Диденко С.В.
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южный федеральный университет»

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ПРОЕКТОВ ГОСУДАРСТВЕННО – ЧАСТНОГО ПАРТНЕРСТВА

Аннотация: *В условиях развития механизмов государственно – частного партнерства особую значимость приобретает информационная безопасность, особенно безопасность использования персональных данных. С переходом на электронные платформы, где осуществляется обмен данными между государственными органами и частными партнерами, риски утечек информации и взломов систем существенно повышаются. Это вызывает необходимость разработки и внедрения современных технологий защиты информации, которые способны предотвратить несанкционированный доступ и обеспечить целостность данных. Регулирование данного вопроса требует усовершенствованного законодательства для обеспечения эффективного взаимодействия государства и общества. Разработка и внедрение методов информационной безопасности в системе государственно – частного партнерства обуславливает актуальность данного вопроса. Эффективные механизмы защиты информации в условиях цифровизации включают в себя многоуровневые стратегии, направленные на предотвращение утечек, несанкционированного доступа и искажения данных.*

Ключевые слова: *государственно – частное партнерство, цифровизация, информационная безопасность, электронные платформы, персональные данные, частные партнеры*

Didenko S.V.
Federal State Autonomous
Educational Institution of Higher Education
Southern Federal University

ENSURING INFORMATION SECURITY WHEN IMPLEMENTING PUBLIC–PRIVATE PARTNERSHIP PROJECTS

Abstract: In the context of the development of public–private partnership mechanisms, information security, especially the security of the use of personal data,

is of particular importance. With the transition to electronic platforms where data is exchanged between government agencies and private partners, the risks of information leaks and hacking systems are significantly increased. This necessitates the development and implementation of modern information security technologies that can prevent unauthorized access and ensure data integrity. Regulation of this issue requires improved legislation to ensure effective interaction between the State and society. Development and implementation of information security methods

Цифровая трансформация кардинально меняет структуру и динамику современного общества. Технологические новшества влияют на все аспекты нашей жизни: от общения и образования до экономики и политики. Важным аспектом развития общества в условиях цифровизации становится адаптация к новым условиям.

Информационные технологии и информационно – коммуникационые системы являются ключевыми ресурсами общества и государства. В условиях цифровизации особую значимость приобретает информационная безопасность. Переход к электронным системам требует от государства не только внедрения новых технологий, но и обеспечения защиты данных, которые обрабатываются в этих системах. При реализации проектов государственно – частного партнерства утечка конфиденциальной информации или кибератаки могут нанести серьезный ущерб, как самому государству так и частному партнеру.

Основной задачей является защита персональных данных всех участников проектов государственно – частного партнерства, что требует не только технических решений, но и создания четкой правовой базы. Законодательство должно предусмотрительно реагировать на новые вызовы и обеспечивать защиту прав всех сторон проекта.

Основным критерием эффективности обеспечения информационной безопасности является высокий уровень безопасности в информационной среде и минимизации соответствующих затрат. Совокупность внутренних и внешних информационных угроз создают предпосылки нарушения эффективного функционирования системы государственно – частного партнерства.

Информационная безопасность в системе государственно – частного партнерства является актуальным аспектом стабильного и стойкого состояния данной системы, которая при влиянии внутренних и внешних угроз сохранит существенно важные данные для стабильного функционирования и развития.

Персональные данные представляют собой любую информацию, относящуюся к идентифицированному или идентифицируемому лицу. В современном цифровом мире, где технологии играют ключевую роль в повседневной жизни, защита таких данных становится особенно актуальной. В процессе государственно-частного партнерства используются значительные объемы персональных данных — от имени, фамилии, адреса до более чувствительных данных, таких как финансовые показатели.

Использование персональных данных в государственно – частном партнерстве представляет собой двойственный процесс, который требует внимательного подхода и соблюдения правовых норм.

Ключевым аспектом в этом контексте является обеспечение защиты персональных данных. Государственные органы обязаны соблюдать законы о конфиденциальности и демократических принципах, гарантируя, что информация используется исключительно в законных целях. Это предполагает наличие четких регламентов о том, кто имеет доступ к данным, а также за счет каких процедур осуществляется их обработка и хранение.

