Закрытое акционерное общество «Центр Цифровых Сертификатов»

Место нахождения: г. Новосибирск
Почтовый адрес: 630055, г. Новосибирск, ул. Шатурская, д. 2
ИНН 5407187087; КПП 540801001; БИК 045004832
р/с 40702810300000000075 в РНКО «Платежный Центр» (ООО)
к/с 30103810100000000832 в Сибирском ГУ Банка России
тел/факс: 8 (383) 336-49-49

Информационное письмо о соблюдении требований к информационной безопасности в сервисе «Безбумажный офис F.Doc»

Уважаемый Пользователь!

Основными риски, с которыми пользователи информационных систем и ресурсов регулярно сталкиваются являются: утечка данных (включая утечку конфиденциальной информации); изменение информационных данных; финансовые и репетиционные потери.

В системе электронного документооборота помимо вышеуказанных существуют дополнительные риски:

1. **Угроза DDoS-атак**.

Атаки на инфраструктуру сервиса могут привести к временной недоступности системы, что может негативно повлиять на бизнес-процессы. Кроме того, злоумышленники могут попытаться проникнуть в систему, чтобы получить несанкционированный доступ к конфиденциальным данным с помощью вирусов или вредоносных программ.

2. **Фишинг и социальная инженерия**.

Целью атаки, направленных на пользователей, может являться получение конфиденциальной информации, например, пароля или персональных данных.

3. **Риски утечки данных**.

Недостаточная защита данных может привести к случайным или преднамеренным утечкам конфиденциальной информации. Это может нанести ущерб репутации компании, привести к возникновению риска получения штрафа за нарушение законодательных требований к защите данных.

4. **Неприменение необходимых методов безопасности при работе в системе** (отсутствие методов аутентификации и авторизации при входе и в работе в системе).

Из-за слабой системы управления доступом к данным неуполномоченные третьи лица могут получить доступ к конфиденциальной информации или проводить мошеннические операции от имени других пользователей.

5. **Риски возникновения нарушений целостности данных**.

Изменение или фальсификация данных в электронных документах могут негативно отразиться на отношениях участников электронного взаимодействия, стать причиной появления недоверия сторон электронного документооборота к системе в целом.

6. **Внутренние угрозы**.

Уполномоченные для работы в системе сотрудники, имеющие права управления данными в системе, являются потенциальным источником угроз информационной безопасности. Это риск возрастает при отсутствии у указанных сотрудников необходимых для работы в системе знаний в части соблюдения требований информационной безопасности.

ЗАО «ЦЦС», осознавая в должной мере масштаб возможных негативных последствии при реализации угроз информационной безопасности, разработал комплексную стратегию безопасности сервиса «Безбумажный офис F.Doc» (далее-«Сервис»), включающую, в том числе технические, организационные, физические и обучающие меры и методы защиты конфиденциальной информации, а именно:

1. **Организационные меры защиты конфиденциальной информации**.

a. Разработка организационно распорядительных документов, регламентирующих вопросы защиты информации (политики, стандарты, положения, регламенты, порядки и т.д).

Доступ к конфиденциальной информации имеют только сотрудники, которым необходимо обрабатывать информацию для выполнения своих служебных полномочий (ограниченный доступ с соблюдение принципов минимизации прав и полномочий). Каждый такой сотрудник подписывает обязательство о сохранности информации ограниченного доступа. Для контроля доступа используется автоматизированная система контроля доступа.

b. Проведение внешних и внутренних аудитов.

С целью проведения тестирования на возможность проникновения извне во внутренний контур Сервиса ЗАО «ЦЦС» регулярно привлекает специализированные организации, имеющие соответствующие лицензии. Кроме того проводятся внутренние проверки соответствия существующих политик и процедур требованиям безопасности, осуществляется оценка эффективности используемых мер безопасности, в ходе которых выявляются уязвимости и формируются рекомендации по их устранению.

2. **Физические меры защиты конфиденциальной информации**.

