Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Водолазова Е.В. Информационная безопасность данных СЭД // Академия педагогических идей «Новация». – 2019. – №1 (январь). – АРТ 15-эл. – 0,2 п. л. – URL: http://akademnova.ru/page/875548

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056

Водолазова Елена Владимировна
студентка 4 курса, факультета управления
Научный руководитель: Перова М.В.
доцент кафедры информационных технологий
ЮРИУ РАНХИГС
г. Ростов-на-Дону, Российская Федерация
ya.ellenru@yandex.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДАННЫХ СЭД

Аннотация: В данной статье проводится современный анализ внедрения в деятельность организации системы электронного документооборота. Дана характеристика основных положительных и отрицательных факторов внедрения систем электронного документооборота.

Ключевые слова: система электронного документооборота, безопасность данных, информационное развитие.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Vodolazova Elena Vladimirovna
4rd year students, faculty of Management
Science supervisor: Perova M.V.
Assistant professor of IT
URIU RANEPA
Rostov-on-Don, Russian Federation

INFORMATION SECURITY DATA ECM

Annotation: This article provides a modern analysis of the implementation of the electronic document management system in the organization. The characteristic of the main positive and negative factors of the introduction of electronic document management systems is given.

Keywords: electronic document management system, data security, information development.

Автоматизация документооборота на современном этапе общественного развития характеризуется как элемент функционирования успешной организации. Документационное обеспечение управленческой деятельности осуществляется с помощью использования системы электронного документооборота (СЭД). Системы электронного документооборота являются особым и радикальным управленческим решением, которое не имеет аналогов с традиционными информационными потоками управления организацией. Применение систем электронного документооборота детерминируются такими положительными качествами

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

как оптимизация скорости протекания информационных процессов и повышение конкурентоспособности организации.

Современный этап информационного развития России можно охарактеризовать как этап качественного перелома, так как положение о применении и внедрении системы электронного документооборота получило общественное признание, как одна из основополагающих частей информационной системы деятельности любой компании. Руководящий коллектив организации понимает, что применение системы электронного документооборота означает упорядочивание документации, а также является сильнейшим экономическим фактором.

Исходя из данных представленных CNews Analytics, рынок СЭД в последнее десятилетие характеризуется как один из наиболее динамично развивающихся сегментов отечественной ИТ-индустрии. В качестве лидирующих СЭД на российском рынке можно выделить такие программные продукты как: Microsoft SharePoint Products and Technologies, CompanyMedia, 1С: Документооборот, LanDocs, ДЕЛО, Е1 ЕВФРАТ [1].

Но необходимо отметить, что приобретение СЭД характеризуется и наличием негативных факторов, так ведение информационных потоков с помощью СЭД ведет к необходимости решения задачи в сфере обеспечения информационной безопасности, особенно в случае, когда планируется создание юридически значимого электронного документооборота.

Внедрение в деятельность организации системы электронного документооборота позволяет приобрести огромную гибкость в хранении и обработке информации, а также заставляет бюрократическую систему организации работать наиболее скоординировано и слажено. Но в случае пренебрежения защитных механизмов СЭД приведет к возникновению угрозы конфиденциальности.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Исходя из мнения экспертов, основными видами угроз информационной безопасности выступают: вредоносные программные воздействия на средства вычислительной информации и технические средства, ошибочные действия пользователей и персонала, сбои и отказы программных средств и противоправные действия третьих лиц.

Кроме умышленных и случайных действий человека источниками угроз информационной безопасности могут выступать сбои и отказы технических и программных средств, техногенные катастрофы, акты террористической деятельности, стихийные бедствия. Подобным образом, данные, которые находятся в системе электронного документооборота требуют обеспечения информационной безопасности.

СЭД должна обеспечить сохранность документов от потери и порчи и иметь возможность их быстрого восстановления. Данная задача функционирования и развития СЭД обусловлена исходя из положений Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ, в котором регламентирована необходимость защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статистика показывает следующие факты: в 45% случаев потери важной информации приходятся на физические причины (отказ аппаратуры, стихийные бедствия и подобное), 35% обусловлены ошибками пользователей и менее 20% - действием вредоносных программ и злоумышленников.