Кроме того, важно развивать культуру ответственного использования персональных данных среди государственных служащих. Обучение и повышение осведомленности о рисках, связанных с утечкой информации, помогут избежать потенциальных угроз, как для граждан, так и для самой системы государственного управления. Эффективный подход к управлению персональными данными в органах власти будет способствовать не только росту доверия к государственным институтам, но и улучшению общего климата в обществе.

С увеличением объема собираемых данных растет и угроза их утечки. Хакеры и мошенники постоянно совершенствуют свои методы, и случаи нарушения безопасности становятся все более частыми. В связи с этим усовершенствование законодательной базы о защите персональных данных, становятся необходимыми мерами для обеспечения конфиденциальности и безопасности пользователей.

Развитие информационно – коммуникационных процессов в условиях цифровой трансформации дает основание рассматривать обеспечение информационной безопасности, как одну из глобальных и приоритетных задач государственного и муниципального управления.

Современные технологии обработки информации и персональных данных предусматривают использование информационных систем. Данные системы представляют собой взаимосвязанную совокупность средств, методов и персонала, которые обеспечивают сбор, хранение, обработку, передачу и отображение информации с целью достижения поставленных целей. Информация является основным компонентом информационных систем. При этом объектом защиты является информационная система, с помощью которой обрабатывается информация с применением соответствующих информационных технологий, сами информационные технологии и сама информация.

Реализация проектов государственно-частного партнерства (ГЧП) предполагает интенсивный обмен персональными данными между государственным и частным партнерами, а также с третьими лицами. Это требует особого внимания к обеспечению их защиты, согласно требованиям Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных".

Ключевые аспекты защиты включают: определение цели обработки данных, объема обрабатываемых данных, сроков хранения и круга лиц,

имеющих к ним доступ. Необходимо разработать и внедрить организационные и технические меры, обеспечивающие конфиденциальность и безопасность персональных данных. Важно предусмотреть порядок реагирования на инциденты, связанные с утечкой или неправомерным доступом к информации.

Ответственность за соблюдение требований законодательства о персональных данных несут как государственный, так и частный партнеры. Договор государственно – частного партнерства должен четко регламентировать распределение ответственности и полномочий в этой сфере. Независимая оценка рисков и регулярный аудит системы защиты данных необходимы для поддержания ее эффективности.

Необходимо также учитывать специфику каждого конкретного проекта государственно – частного партнерства. Например, если проект связан с созданием или модернизацией объектов здравоохранения или образования, то требуется особое внимание к защите специальных категорий персональных данных. В таких случаях, необходимо применять дополнительные меры защиты, предусмотренные законом.

Особое внимание следует уделить процессу передачи персональных данных третьим лицам, например, субподрядчикам или поставщикам услуг. Передача данных должна осуществляться только на основании договора, содержащего положения об обеспечении конфиденциальности и безопасности данных, а также с согласия субъектов персональных данных, если это требуется законом. Важно обеспечить контроль за деятельностью третьих лиц в части обработки персональных данных.

Реализация эффективной системы защиты персональных данных в проектах государственно – частного партнерства – это не только требование законодательства, но и важный фактор повышения доверия граждан к таким проектам. Открытость и прозрачность в вопросах обработки персональных данных, предоставление субъектам данных возможности контролировать свои данные – это необходимые условия успешной и устойчивой реализации проектов государственно – частного партнерства.

Угрозы информационной безопасности делятся на внутренние и внешние. К внешним угрозам относятся угрозы, которые возникают и которыми руководят за пределами информационных систем. Внутренние угрозы возникают непосредственно в пределах информационных систем.

По проведенным исследованиям, особое внимание противодействию угрозам информационной безопасности относительно персональных данных, уделяется со стороны операторов информационных систем [5]. Практически во все информационных системах, где используются персональные данные, должны быть средства защиты, как от внутренних, так и внешних угроз. Противодействию внешним угрозам уделяется особое внимание.

Для обеспечения защиты персональных данных необходимо внедрять многоуровневую систему безопасности, которая включает в себя как технические, так и организационные меры. На первом этапе важно проводить регулярные аудиты безопасности, чтобы выявить уязвимости системы и

предотвратить возможные утечки информации. Современные технологии, такие как шифрование данных и двухфакторная аутентификация, становятся обязательными элементами в защите от внешних атак.

Также необходимо уделять внимание и внутренним угрозам. Одной из основных причин актуальности внутренних угроз является несанкционированный отток информации за пределы защищенных информационных систем. Минимизировать данные угрозы возможно путем внедрения систем противодействия внутренним угрозам информационной безопасности.

