**Исследование систем безопасного и доверенного электронного документооборота организации**

**Аннотация**

В статье исследуются вопросы обеспечения безопасности в системах электронного документооборота (СЭД) в условиях цифровой трансформации. Проведен сравнительный анализ традиционного и электронного документооборота, выявлены ключевые преимущества современных СЭД, а также новые угрозы, связанные с утечкой данных, кибератаками и несанкционированным доступом. Особое внимание уделено необходимости внедрения надежных систем управления информационной безопасностью (СУИБ) для защиты конфиденциальной документации и персональных данных.

Целью исследования является разработка СЭД с усовершенствованными алгоритмами СУИБ, способными эффективно противодействовать современным угрозам. В работе решаются следующие задачи:

* анализ актуальных угроз информационной безопасности в электронном документообороте;
* обзор существующих решений СЭД и СУИБ;
* разработка и тестирование системы с усиленными механизмами защиты.

Ключевые слова

Электронный документооборот, информационная безопасность, СУИБ, защита данных, киберугрозы, цифровая трансформация, «1С:Предприятие».

Введение

До появления электронного документооборота использовался традиционный документооборот. Безопасность обеспечивалась преимущественно физическими или организационными мерами, что было эффективно для своего времени, но также требовало множество затрат на персонал и помещения для хранения документов. С развитием информационных технологий появились системы управления электронным документооборотом организации, которые стали важнейшим звеном в управлении деятельностью организации 21 века. С их появлением полностью изменились подходы к безопасности документооборота организации. Электронный документооборот расширил инструментарии безопасности, теперь они стали технологичными и более эффективными, но при этом и степень гроз для документооборота также вырос.

В настоящее время существует множество решений систем электронного документооборота, которые выполняют функционал, необходимый для ведения документооборота, в полном объеме. Все эти решения были разработаны с использованием современных стандартов по обеспечению информационной безопасности этих систем. Чтобы обеспечить безопасность систем электронного документооборота, необходимо внедрять надежные СУИБ – системы управления информационной безопасностью. Система способна обеспечивать безопасность электронного документооборота в рамках всей организации, поэтому так важно использовать надежные алгоритмы СУИБ, способных эффективно противодействовать развивающимся угрозам безопасности.

**Основной текст**

Электронные документы представляют интерес для мошенников по ряду причин:

* электронные документы содержат конфиденциальную информацию, которые мошенники могут использовать для получения выгоды;
* техническое несовершенство систем позволяет взламывать защиту;
* мошенники могут использовать быстрые схемы обмана.

Электронные документы, как и бумажные подвержены риску и требуют серьезной защиты от различных угроз. Если раньше главной опасностью было физическое похищение документов, то теперь главные риски – это риски, связанные с кибератаками и уязвимостями ПО.

Угрозы для СЭД могут быть внешними и внутренними[16]. К внешним угрозам относятся:

* кибератаки и вредоносное ПО;
* взлом и несанкционированный доступ;
* уязвимости в программном обеспечении;
* природные катастрофы (наводнения, ураганы);
* сбои в электроснабжении;
* другие угрозы от внешних источников.

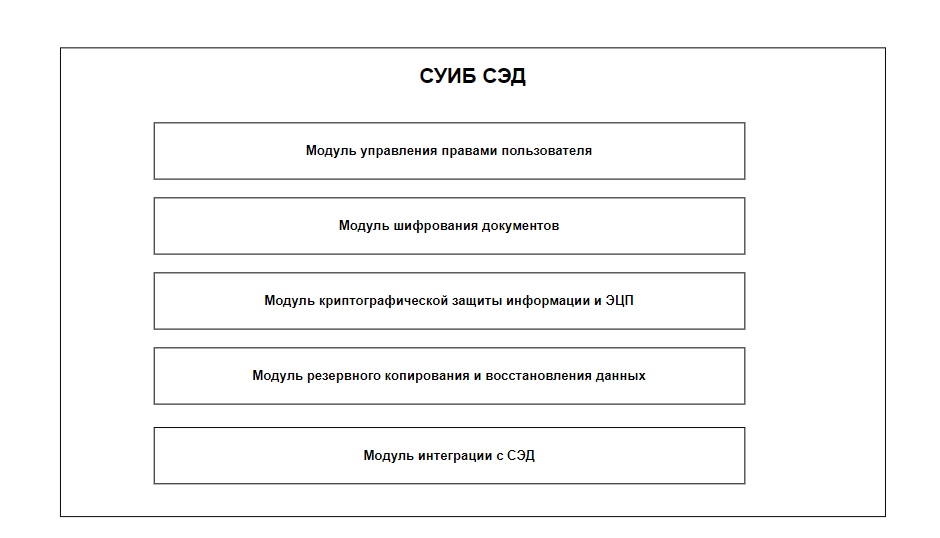
К внутренним угрозам относятся:

* неправильное использование корпоративных систем;
* нарушение установленных правил безопасности;
* случайные ошибки сотрудников;
* непреднамеренное раскрытие информации;
* умышленный саботаж.

