэтики в цифровой среде являются:

- Endpoint Detection and Response (EDR) — система защиты, которая обнаруживает и предотвращает угрозы в режиме реального времени на устройствах конечных пользователей, таких как рабочие станции, ноутбуки и мобильные устройства;
- Cloud Access Security Broker (CASB) — платформа, которая обеспечивает контроль и безопасность доступа к облачным сервисам, и предотвращает утечки данных в облаке;
- User and Entity Behavior Analytics (UEBA) — подход к анализу поведения пользователей и сущностей, который использует машинное обучение для выявления вредоносных действий внутри сети;
- Security Information and Event Management (SIEM) — система, которая собирает и анализирует данные о событиях безопасности в режиме реального времени, чтобы обнаружить аномалии и потенциальные угрозы безопасности;
- Data Leak Prevention (DLP) — набор технологий, политик и процессов, для контроля и управления информацией, предотвращая несанкционированный доступ, использование и распространение конфиденциальных данных [11].

Каждая из перечисленных систем может быть полезной в зависимости от потребностей и требований предприятий. Их эффективность основана на комплексном походе, включая в себя не только общий мониторинг, но и попытки предотвращения утечек в облачных сервисах. Однако необходимо учитывать, что помимо инвестиций в системы обеспечения безопасности, необходимо адаптировать внутреннюю политику и специалистов компании к новым киберугрозам.

9. Заключение

Цифровая трансформация, охватившая все сферы общества, повлияла не только на цифровизацию социальной жизни и государственных систем, но и создала новые глобальные вызовы. Как показал анализ, постоянно растущее количество утечек данных и кибератак требует укрепления нормативной базы, внедрения новых этических принципов и более ответственного подхода к обеспечению и применению многоуровневых систем защиты компаний.

Таким образом, цифровая безопасность в условиях глобальной трансформации общества представляет собой комплексную проблему, решение которой возможно лишь при интеграции технологических, правовых и этических подходов.

Анализ динамики киберугроз, причин утечек конфиденциальных данных и регуляторных практик позволил выявить системные противоречия, лежащие в основе современных вызовов киберпространства.

Ускоренное развитие облачных технологий, интернета вещей и алгоритмов искусственного интеллекта не только расширяет возможности злоумышленников, но и демонстрирует слабые места защитных механизмов, особенно в контексте гибридных моделей работы государственных структур и малого бизнеса. При этом ключевым барьером на пути минимизации рисков остается разрыв между декларируемыми принципами киберэтики, такими как конфиденциальность и подотчетность, и их реализацией в условиях разнонаправленных интересов бизнеса, государства и пользователей.

Эффективность противодействия киберпреступности напрямую зависит от синхронизации международных регуляторных инициатив. Отсутствие единых стандартов защиты данных, несоразмерность санкций масштабам ущерба и юрисдикционные конфликты создают среду для эксплуатации правовых пробелов. В этом контексте особую значимость приобретает опыт гармонизации нормативных требований с просветительскими практиками, направленными на формирование цифровой культуры ответственности. Примеры внедрения этичного хакинга и применения принципов цифровой этики подчеркивают потенциал сочетания «мягких» регуляторных инструментов с технологическими инновациями.

Перспективным направлением развития кибербезопасности становится переход от реактивных мер к превентивным стратегиям, основанным на прогнозировании угроз с помощью междисциплинарных моделей. Такие модели должны объединять машинное обучение для анализа поведения пользователей, правовые механизмы для усиления ответственности организаций и этические принципы для баланса между безопасностью и цифровыми свободами. Реализация этой парадигмы невозможна без активного диалога между государством, бизнесом и гражданским обществом, а также пересмотра образовательных программ в сторону повышения цифровой грамотности на всех уровнях.

Таким образом, дальнейшее развитие цифрового общества требует сбалансированного подхода, включающего совершенствование нормативно-правовой базы, внедрение современных технологий защиты информации, повышение цифровой грамотности населения и развитие международного сотрудничества в сфере кибербезопасности.

Литература

[1] Волков В. Э. Цифровое право. Общая часть: учеб. пособие. Самара: Издательство Самарского университета, 2022. 110 с.

[2] Киселева Л. С., Семёнова А. А. Цифровая трансформация общества: тенденции и перспективы // Проблемы деятельности ученого и научных коллективов. 2018. № 4 (34). С. 157-169.

[3] Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М. С., Русанов А. А. Модель цифровых навыков кибербезопасности // Современные информационные технологии и ИТ-образование. 2020. № 3. С. 695-710. DOI: 10.25559/SITITO.16.202003.695-710.

[4] Лукошкин А. А. Цифровая безопасность личности в условиях развития цифрового права // Образование и право. 2024. № 1. С. 475-482. DOI:10.24412/2076-1503-2024-1-475-482.

[5] Пучков Д. В. Проблемы взаимодействия кибертехнологий с моралью и правом в современном обществе // Проблемы права. 2017. № 5 (64). С. 95-102.

[6] Авдеева И. А. Информационная, компьютерная и прикладная этика как теоретические составляющие этики глобального коммуникативного пространства // Вестник ТГУ. 2014. № 9 (137). С. 7-13.

[7] Baird R., Ramsower R., Rosenbaum S. Cyberethics: Social & Moral Issues in the Computer Age. Amherst, NY: Prometheus Books, 2000. 335 p.

