

СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА, ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ И ПРЕИМУЩЕСТВА ПЕРЕХОДА НА ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Крягин Роман Витальевич

магистрант, ФГБОУ ВО Рязанский государственный радиотехнический университет им. В.Ф. Уткина, РФ, г. Рязань

Документооборот – это процесс движения документов в организации от момента их создания или получения и до завершения работы по ним или же отправления. Документооборот является комплексом работы с документами – прием, регистрация, контроль исполнения, формирование и хранение документации, рассылка и справочная работа.

Электронный документооборот (ЭДО) представляет собой единый механизм по работе с документами, представленными в электронном виде, являясь реализацией концепции «безбумажного делопроизводства». Электронный документооборот существенно повышает эффективность работы любого предприятия, позволяя более быстро обрабатывать и передавать документы, а также облегчая их хранение и учет в информационной системе предприятия.

Одним из ключевых понятий электронного документооборота является сам электронный документ(ЭД) - документ, созданный с помощью средств электронной обработки информации и подписанный электронной подписью(ЭЦП) и сохраненный на электронном носителе в виде файла определенного формата. Электронная цифровая подпись – это электронный аналог собственноручной подписи, являющийся одним из основных средств защиты информации. Она обеспечивает возможность подтверждения подлинности электронных документов.

Защита электронного документооборота является одной из основных проблем при разработке систем ЭДО. Сейчас эта проблема становится актуальнее с каждым днем. Можно выделить несколько причин, почему это происходит:

- Происходит все более активное внедрение электронного документооборота в государственные услуги. От этого возникает необходимость защиты конфиденциальной информации.
- Услуги, предоставляемые в электронном виде, должны базироваться в правовом поле. Как правило, в этом случае созданию финального электронного документа предшествует обмен документами между различными ведомствами и эти документы чаще всего не следует делать общедоступными.
- Появляется необходимость приданию электронным документам юридической силы

Ввиду указанных выше причин, проблема защиты ЭДО сейчас поднимается на государственном уровне. Для создания системы защищенного документооборота в организации, должны иметься следующие факторы:

- Наличие определенного количества документов с грифом ограниченного доступа
- Необходимость управления потоками документов
- Наличие большого архива документов
- Необходимость постоянного поиска информации
- Наличие территориально-удаленных подразделений
- Обеспечение безопасности данных при пересылке необходимых документов

При разработке защиты электронного документооборота, помимо внедрения электронной цифровой подписи, что является практически обязательной вещью, важно определиться, что важнее – внутренняя защита документов или же его защита при пересылке.

Большинство средств защиты электронного документооборота базируется на основе технологии инфраструктуры открытых ключей PKI(Public Key Infrastructure). Эта технология предполагает наличие двух разных ключей – открытого ключа и закрытого. Таким образом, защищенность документа обеспечивается их шифрованием, а достоверность – использованием электронной цифровой подписи. Подобный уровень применяемых средств защиты позволяет обмениваться электронными документами, содержащими конфиденциальную информацию.

Помимо этого, для защиты электронных документов используются сертифицированные средства криптографической защиты информации(СКЗИ). Для работы в этой системе, каждый пользователь получает уникальный сертификат, используемый для подтверждения доступа к документам, которые данный пользователь желает просмотреть или обработать.

Благодаря этим разработкам доступ к конфиденциальным документам имеет право только автор документа. Остальные пользователи по умолчанию не имеют данного права. Доступ к документам регулируется системой ЭДО, а правила этой системы настраиваются администратором безопасности.

Необходимость защиты электронного документооборота возникает не только при работе с документами, но и при их передаче. Важно, чтобы отправленный документ не был перехвачен, прочитан и изменен. В таком случае применяются защищенные системы передачи сообщений и файлов, в которых используется шифрование всех файлов, передаваемых через них.

Шифрование документа и установка в них электронной подписи происходит автоматически. Для этого используется средства криптографической защиты, такие «КриптоПро», «ВербаOW», «VIPNET CSP» и т.д. Внедрение такой защиты позволяет не только снизить вероятность потерь документов, но что будет достигнута полная конфиденциальность информации в них.

Очень важно обеспечить защищенный доступ с применением механизмов двухфакторной аутентификации. В настоящее время, кроме классической защиты информационной системы, прибавились дополнительные функции, такие как:

- Аутентификация пользователей и разделения доступа;
- Подтверждение авторства электронного документа;
- Контроль целостности электронного документа;
- Конфиденциальность электронного документа;
- Обеспечение юридической значимости электронного документа;
- Регистрация событий в информационных системах;
- Разработка криптографической и антивирусной защиты;
- Межсетевое экранирование;
- Виртуальные частные сети;
- Аудит информационной безопасности.

Все эти функции должны быть четко разработаны и учтены при создании систем защиты электронного документооборота. Например, при аутентификации пользователей чаще всего применяют биометрические способы идентификации. Строгая аутентификация позволяет не только разделить, но и персонализировать доступ к документам.

В то же время, организациям, имеющим территориально-удаленные филиалы, особенно следует побеспокоиться о защите и сохранении информации при пересылке. Для этого больше всего подходят Workflow-системы, которые обеспечивают автоматизацию не только отдельных функций, но и всех бизнес-процессов организации. Система помогает определить неправильно заполненные или просроченные документы, тем самым существенно упрощая электронный документооборот в организации.

Заключение

Проанализировав всё вышесказанное, можно сделать вывод, что разработка системы защиты электронного документооборота – один из приоритетов любой современной организации, еще не внедрившей её в свою работу. Правильно разработанная система защиты – это наука, которая должна осуществляться на основе твердых методических разработок. Защита системы – это защита её работоспособности и конфиденциальных данных компании.

Защищенный электронный документооборот должен состоять из целого комплекса действий по защите информации и обеспечении конфиденциальности. Мероприятия по защите документооборота должны учитывать правильно разработанные действия технического, программного и организационного обеспечения по ограничению доступа к защищаемой информации.

Список литературы:

1. Перпеляк А. И., Саломатина Е. В. Цифровая экономика: новые возможности для бизнеса // Научное сообщество студентов XXI столетия. Технические науки: сборник статей по материалам LII международной студенческой научно-практической конференции — №4(51).
2. Косоруков А. А. Цифровое правительство в практике современного государственного управления (на примере Российской Федерации) // Тренды и управление. — 2017. — № 4.
3. Основные тенденции развития систем электронного документооборота. [Электронный ресурс] URL: <https://rkit.ru/blog/60/37305/> (дата обращения: 01.12.2022).
4. Экономическая эффективность внедрения СЭД. [Электронный ресурс] URL: <http://www.sfxsula.ru/news/infoblog/8458/> (дата обращения: 01.12.2022).
5. Цифровое правительство 2020. Перспективы для России. [Электронный ресурс] URL: <http://www.iis.ru/docs/DigitalGovernmentRussia2020RUS.pdf>. (дата обращения: 03.12.2022).
6. Волостных В.А., Штеренберг С.И., Гвоздев Ю.В. Проблемы обеспечения безопасности персональных данных в высших учебных заведениях // Информационные технологии и телекоммуникации, 2014. – Т. 2. – № 4. – С. 134-141.