За 2017 год российские компании потеряли примерно 116 млрд руб. из-за кибератак — убытки из-за хакеров признает почти каждая пятая российская компания.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Средняя сумма убытков одной российской компании от кибератак в 2017 году в России составила 299,9 тыс. руб.; в целом по стране потери бизнеса от таких инцидентов оцениваются в 115,97 млрд руб., подсчитал аналитический центр Национального агентства финансовых исследований (НАФИ) на основании опроса, проведенного в ноябре 2017 года среди 500 руководящих сотрудников предприятий в восьми федеральных округах России. При этом учитывались только прямые потери компаний.

Выяснилось также, что в 2017 году с киберугрозами сталкивались половина респондентов. В первую очередь — крупный бизнес (62 против 46–47% в малых и средних предприятиях). Чаще всего это выражалось в заражении вирусами рабочих компьютеров сотрудников, в том числе с последующим вымогательством денег (20%), во взломе почтовых ящиков (12%), атаках на сайт компании (10%) (Рис.1) [2].

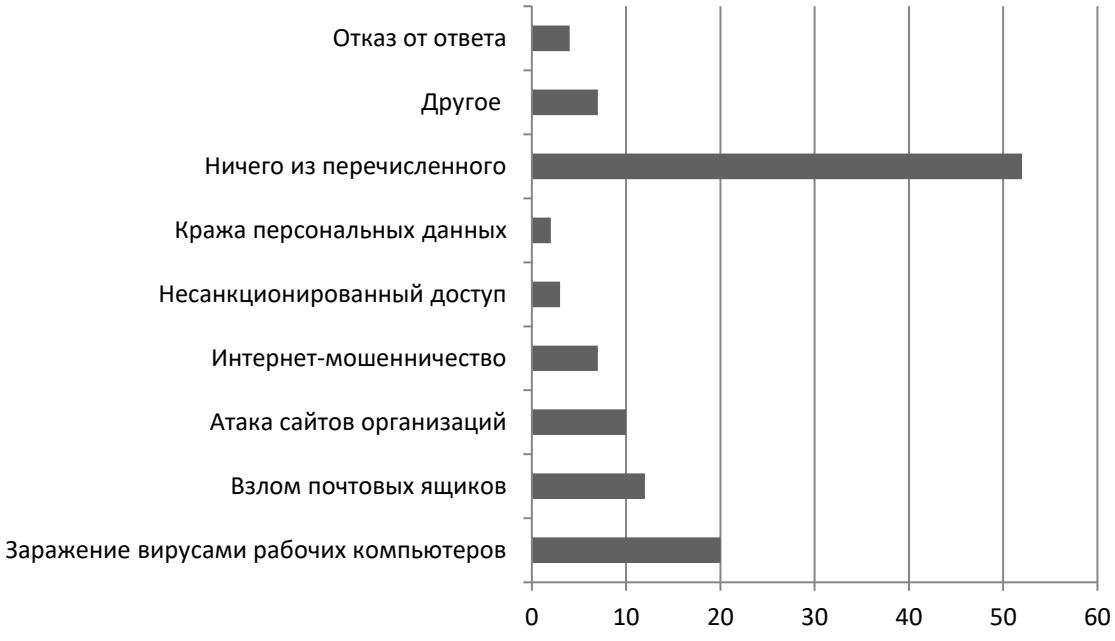

Рис. 1. Данные опроса «С какими информационными угрозами приходилось сталкиваться вашей компании за последний год?»

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Представители компаний, которые пережили потерю данных считают, что причиной инцидента являлось халатное отношение к правилам информационной политики организации, и лишь 20% из числа опрошенных считают, что интеллектуальная собственность их организаций защищена надежным образом. Всего 4% респондентов заявило, что их работодатели обращают внимание на информационную безопасность деятельность компании. В отношении эффективности защиты СЭД организации уверено лишь 24% из числа участников опроса [3].

Например, СЭД, в основе которой используются базы данных Oracle или Microsoft SQL Serve, считают целесообразным использование средств резервного копирования от основного разработчика СУБД. Другие системы характеризуются наличием собственных подсистем резервного копирования, которые разработаны непосредственно производителем СЭД. Сюда необходимо отнести и возможность восстановления данных, и возможность восстановления самой системы в случае её повреждения.

Наиболее востребованная в России система «ДЕЛО» в целях совершенствования документационного обеспечения управления применяется и при работе органов МФЦ. Система оказания государственных и муниципальных услуг в электронном виде (СОГУ) на базе СЭД «ДЕЛО» позволяет перевести в электронную форму процесс оказания электронных услуг на всех уровнях – федеральном, региональном и муниципальном. Это обеспечивается путем интеграции с «Единым порталом государственных и муниципальных услуг» (ЕПГУ) через Систему межведомственного электронного взаимодействия (СМЭВ) [4].