[8] Грэм Д. Г. Этичный хакинг. Практическое руководство по взлому // СПб.: Питер. 2023. 384 с.

[9] Капустин Ф. А. Информационная безопасность и защита информации в современном обществе // Актуальные проблемы авиации и космонавтики. 2016. № 12. С. 56-58.

[10] Морозова С. С., Смирнова Ю. Г. Особенности правового регулирования цифрового управления и безопасности в современной России // Политэкс. 2023. № 1. С. 123-132.
[11] Губенко Н. Е., Потреба Е. Ю. Анализ методов и средств предотвращения утечек конфиденциальных данных // Проблемы искусственного интеллекта. 2023. № 3(30). С. 55-64. DOI: 10.34757/2413-7383.2023.30.3.005.

Leaks of Confidential Data in the Digital Age: Ethical and Legal Aspects of Cybersecurity

S. Vashchenko

Saint Petersburg State University

The article analyzes the ethical and legal aspects of digital security in the context of growing cyber threats and societal transformation driven by digital technologies. It examines the ethical principles underlying the fight against cybercrime, including accountability for actions in cyberspace. Special attention is given to the causes of confidential data breaches and an analysis of legal mechanisms aimed at ensuring cybersecurity, with an assessment of their effectiveness. The study explores key challenges related to data breaches, including technological vulnerabilities, shortcomings in legal regulation, and ethical dilemmas in cyberspace. Focus is placed on the reasons behind the rise in cybercrime, such as the increasing complexity of cyber systems, the lack of international data protection standards, and low user awareness. An analysis of breach statistics and regulatory practices demonstrates that modern cybersecurity mechanisms often fail to keep pace with evolving threats, necessitating a reevaluation of existing approaches. The main finding of the study is the identification of systemic contradictions between technological progress, legal regulation, and ethical norms. Examining specific data breach cases reveals that they result not only from technical factors (API vulnerabilities, human error) but also from weak enforcement mechanisms, especially compared to the stringent General Data Protection Regulation standards. An assessment of cyber ethics principles (confidentiality, transparency, accountability) confirms their largely declarative nature in the absence of effective implementation tools. At the same time, initiatives such as Russia’s «Digital Ethics Charter» and ethical hacking practices demonstrate the potential of combining «soft» regulation with technological solutions.

Keywords: digital security, cybersecurity, cyber ethics, confidential data breaches, cyber threats, cybercrime

Reference for citation: Vashchenko S. A., Leaks of Confidential Data in the Digital Age: Ethical and Legal Aspects of Cybersecurity // Information Society: Education, Science, Culture and Technology of Future. Vol. 9 (Proceedings of the XXVIII International Joint Scientific Conference «Internet and Modern Society», IMS-2025, St. Petersburg, June 23–25, 2025). – St. Petersburg: ITMO University, 2025. P. 103-114. DOI: 10.17586/3033-5574-2025-9-103-114.

Reference

[1] Volkov V. E. Cifrovoe pravo. Obshchaya chast': ucheb. posobie. Samara: Izdatel'stvo Samarskogo universiteta, 2022. 110 p. (In Russian)
[2] Kiseleva L. S., Semenova A. A. Digital transformation of society: trends and prospects // Problemy deyatel'nosti uchenogo i nauchnykh kollektivov. 2018. No. 4(34). P. 157-169.
[3] Sukhomlin V. A., Belyakova O. S., Klimina A. S., Polyanskaya M. S., Rusanov A. A. A Cybersecurity Digital Skills Model 2020 // Sovremennye informatsionnye tekhnologii i IT-obrazovanie. 2020. No. 3. P. 695-710. DOI: 10.25559/SITITO.16.202003.695-710. (In Russian)

[4] Lukoshkin A. A. Digital security of the individual in the context of the development of digital law // Obrazovanie i pravo. 2024. No. 1. P. 475-482. DOI:10.24412/2076-1503-2024-1-475-482. (In Russian)
[5] Puchkov D. V. Problems of interaction of cyber technologies with morality and law in modern society // Problemy prava. 2017. No. 5(64). P. 95-102. (In Russian)
[6] Avdeeva I. A. Information, computer and applied ethics as theoretical components of global communication space // Vestnik Tomskogo gosudarstvennogo universiteta. 2014. No. 9 (137). P. 7-13. (In Russian)
[7] Baird R., Ramsower R., Rosenbaum S. Cyberethics: Social & Moral Issues in the Computer Age. Amherst, N Y: Prometheus Books, 2000. 335 p.
[8] Graham D. G. Etichnyj haking. Prakticheskoe rukovodstvo po vzlomu. // St. Petersburg: Piter, 2023. 384 p.
[9] Kapustin F. A. Information security and data protection in modern society // Aktual'nye problemy aviatsii i kosmonavtiki. 2016. No. 12. P. 56-58. (In Russian)
[10] Morozova S. S., Smirnova Yu. G. Features of digital government and security legal regulation in modern Russia. // Politeks. 2023. No. 1. P. 123–132.
[11] Gubenko N. E., Potreba E. Yu. Analysis of methods and means of preventing confidential data leaks // Problemy iskusstvennogo intellekta. 2023. No. 3 (30). P. 55-64. DOI: 10.34757/2413-7383.2023.30.3.005. (In Russian)