УДК 004 **Информационные технологии**

Кадомец Кристина Сергеевна, *магистрант, ДГТУ, Ростов-на-Дону, РФ*

МЕТОДЫ ИНТЕГРИРОВАННОЙ ЗАЩИТЫ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ПРЕДПРИЯТИИ

Аннотация: В цифровую эпоху, когда информация является источником жизненной силы организаций, эффективное управление электронными документами и их защита имеют первостепенное значение для их успеха и безопасности. Системы электронного документооборота стали основой современных предприятий, обеспечивая эффективное хранение, поиск и совместную работу над важной информацией. Однако с ростом распространенности киберугроз и утечек данных для организаций крайне важно внедрить надежные методы интегрированной защиты для защиты своих систем электронного документооборота.

Внедряя эти методы интегрированной защиты, предприятия могут снизить риск несанкционированного доступа, утечки данных и потери информации. Они могут защитить свои системы электронного документооборота от внешних и внутренних угроз, создав безопасную среду для конфиденциальных данных и укрепив доверие заинтересованных сторон.

Ключевые слова: персональные данные, защита данных, информационная безопасность.

Annotation: Fast workflow mechanisms have become priority enterprises, discovery discovery, search and collaboration on reliability. However, with the rise of cyber threats and data breaches, it is essential for organizations to implement strong internal security mechanisms to protect their system documents.

By implementing these end-to-end security methods, an enterprise reduces the risk of unauthorized access, data leakage, and information loss. They can create their

own workflow against external and internal threats by creating secure data protection for sensitive data and building trust in external manifestations.

Key words: personal data, data protection, information security.

Введение

В сегодняшнюю цифровую эпоху эффективное управление электронными документами и их защита имеют первостепенное значение для успеха и безопасности предприятий. С ростом зависимости от систем электронного документооборота организации должны внедрять надежные методы интегрированной защиты для защиты своей конфиденциальной информации. В этой работе будут рассмотрены различные стратегии и методы, которые можно использовать для обеспечения целостности, конфиденциальности и доступности электронных документов на предприятии.

Основная часть

Комплексная система защиты электронного документооборота относится к набору интегрированных мер, стратегий и практик, используемых организацией для обеспечения безопасности, целостности, конфиденциальности и доступности ее системы электронного документооборота (EDMS). Она включает в себя целый ряд защитных мер, которые работают сообща для защиты электронных документов от различных угроз, уязвимостей и рисков.

Такая система обычно включает в себя несколько уровней контроля безопасности и мер предосторожности, которые касаются различных аспектов защиты. Они могут включать:

Контроль доступа: внедрение надежных механизмов аутентификации, таких как пароли, биометрические данные или двухфакторная аутентификация, для проверки личности пользователей и предоставления им соответствующих прав доступа в соответствии с их ролями и обязанностями.

Шифрование: Использование алгоритмов и протоколов шифрования для защиты конфиденциальности электронных документов как при хранении, так и при передаче, гарантируя, что только уполномоченные лица смогут

расшифровать информацию.

Резервное копирование и восстановление данных: Регулярное создание резервных копий электронных документов для предотвращения потери данных и обеспечения их доступности в случае системных сбоев, катастроф или кибератак. Это включает в себя хранение резервных копий в безопасных местах и тестирование процесса восстановления.

Меры безопасности: Внедрение брандмауэров, систем обнаружения вторжений, антивирусного программного обеспечения и других средств безопасности для обнаружения и предотвращения несанкционированного доступа, заражения вредоносными программами и других внешних угроз.

Мониторинг и ведение журнала: Постоянный мониторинг EDMS на предмет любых подозрительных действий или попыток несанкционированного доступа и ведение подробных журналов действий пользователей и системных событий. Это позволяет своевременно обнаруживать инциденты безопасности, реагировать на них и расследовать их.

Обучение пользователей и повышение их осведомленности: Проведение регулярных тренингов по повышению осведомленности о безопасности с целью ознакомления сотрудников с передовыми практиками, потенциальными угрозами и их ролью в поддержании безопасности СЭД. Это способствует формированию культуры безопасности и снижает риск человеческих ошибок или инсайдерских угроз.

Регулярные оценки и аудиты: Проведение оценок уязвимостей, тестирования на проникновение и аудитов для выявления и устранения любых слабых мест в системе безопасности или уязвимостей в EDMS. Это помогает организациям заблаговременно повышать уровень своей безопасности и обеспечивать соблюдение соответствующих правил и стандартов.

