Педагогические науки

УДК 004.01

В.В. Кириленко

Кириленко Виктория Владимировна, студентка 4 курса группы ДОК/бак-18 информационно-библиотечного факультета Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: vika.kirilenko.00@bk.ru

Научный руководитель: **Матвеева Анастасия Сергеевна**, кандидат педагогических наук, доцент кафедры документоведения и проектной деятельности Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: doc1996@mail.ru

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В данной статье рассмотрены проблемы защиты информации при использовании систем электронного документооборота, а также рассмотрены способы решения данных проблем.

Ключевые слова: электронный документооборот, защита электронного документооборота, электронный документ.

V.V. Kirilenko

Kirilenko Victoriya Vladimirovna, 4th course student of the DOK/bak-18 group of information and library faculty of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: vika.kirilenko.00@bk.ru

Research supervisor: **Matveeva Anastasiya Sergeevna**, candidate of pedagogical sciences, associate professor of department of documentation and project activities of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy st., Krasnodar), e-mail: doc1996@mail.ru

INFORMATION SECURITY PROBLEMS IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

This article discusses the problems of information protection when using electronic document management systems, as well as ways to solve these problems.
***Key words**:* electronic document management, electronic document management protection, electronic document.

Защищенный электронный документооборот в современном мире является сложным, комплексным процессом. В настоящее время эффективная работа любого предприятия невозможна без его правильного подбора и внедрения.

Система защиты электронного документооборота является подклассом систем электронного документооборота, обеспечивающая не только безопасность передачи, но и целостность самой информации.

Можно выделить несколько причин, по которым защита становится объектом внимания:

– происходит развитие государственных услуг в электронном виде, в которых принимают участие первые лица государства. В этом случае возникают вопросы защиты конфиденциальной информации;

– услуги, которые предоставляются в электронном виде, должны базироваться в правовом поле. Как правило, в этом случае созданию электронного документа предшествует огромная работа по обмену

документами между различными ведомствами, которые не всегда надо делать общедоступными;

– появляется реальная необходимость наделения электронных документов юридической силой;

– хакерские атаки: подделка документов, подмена клиента, срыв сделки, в частности, перехват заказов вследствие нарушения конфиденциальности информации о проводимых сделках;

– утечка конфиденциальной информации коммерческой, финансовой, научно-технической деятельности организации;

– несанкционированный доступ к системам управления организацией и технологическим процессам;

– мошенничество при проведении торговых и финансовых операций [2, с. 12].

Ввиду вышеуказанных причин проблема защиты электронного документооборота в настоящее время начинает решаться и на государственном уровне.

Для обеспечения защиты информации в электронном документообороте можно рассмотреть следующие варианты:

1. Установить пароль на документ или электронный архив.

2. Обеспечить доступ по цифровому (электронному) ключу. Метод основывается на наличии у пользователя физического ключа (флеш-накопителя или SD-карты) для расшифровки документа. Благодаря ему, даже если злоумышленник получил доступ/скопировал информацию, он не сможет без необходимого ключа открыть документ и отредактировать его. Но все же данный метод защиты также обладает рядом недостатков:

− ответственность за сохранность и правомерное использование лежит на владельце электронного ключа;

− необходимо обеспечить безопасную передачу такого ключа между лицами, у которых есть доступ к данному документу;

− сам по себе носитель электронного ключа имеет свою стоимость;

− носитель электронного ключа может выйти из строя.

3. Ввести систему управления правами доступа. В основном этот метод защиты документов используется для корпоративных пользователей на базе службы управления правами Active Directory (AD RMS). Документы, защищенные AD RMS, шифруются, а автор может устанавливать разрешения для тех, кто получит доступ к файлам.

Список возможных ограничений прав:

− Чтение, изменение, печать.

− Срок действия документа.

− Запрет пересылки электронного письма.

− Запрет печати электронного письма.

4. Использовать комбинированные методы защиты документов.

5. Установить антивирусные программы. Типичный антивирус для среды Windows обычно включает такие программы, как:

– сканер с графическим интерфейсом и сканер с интерфейсом командной строки (проверяют носители информации на наличие вирусов, обнаруживают и обезвреживают вирусы в оперативной памяти компьютера, на дисках и в электронной почте);

– резидентный сторож(проверяет файлы на ходу при обращении к ним из какой-либо программы, оповещает пользователя при обнаружении инфицированных или подозрительных файлов);

– почтовый сторож (проводит проверки входящих и исходящих сообщений электронной почты и делает это зачастую на уровне почтовых протоколов);

– планировщик заданий (позволяет автоматизировать запуск программ, входящих в состав антивируса);

– модуль обновления (предназначен для получения дополнений вирусных баз и новых версий программных компонентов) [1, с. 43].