Системы мониторинга и аудита позволяют регистрировать действия пользователей и процессов в информационных системах, в том числе действия и процессы, которые связаны с использованием данных за пределами информационных систем. Данные системы являются важным средством при рассмотрении зафиксированных случаев несанкционированного оттока информации за пределы защищенных информационных систем и проведении их анализа. Недостатком данных систем является отсутствие возможности предупреждения несанкционированной утечки информации. В работе систем мониторинга и аудита не предусмотрен анализ зафиксированных событий. На данном этапе невозможно определить допустимо ли зафиксированное событие с точки зрения информационной безопасности. В данных системах также не предусмотрены какие либо алгоритмы блокирования передачи данных сетевыми каналами.

Системы аутентификации пользователей информационных систем применяются для защиты от несанкционированного доступа к персональным данным. В их основе лежит процесс аутентификации пользователей. Данный процесс может быть двухэтапный и трехэтапный. По результатам процесса аутентификации пользователю дается доступ к информационным системам или отказывается в доступе. Таким образом, предупреждается несанкционированный доступ к системам баз персональным данных. Данный способ защиты информации персональных данных не могут защитить информацию от пользователя, который по нормам безопасности имеет доступ к информационным системам, согласно должностным обязанностям, но при этом планирует использовать их в целях, которые противоречат нормам действующего законодательства.

Кроме того, сотрудники должны проходить обучение по вопросам безопасности и осознавать потенциальные риски, связанные с утечкой данных. Часто человеческий фактор играет ключевую роль в появлении угроз, и поэтому организации должны развивать культуру безопасности среди своих работников. Внедрение строгих политик в отношении доступа к данным поможет ограничить круг лиц, имеющих возможность взаимодействовать с личной информацией.

Не менее важным является постоянный мониторинг системы на предмет обнаружения подозрительной активности. Инструменты мониторинга и

реагирования на инциденты способны оперативно выявлять атаки и минимизировать их последствия. Эффективная защита персональных данных требует комплексного подхода и координации между всеми уровнями организации, что является залогом успешной борьбы с внешними угрозами.

Современные методы защиты персональных данных являются критически важными для обеспечения конфиденциальности и безопасности пользователей. Одним из основных подходов к защите данных является использование шифрования. Этот метод позволяет преобразовать информацию в недоступный формат, который может быть расшифрован только с использованием специального ключа. Существует множество алгоритмов шифрования, каждый из которых подходит для различных уровней защиты.

Методы шифрования информации изменяют данные таким образом, что их невозможно распознать без соответствующих программ. Данный метод защиты персональных данных защитит данные от утечки информации при ее обработке и хранении за пределами информационной системы, которая обладает средствами защиты.

Другим ключевым методом защиты является контроль доступа, который обеспечивает ограничение на использование и доступ к данным только авторизованным пользователям. Это может быть достигнуто с помощью многофакторной аутентификации и систем управления правами доступа, что в свою очередь снижает вероятность несанкционированного доступа и утечки данных.

Регулярное обновление программного обеспечения и использование антивирусных решений являются важными мерами для защиты от кибератак. Современные угрозы постоянно эволюционируют, и важно следить за новыми вредоносными программами и своевременно применять патчи и обновления для обеспечения максимальной безопасности персональных данных.

Также используются информационные системы выявления и предупреждения утечки информации, которые проводят сканирование возможных каналов утечки персональных данных в реальном времени, и контроль действий пользователей и процессов обработки и передачи информации в пределах информационных систем. Различают комплексные и локальные системы защиты.

Комплексные системы защиты контролируют несколько каналов утечки информации. Например, копирования на мобильные носители, сетевые каналы передачи информации.

Локальные системы контролируют лишь один из возможных каналов оттока информации, в основном сетевой. Дополнительной функцией данных систем защиты может быть шифрование данных в процессе записи на внешние носители или в процессе формирования в файлы.

Не менее значимой мерой является внедрение строгих стандартов и протоколов в области безопасности информации. Разработка и интеграция таких стандартов не только обеспечит единую базу для защиты персональных данных, но и создаст условия для их гармоничной совместимости с

международными нормами. Это, в свою очередь, повысит уровень защиты данных на глобальном уровне и упростит взаимодействие с партнёрами.