Создание подобной системы обусловлено множеством положительных факторов, но в тоже время постоянно «вспылывает» проблема безопасности информационного обмена. Одним из происшествий,

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

связанным с утечкой данных была копия паспортов и иных документов, которые хранятся в открытом доступе на компьютерах многофункциональных центров предоставления государственных услуг.

По данным «Коммерсанта», в каждом МФЦ используется компьютер общего пользования, подключенный к сканеру. Любой желающий может самостоятельно использовать ПК, например, для загрузки копий документов на портал госуслуг.

Проверке подверглись ряд МФЦ в Москве, где было выяснено, что на этих компьютерах в общем доступе хранятся сотни разных документов: копии паспортов, СНИЛС, анкет с указанием мобильных телефонов, реквизитов счетов в банках. Владельцы документов, воспользовавшись общим компьютером, забыли удалить файлы, сотрудники МФЦ также не озаботились этим. Скан-копии любой желающий может скачать на флешку или же отправить себе по почте.

По словам ведущего аналитика «СерчИнформ», эти сведения мошенники могут продать в интернете. Стоимость одной скан-копии варьируется от 100 до 500 рублей в зависимости от качества и количества страниц, сказал эксперт. Он отметил, что сканы могут использовать как для рекламной рассылки, так и для получения микрозаймов.

Эксперты RTM Group говорят, что получить компенсацию ущерба в таком случае будет затруднительно. Для этого придется доказывать прямую связь между сканированием документов в МФЦ и полученным вредом.

В пресс-службе центров госуслуг Москвы сообщили газете, что сотрудники должны удалять данные раз в день, в соответствии с внутренними правилами. Более того, подключенные к сканерам компьютеры не имеют полного доступа в интернет.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

В Минэкономики отмечено, что существуют методические рекомендации ведомства о деятельности МФЦ, в которых в числе прочего определены и требования к информационной безопасности, но практический опыт исследователей доказывает, что надежная защита информации в СЭД характеризуется наличием и применением комплексных аппаратных средств и программ защиты, которые разрабатываются исходя из всех необходимых технических, организационных и режимных мероприятий. Наиболее эффективными и актуальными для защиты информации в СЭД выступают определенные типы аппаратно-программных систем и средств. В частности это могут быть: система защиты от несанкционированного доступа и/или взлома; система защиты от внешних атак; средства защиты компьютерных вирусов; система обнаружения вторжений в режиме реального времени и средства криптографической защиты, к которым относятся шифрование и электронная цифровая подпись.

В целях обеспечения юридически значимой системы документооборота и исходя из положений Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», в системе электронного документооборота «Дело» используется усиленная квалифицированная электронная подпись. Подобный вид подписи позволяет идентифицировать человека, который поставил свою подпись, а также обеспечить защиту документа от различных изменений. Квалифицированная электронная подпись имеет существенное отличие от неквалифицированной электронной подписи, так как при её создании и проверке применяются средства криптозащиты, которые проходят обязательную сертификация ФСБ РФ.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Таким образом, изучив информацию относительно информационной безопасности в СЭД, можно сделать вывод о том, что развитие рынка информационной безопасности и развитие рынка СЭД являются неразрывно связанными процессами. Следует согласиться с мнением исследователей о том, что в ближайшие 3-4 года российский рынок СЭД приблизится к западному рынку, так как увеличится понимание важности и необходимости процессов управления защитой информации. Но пока данные процессы протекают положительно лишь на территории отдельных организаций и субъектов, что подтверждает значимость и актуальность данной проблематики.

Список использованной литературы:

1. СЭД (рынок России) [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index. php/Статья:СЭД_(рынок_России), свободный.
2. Российские компании за год потеряли более 100 млрд руб. из-за кибератак [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581b, свободный.
3. ИТ на уровне регионов: выравнивание ситуации и обеспечение открытости Режим доступа: https://www.osp.ru/cio/2013/10/13038132/, свободный.
4. Обеспечение безопасности в системах электронного документооборота Режим доступа: https://it-iatu.ru/is/informacionnaya-bezopasnost-i-zaschita-informacii/obespechenie_bezopasnosti_v_sistemah_elektronnogo_dokumentooborota, свободный.
5. Многофункциональные центры предоставления госуслуг Режим доступа: http://www.tadviser.ru/index.php , свободный.

Дата поступления в редакцию: 09.01.2019 г.
Опубликовано: 16.01.2019 г.