Одним из основных методов комплексной защиты является реализация надежного механизма контроля доступа. Контроль доступа включает в себя проверку личности пользователей и предоставление им соответствующих разрешений на доступ и изменение электронных документов. Используя строгие

методы аутентификации, такие как двухфакторная аутентификация или биометрия, предприятия могут значительно снизить риск несанкционированного доступа. Кроме того, использование управления доступом на основе ролей позволяет организациям назначать определенные привилегии на основе должностных ролей и обязанностей, гарантируя, что только уполномоченный персонал может выполнять определенные действия с конфиденциальными документами.

Шифрование играет решающую роль в защите конфиденциальности электронных документов. Шифруя данные как в состоянии покоя, так и при передаче, организации могут снизить риск несанкционированного доступа и утечки данных. Надежные алгоритмы шифрования, такие как Advanced Encryption Standard (AES), могут использоваться для шифрования содержимого электронных документов, что делает их недоступными для чтения посторонними лицами. Этот метод гарантирует, что даже если злоумышленник получит доступ к документам, он не сможет расшифровать информацию без ключа шифрования. Кроме того, протоколы безопасной передачи, такие как Secure Sockets Layer (SSL) или Transport Layer Security (TLS), могут использоваться для шифрования данных во время их передачи по сети, гарантируя их конфиденциальность.

Регулярное резервное копирование данных — еще один важный аспект комплексной защиты систем электронного документооборота. Предприятиям следует внедрить автоматизированные механизмы резервного копирования для создания избыточных копий важных документов. Регулярно создавая резервные копии электронных документов, организации могут снизить риск потери данных из-за сбоев оборудования, стихийных бедствий или кибератак. Крайне важно хранить резервные копии в безопасных местах, предпочтительно за пределами офиса или в облаке, чтобы обеспечить их доступность в случае возникновения чрезвычайных ситуаций. Регулярное тестирование процессов резервного копирования и восстановления также необходимо для проверки целостности и надежности системы резервного копирования.

Крайне важно внедрить надежные меры безопасности для защиты от

внешних угроз, таких как вредоносное ПО, фишинговые атаки или несанкционированный доступ к сети. Этого можно достичь за счет использования брандмауэров, систем обнаружения и предотвращения вторжений и программного обеспечения для защиты от вредоносных программ. Предприятия должны регулярно обновлять и исправлять свои программные системы для защиты от недавно обнаруженных уязвимостей. Обучение сотрудников вопросам безопасности также имеет решающее значение для информирования их о потенциальных угрозах, таких как социальная инженерия или попытки фишинга, а также для продвижения культуры безопасности в организации.

Журналы аудита и механизмы регистрации играют жизненно важную роль в интегрированной защите систем электронного документооборота. Ведя подробные записи о действиях пользователей и системных событиях, организации могут отслеживать и обнаруживать любые подозрительные или несанкционированные действия. Эти журналы могут предоставить ценные доказательства в случае инцидентов безопасности и помочь в расследовании и устранении потенциальных нарушений. Регулярный анализ и просмотр журналов аудита может помочь выявить слабые места в системе безопасности и принять соответствующие меры для усиления защиты электронных документов.

Наконец, непрерывный мониторинг и периодические оценки безопасности имеют решающее значение для обеспечения эффективности комплексных мер защиты. Внедряя элементы управления безопасностью, такие как системы обнаружения вторжений и решения для управления информацией и событиями безопасности (SIEM), организации могут заблаговременно обнаруживать инциденты безопасности и реагировать на них. Регулярные оценки уязвимостей и тестирование на проникновение могут выявить потенциальные недостатки в системе управления электронными документами, позволяя организациям устранять их до того, как ими воспользуются злоумышленники.

Вывод

В заключение следует отметить, что комплексная защита систем

электронного документооборота жизненно важна для безопасности и успеха предприятий. Применяя комплексный подход, включающий механизмы контроля доступа, шифрование, резервное копирование данных, надежные меры безопасности, журналы аудита и непрерывный мониторинг, организации могут эффективно защищать свою конфиденциальную информацию. Предприятиям крайне важно осознавать развивающиеся.

Библиографический список:

1. Белов С.П. Подготовка к внедрению систем электронного документооборота: Монография. - М.: Мир науки, 2016. - 210 с.

2. Анацкая А.Г. Защита электронного документооборота: Учебное пособие. - Омск: СибАДИ, 2019. - 87 с.

3. Шишин И.О. Информационные технологии управления документами. - СПб.: Санкт-Петербургский государственный экономический университет, 2017. - 78 с.