Не менее важным аспектом является соблюдение принципа прозрачности в вопросах использования персональных данных. Граждане должны быть информированы о том, какие данные собираются, с какой целью и как они будут использоваться. Это укрепит доверие между государственными органами и обществом, обеспечив уверенность в том, что личная информация обрабатывается с уважением и заботой.

Но, несмотря на все приведенные аргументы, законодательство по использованию персональных данных и их защите требует постоянного усовершенствования.

Главной причиной, по которой необходимо совершенствование законодательства, является быстрое развитие технологий. С каждой новой инновацией открываются новые возможности для сбора и анализа персональных данных. Это может привести к неправильному использованию информации и нарушению прав граждан. Законодательные инициативы должны быть гибкими и адаптивными, чтобы успевать за темпами прогресса, обеспечивая при этом защиту прав пользователей.

Создание эффективной правовой базы, способной адаптироваться к меняющимся условиям, позволит не только защитить права граждан, но и способствовать инновациям в сфере информационных технологий.

В условиях быстрого развития технологий, правовая система должна быть гибкой и динамичной, чтобы реагировать на новые вызовы и угрозы. Это означает необходимость регулярного пересмотра и обновления законодательства, которое учитывало бы последние достижения в области цифровых технологий и интернет - безопасности.

Предложения по усовершенствованию законодательной базы, относительно защиты использования персональных данных, включает в себя разработку законодательных норм, которые регулируют новые технологии и платформы, а также создание новых систем защиты.

Современные технологии стремительно развиваются, и законодательство должно адаптироваться к этим изменениям. Во-первых, необходимо внедрить нормы, которые бы регулировали использование искусственного интеллекта и машинного обучения в обработке персональных данных. Эти технологии могут существенно ухудшить уровень защиты личной информации, если их работа не будет четко регламентирована. Важно, чтобы закон создавал четкие критерии для алгоритмов, используемых в таких системах, а также обеспечивал прозрачность процессов обработки данных.

Вывод: Результаты проведенных исследований показывают, что предупреждению утечки персональных данных способствует усиление контроля каналов их передачи. Данный контроль необходимо осуществлять с использованием технологий и систем, которые предусматривают мониторинг информации, которая передается сетевыми каналами. При этом технологии должны выявлять персональные данные в информации, которая передается.

Анализ существующих методик и подходов показывает, что разработка оптимальных технологий защиты персональных данных базируется на объединении существующих методик контекстного анализа информации с учетом формата их передачи, а также алгоритмов реагирования на попытки взлома персональных данных с целью их передачи. При этом необходимо формирование и поддержка специальных баз данных, которые позволяют проводить анализ и реализацию алгоритмов выявления несанкционированной передачи информации.

Список использованных источников

1. Аверченков, В.И.. Защита персональных данных в организации [Текст] : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. — 2-е изд.,стереотип. — Москва : ФЛИНТА, 2011. — 125 с. : ил. : 21 см.; ISBN 978-5-9765-1273-3.
2. Булетова, Н. Е. Моделирование публично-частного партнерства в рамках цифровой трансформации ФНС России / Н. Е. Булетова, Г. В. Кузибецкая, В. В. Чигаров // Бизнес. Образование. Право. – 2023. – № 3(64). – С. 168-172.
3. Дербин, Е.А. Организационные основы обеспечения информационной безопасности предприятия [Электронный ресурс]: Учебное пособие для студ., обуч. по напр. 090900.68 "Информационная безопасность" / Е.А. Дербин, С.М. Климов; Финуниверситет, Каф. "Информационная безопасность". — Электронные текстовые данные (1 файл: 7.1 Мб). — М.: Финуниверситет, 2013. — Только электронный ресурс. — Доступ на портале Финуниверситета: http://http://portal.ufrf.ru/Content/Data/bfe5ac2d-d57d-4f4a-9929-3d440cab52cb/Elektr_uch._posobie_OOIB1.pdf.
4. Костенко, Д. С. Международный опыт государственно-частного партнерства в сфере обеспечения кибербезопасности / Д. С. Костенко // Право в информационном обществе: трансформация или модернизация? : Материалы V Международного сравнительно-правового конгресса, Красноярск, 20–22 сентября 2018 года. – Красноярск: Сибирский федеральный университет, 2019. – С. 197-202.
5. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и органах местного самоуправления : учебно-методическое пособие / В.А. Мещеряков [и др.]; под ред. В.А. Мещерякова. – Воронеж: Правительство Воронежской области, 2016. – 208 с.