Если не обеспечивать должную безопасность электронного документооборота, это может привести к ряду проблем, таким как:

* прямым убыткам организации;
* ухудшению деловой репутации;
* несанкционированному доступу к конфиденциальной информации;
* репутационным потерям;
* снижению конкурентоспособности;
* хакерским атакам;
* проблемам с доступностью данных.

Представим компонентную модель, которая отображает основные методы защиты в системах электронного документооборота. Она представлена ниже.



Компонентная модель СУИБ

При анализе систем электронного документооборота обратим внимание на аспект информационной безопасности. Рассмотрим эти аспекты в популярных ECM/СЭД. Результат анализа представлен в таблице ниже.

Таблица – Основные критерии сравнительного анализа существующих решений

|  |  |  |  |
| --- | --- | --- | --- |
| Защита информации | 1С:Делопроизводство8 | Directum | Е1 Евфрат |
| 1 | 2 | 3 | 4 |
| Поддержка различных способов аутентификации | + | + | + |
| Назначение прав пользователям | + | + | + |
| Назначение прав группам пользователей | + | - | + |
| Поддержка пользовательских ролей | + | + | + |
| Средства мониторинга событий в системе | + | + | - |
| Использование ЭЦП | + | + | + |
| Применение сертифицированных средств защиты | + | + | + |
| Протоколирование действий пользователя | + | + | - |
| Шифрование данных системы | + | + | + |
| Организация резервного копирования базы данных | + | + | + |

Знаком «-» обозначены возможности, которые реализованы в системах, знаком же «-» обозначены возможности, которые не были реализованы.

Проведенный анализ позволил констатировать недостаточность работ, посвященных проблеме разработки моделей и алгоритмов систем управления информационной безопасностью электронного документооборота предприятия, что подтверждает актуальность темы настоящего исследования.

На основе проведенного анализа угроз и существующих решений была разработана специализированная система электронного документооборота для сети барбершопов на платформе 1С, включающая комплекс механизмов защиты. Рассмотрим ключевые аспекты реализации.

Разработанная система предусматривает детализированное разграничение прав доступа с учетом ролевой модели:

1. Управление правами доступа пользователей

Ролевая модель включает: администратор, бухгалтер, менеджер, мастер, кассир

Настройки прав:

* запрет на экспорт клиентской базы для рядовых сотрудников;
* ограничение доступа к финансовым документам (только для бухгалтерии);
* запрет редактирования завершенных документов.

2) Шифрование текста документов

Для защиты содержимого документов реализованы:

**Полевое шифрование**:

* персональные данные клиентов (паспорта, телефоны) шифруются алгоритмом AES-256;
* ключи хранятся отдельно от базы данных.

**Защита PDF-документов**:

* автоматическая установка паролей на выгружаемые файлы;
* водяные знаки для договоров.

3) Использование криптографии и ЭЦП

Система интегрирована с сертифицированными средствами криптозащиты:

**Работа с ЭП**:

* Подписание всех финансовых документов КЭП;
* Проверка подписей контрагентов через сервис ФНС.

**Криптозащита передачи**:

* Обмен данными по TLS 1.3;
* Хеширование вложений для контроля целостности.

4) Регулярное резервное копирование

Для обеспечения отказоустойчивости реализовано:

**Автоматическое резервирование**:

* Ежедневные резервные копии в 23:00;
* Хранение на локальном сервере и в облаке (MySQL Server).

**Процедура восстановления**:

* Проверка целостности резервных копий;
* Пошаговая инструкция для администратора.

**Заключение**

Проведенное исследование подтвердило, что переход от традиционного к электронному документообороту кардинально изменил подходы к обеспечению информационной безопасности в организациях. Современные СЭД, с одной стороны, предоставили новые технологические возможности защиты данных, а с другой - породили принципиально новые угрозы, связанные с цифровой средой.

Анализ существующих решений показал, что ключевым условием безопасного документооборота является комплексный подход

Практическая значимость исследования заключается в том, что предложенные решения позволяют организациям различных масштабов, включая малый бизнес (на примере барбершопа), внедрять безопасные СЭД с оптимальным соотношением надежности и затрат. Дальнейшие исследования планируется направить на разработку адаптивных систем безопасности, способных автоматически реагировать на новые виды киберугроз.

**Литература**

1. Даниленко А.Ю. Управление доступом в системах электронного документооборота // Труды ИСА РАН 2009. Т. 45. C. 39-45.
2. Информационная безопасность документооборота [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovyib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnostdokumentooborota/
3. Подсистема БСП «Управление доступом», основные объекты и регистры [Электронный ресурс]. URL: https://infostart.ru/1c/articles/1065487/
4. Права доступа в 1С: Документооборот 2.1 [Электронный ресурс]. URL: https://www.doc-lvv.ru/
5. Криптография и электронная подпись в решениях на 1С [Электронный ресурс]. URL: https://infostart.ru/1c/articles/809967/
6. Шифрование текста и файлов с помощью 1С [Электронный ресурс]. URL: https://infostart.ru/1c/articles/1083158/