Молодёжный вестник НФ БГТУ. 2022. Том 02. № 04 (08)
https://rio-nb-bstu.science

ИНФОРМАТИКА. КРАТКИЕ СООБЩЕНИЯ

doi: 10.51639/2713-0576_2022_2_4_73
УДК 004.056.53
ГРНТИ 20.15.13
ВАК 05.13.19

Разработка системы защиты электронного документооборота на предприятии

Дубовикова О. В.

Удмуртский государственный университет
426034, Россия, Удмуртская Республика, г. Ижевск, ул. Университетская 1

e-mail: ovdubovikova@yandex.ru

В статье рассмотрены функции системы электронного документооборота (СЭД), внедренной на предприятии; построена модель нарушителя и актуальных угроз безопасности информации в СЭД; представлена оценка рисков этих угроз.

Ключевые слова: система электронного документооборота, модель нарушителя и угроз информационной безопасности.

СЭД представляют собой решения, преимущественно предназначенные для управления информационными ресурсами средних и крупных предприятий. Основные причины отсутствия таких систем у малых предприятий и индивидуальных предпринимателей: высокая цена приобретения качественной и безопасной системы управления базами данных, а также необходимость привлечения к проектам внедрения высококвалифицированных консультантов и аналитиков.

К настоящему времени фактическим стандартом современных СЭД являются следующие области деятельности:

- общее делопроизводство – обработка входящей корреспонденции и обращений граждан, подготовка исходящих писем и документов, внутренняя и организационно-распорядительная документация, контроль исполнения поручений;
- кадровое делопроизводство - осуществление поддержки процедур приема и увольнения работников, направления работников в командировку, предоставления планового и иных видов отпусков;
- архивное делопроизводство – завершение жизненного цикла документов в организации и поддержка следующих процедур: формирование описей по утвержденным формам, передача дел на архивное хранение, экспертиза ценности документов и дел в целом, уничтожение документов и дел, больше не представляющих ценности для организации, сдача отдельных дел на хранение в структуры Федерального архивного агентства;
- коллегиальная работа – автоматизация документационного обеспечения деятельности коллегиальных органов управления: совещаний, заседаний, советов директоров, собраний акционеров.

От организации документооборота и работы с информационными ресурсами во многом зависит эффективность работы предприятия. Большое количество бумажных документов, длительный поиск нужной информации, потери и дублирование документов, задержки с

отправкой и получением писем, ошибки персонала - все эти проблемы, возникающие при плохой организации документооборота, могут сильно затормозить работу предприятия.
Внедрение СЭД на предприятии позволит реализовать:

- автоматизацию и оптимизацию бизнес-процессов;
- повышение эффективности контроля исполнения документов;
- структурированное хранение информации и быстрый доступ к ней;
- быстрое получение аналитической информации и отчётов для принятия управленческих решений;
- сокращение затрат времени при работе с документами;
- экономию материальных ресурсов за счёт сокращения доли бумажных документов;
- повышение исполнительской дисциплины сотрудников.

Однако эта технология имеет недостаток в области защиты информации, передаваемой по каналам связи. Этим могут воспользоваться конкуренты, пытаясь внедриться в процесс обработки информации предприятия.
Документ в любой форме его представления и на любом этапе его жизненного цикла подвержен угрозам информационной безопасности, поэтому необходимо своевременно идентифицировать их источники. В Российской Федерации полномочия по своевременному выявлению новых угроз и их источников, а также разработке соответствующих методических документов возлагаются на федеральный орган исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России). Источниками угроз, как правило, выступают антропогенные факторы – нарушители, злоумышленники. Успех нарушителя при реализации угрозы определяется следующими факторами: его потенциалом (возможностями, квалификацией), мотивами и положением относительно среды обращения документа (внешний, внутренний), методами реализации угроз и уязвимостями объекта нападения.
Как правило, первоначальным базисом классификации нарушителей в документах ФСТЭК и ФСБ России является их положение относительно среды обращения документа, т. е. наличие у них прав доступа к информации и к компонентам информационной системы, что даёт возможность разделить нарушителей на два типа:

- внешние нарушители – это лица, которые не имеют права доступа к информационной системе (ИС) и её компонентам, но имеют возможность реализовать угрозу за пределами границ ИС;
- внутренние нарушители – это лица, которые имеют право постоянного (разового) доступа к ИС и её компонентам.

При этом важно учитывать, что внутренние нарушители обладают наибольшими возможностями при реализации угроз:

- внешний нарушитель может действовать совместно с внутренним, а также в составе группы;
- реализация угрозы возможна в любой точке ИС, а в качестве точки атаки на всю ИС нарушитель выберет самое слабое звено ИС;
- при наличии подключения к сети Интернет высока вероятность воздействия со стороны внешнего нарушителя.