В офисных программах Word, Excel и Power Point для защиты от макросов (которые давно и активно используются вирусами) есть

возможность задавать уровень безопасности, который будет применяться при открытии файлов, а также список тех источников макросов, которые считаются надежными.

Является важным также подбор самой системы электронного документооборота, так как качество и разработанность системы должны обеспечивать защиту документов, но многие системы могут не справляться с поставленной задачей.

В данный момент рынок систем защиты электронного документооборота является одной из наиболее развивающихся отраслей ИТ-индустрии.

Для защиты различные компании предлагают свои авторские разработки.

Например, компания «Диалог Наука» предлагает свою разработку, которая базируется на основе технологии инфраструктуры открытых ключей PKI (Public Key Infrastructure). Эта технология предусматривает использование асимметричных криптографических алгоритмов. Такая защита предполагает наличие двух различных ключей – открытого и закрытого. Таким образом, защищенность документооборота достигается путем шифрования документов, а достоверность – использованием электронной цифровой подписи (ЭЦП) [3, с. 18].

Кроме этого, для защиты электронных документов используются сертифицированные средства криптографической защиты информации (СКЗИ). Для возможности работы в этой системе пользователь должен получить сертификат в самом центре научно-производственного предприятия Info Trust.

Необходимость защиты электронного документооборота важна не только при работе с документами, но и при их отправке. В этом случае применяется Система «СТЭК-ТРАСТ», которая может организовать передачу сообщения и файлов любых форматов в зашифрованном виде с электронной подписью. Это гарантирует то, что корреспонденцию могут

прочитать только указанные пользователи при наличии у них ключей электронной подписи.

Также для крупных компаний, имеющих отдельные филиалы, больше всего подходят Workflow-системы, которые обеспечивают автоматизацию не только отдельных функций, но и всех бизнес процессов компании. Эта система четко определяет процесс: что, кто, когда и как делает, откуда получает и куда отправляет. В этом случае пользователь не задумывается над тем, как создать документ, как его получить, как его обработать. Все это закреплено в системе. При этом сотрудник не сможет неправильно заполнить документ или пропустить сроки (в этой системе предусмотрены напоминания). Единственным минусом такой системы является сложность и длительность внедрения, а также они не могут иметь электронный архив [4, с. 267].

Таким образом, организация защиты информации в документообороте – это целый комплекс мероприятий. Защита системы – это защита ее работоспособности.

Мероприятия по защите документооборота должны учитывать правильно разработанные действия технического, программного и организационного обеспечения по ограничению доступа к защищаемой информации, и в этом случае не последнюю роль играет человеческий фактор. Необходимо, чтобы каждый пользователь на своем рабочем месте понимал ответственность за порученное дело.

Список используемой литературы:

1. *Коржук, В. М.* Защищенный документооборот. Часть 1: учебно-методическое пособие / В.М. Коржук, И.Ю. Попов, А.А. Воробьева. – СПб.: Университет ИТМО, 2021. – 67 с.

2. *Яппаров, Р. М.* Некоторые проблемы защиты конфиденциальной информации в системах электронного документооборота / Р.М. Яппаров // Вестник Уфимского юридического института МВД России. – 2019. URL:

https://cyberleninka.ru/article/n/nekotorye-problemy-zaschity-konfidentsialnoy-informatsii-v-sistemah-elektronnogo-dokumentooborota (дата обращения: 20.09.2021).

3. *Булдакова, Т. И.* Оценка эффективности защиты систем электронного документооборота / Т.И. Булдакова, Б.В. Глазунов, Н.С. Ляпина // Доклады ТУСУР. – 2012. – № 1(25). – Ч. 2. – С. 52–56.

4. *Семашк, А. В.* Механизмы защиты системы электронного документооборота предприятия / А.В. Семашко, К.И. Болотов, А.В. Гуменникова // Актуальные проблемы авиации и космонавтики. – 2013. URL: https://cyberleninka.ru/article/n/mehanizmy-zaschity-sistemy-elektronnogo-dokumentooborota-predpriyatiya (дата обращения: 20.09.2021).