Хранилище электронных документов размещено в ЦОДе. Помещения ЦОДа расположены на территории РФ. Доступ на территорию ЦОДа осуществляется в соответствии с правилами внутриобъектового режима и контролируется оперативными дежурными. Доступ в ЦОДа возможен только по индивидуальным пропускам. Доступ в серверные и телекоммуникационные ЦОДа ограничен списком уполномоченных сотрудников. На территории ЦОДа ведется видеонаблюдение. В ЦОДе установлена и функционирует газовая система пожаротушения. Серверы оснащены источниками бесперебойного питания и несколькими дизельгенераторами.

3. **Технические средства защиты конфиденциальной информации.**

a. Система предотвращения утечек данных.

В рамках повышения уровня защищенности данных в Сервиса, а также с целью усиления системы внутреннего контроля обработки, передачи и хранения информации конфиденциального характера (в том числе персональных данных) для объектов информационной инфраструктуры Сервиса внедрена система предотвращения утечек конфиденциальной информации (Data Leak Prevention, DLP) InfoWatch Traffic Monitor.

b. Системы обнаружения и предотвращения вторжений.

В Сервисе используются IDS (Intrusion Detection System)/ IPS (Intrusion Prevention System) - системы обнаружения и предотвращения вторжений. IDS/IPS анализируют данные и сетевое поведение для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки, направленные на нарушение защиты Сервиса, атаки, на повышение привилегий (прав доступа) к работе в Сервисе, а также направленные на получение неавторизованного доступа к файлам, на запуск в систему вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

c. Защита приложений от атак.

Для защиты атак на прикладном уровне применяется система защиты от атак межсетевым экраном приложений Web Application Firewall (WAF) компании Positive Technologies (PT), которая имеет действующий сертификат ФСТЭК и обеспечивает непрерывную защиту приложений за счет выявления и блокирования атак, включая атаки из списка OWASP ТОП-10, классификации WASC и атак нулевого дня, а также не позволяет злоумышленникам использовать уязвимости.

d. Защита от воздействия вредоносного кода.

В инфраструктуре Сервиса применяются средства антивирусной защиты на уровне физических АРМ Пользователей и эксплуатационного персонала, серверного оборудования, контроля межсетевого трафика, контроля почтового трафика, входного контроля устройств и переносных (отчуждаемых) носителей информации. Средства защиты от вредоносного кода функционируют в постоянном автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных. Применяются средства, реализующие функцию контроля целостности их программных компонентов.

e. Применение принципов безопасной разработки.

Secure Software Development Lifecycle (SSDL) - это методология разработки программного обеспечения, ориентированная на обеспечение безопасности приложений на всех этапах их жизненного цикла. Она включает в себя ряд шагов, практик и стандартов, направленных на минимизацию уязвимостей и повышение защиты программного обеспечения от атак. Основные принципы SSDL включают анализ угроз, применение безопасных практик разработки, тестирование на безопасность и постоянное обновление защитных мер. Реализация SSDL помогает предотвратить множество видов уязвимостей и сделать программное обеспечение более надежным и безопасным для конечных пользователей.

f.Резервное копирование и восстановление.

Регулярное создание резервных копий данных и разработка планов восстановления позволяют минимизировать последствия инцидентов информационной безопасности и быстро восстановить работоспособность системы.

g. Анализ и мониторинг безопасности

Применение специализированных инструментов для анализа и мониторинга безопасности помогает выявлять аномалии и предупреждать о потенциальных угрозах.

Обеспечение надёжной защиты при организации подписания и обмене электронными документами является для ЗАО «ЦЦС» одной из приоритетных задач. Проведенный анализ возможных рисков информационной безопасности для работы Программы «Безбумажный офис F.Doc» показал, что предусмотрены все необходимые меры для обеспечения надежной информационной безопасности.

Сервис «Безбумажный офис F.Doc» имеет сертификат соответствия, свидетельствующий о высоком уровне безопасности внешнего контура Программы для ЭВМ «Безбумажный офис F.Doc» (сертификат № РТМ-19/23 от 29.12.2023 г.).

Директор ЗАО «ЦЦС» А.В. Гудков