Типовая модель угроз для ИС, имеющих подключение к сетям общего пользования, включает в себя:

- угрозы утечки информации по техническим каналам;
- угрозы несанкционированного доступа (НСД) к данным, обрабатываемым на автоматизированном рабочем месте, в том числе угрозы из внешних сетей [3].

В табл. 1 представлена модель угроз по отношению к системам электронного документооборота, осуществляющих обработку сведений конфиденциального характера.

Молодёжный вестник НФ БГТУ. 2022. Том 02. № 04 (08)
https://rio-nb-bstu.science

Таблица 1

Категории нарушителей информационной безопасности

Тип нарушителя	Категория ФСБ – Hi, ФСТЭК – Nj (условное обозначение)	Способ доступа и полномочия доступа к персональным данным
Внешний	H1, H2, N0	Лица без доступа к ИС и защищаемым данным, но с возможностью самостоятельно планировать и осуществлять атаки только за пределами контролируемой зоны (КЗ), а также в пределах КЗ без физического доступа к аппаратным элементам ИС
Внутренний	H3, N1	Зарегистрированные пользователи ИС, имеющие санкционированный доступ к аппаратным компонентам ИС, на которых в том числе реализованы средства криптографической защиты информации (СКЗИ), но не имеющие доступа к защищаемым данным. Лица, осуществляющие разработку, поставку, сопровождение и ремонт технических средств ИС
	H4, H5, N2, N3	Зарегистрированные пользователи ИС, осуществляющие доступ к ресурсам ИС с рабочего места. Зарегистрированные пользователи ИС, имеющие удаленный доступ к защищаемым данным. Имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ
	H4, H5, N4, N5, N6	Зарегистрированные пользователи ИС с полномочиями системного администратора, администратора безопасности сети (сегмента сети) ИС. Имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ
	H6, N7	Программисты-разработчики прикладного программного обеспечения (ПО) и лица, обеспечивающие поставку и сопровождение ПО в ИС. Имеют возможность привлекать специалистов в области разработки и анализа СКЗИ

Основные угрозы электронному документообороту (ЭД) можно представить в табл. 2.

Таблица 2

Основные угрозы ЭД

Угроза ЭД предприятия	Способы реализации угроз
I. Угроза целостности	а) повреждение
	б) уничтожение информации
II. Искажение информации	а) сбои и ошибки
	б) повреждение
	в) подмена
III. Угроза работоспособности системы	а) ошибки пользователя
	б) компьютерные атаки
	в) вредоносное ПО
IV. Угроза конфиденциальности	а) кража информации
	б) подмена маршрутов следования
	в) НСД

В настоящее время существует несколько подходов к измерению рисков информационных угроз безопасности защищённого документооборота. Наиболее распространенным из них является оценка рисков по двум или трем факторам. В простейшем случае учитываются два фактора: вероятность происшествия и тяжесть возможных последствий. Причем считается,

что чем больше риск, тем выше вероятность происшествия и тяжесть последствий. Эта зависимость выражается формулой (1).

$$Риск = P_{происшествия} \times Цена\ потери. \quad (1)$$

В методиках, предполагающих более высокие требования к безопасности, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери, где:

- угроза – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации;
- уязвимость – слабость в системе защиты, которая делает возможным реализацию угрозы.

Вероятность происшествия является величиной, зависящей от уровней угроз и уязвимостей, и выражается формулой (2).

$$P_{происшествия} = P_{угрозы} \times P_{уязвимости}. \quad (2)$$

Следовательно, риск рассчитывается по формуле (3).

$$Риск = P_{угрозы} \times P_{уязвимости} \times Цена\ потери. \quad (3)$$

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал – качественная.

Таким образом, для оптимальной работы СЭД на предприятии необходимо четко выявлять уязвимости информационной системы и своевременно разрабатывать способы защиты от них.

Конфликт интересов

Автор статьи заявляет, что у неё конфликта интересов по материалам данной статьи с третьими лицами на момент подачи статьи в редакцию журнала, и ей ничего не известно о возможных конфликтах интересов в настоящем со стороны третьих лиц.

Список литературы

1. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.
2. ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности.
3. Ложников П. С., Жумажанова С. С. Об угрозах безопасности сведений ограниченного доступа в системах смешанного документооборота и правовом регулировании в области применения цифровых подписей с биометрической активацией // Доклады ТУСУР, том 21, № 4, 2018. С. 35–43.

Development of a system for protecting electronic document flow at an enterprise

Dubovikova O.V.

Udmurt State University
426034, Russia, Udmurt Republic, Izhevsk, Universitetskaya st., 1.

The article considers the functions of the electronic document flow system (EDFS) implemented in the enterprise; a model of the intruder and actual threats to the security of information in the EDFS has been built; an assessment of the risks of these threats is presented.

Key words: electronic document flow system, model of an intruder and threats to information security.