УДК 004

А.А. Семенова[1], Н.И. Глухов[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

АНАЛИЗ УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Аннотация. Представлен обзор функционирования систем электронного документооборота (СЭД), представлены модели нарушителей, так же проведен анализ способов защиты СЭД при попытках несанкционированного доступа к СЭД.

Ключевые слова: система электронного документооборота, угроза, уязвимость, система защиты, криптостойкость, центр регистрации (ЦР), центр сертификации (ЦС), список доверенных элементов (СДЭ), удостоверяющий центр (УЦ), электронная подпись (ЭП).

A.A. Semenova[1], N.I.Gluhov[1]

[1] Irkutsk State Transport University, Irkutsk, Russia

ANALYSIS OF VULNERABILITI OF MODERN ELECTRONIC DOCUMENTATION SYSTEMS

Abstract. An overview of the functioning of electronic document management systems (EDMS) is presented, models of violators are presented, an analysis of ways to protect EDMS in attempts of unauthorized access to EDMS is also carried out.

Keywords: electronic document management system, threat, vulnerability, security system, cryptographic strength, registration center (CD), certification center (CA), list of trusted elements (SDE), certification center (CA), electronic signature (ES)

Введение

Внедрение системы электронного документооборота (СЭД), дает возможность приобрести большую гибкость при обработке и хранении информации и заставляет компанию работать эффективнее. При этом СЭД создает новые риски, и пренебрегая защите непременно появятся новые угрозы конфиденциальности.

В последнее время популярность систем электронного документооборота (СЭД) возросла, и по прогнозам экспертов, данный спрос увеличится.

Перед тем, как внедрить СЭД не нужно забывать о безопасности системы, потому что особый интерес со стороны злоумышленников имеют непосредственно документы физических и юридических лиц.

Главный элемент любой СЭД – это документ, который находится в системе, это может быть файл, база данных. Если говорить о защищенном документообороте, то это непосредственно сама защита документов, защита информации, которые несут в себе те или иные документы. В данном случае все заключается в задаче защиты данных от несанкционированного доступа.

Из чего следует, что нужно защищать, аппаратные элементы системы. Это компьютеры, сетевое оборудование, серверы. Не малую важность имеют такие угрозы как неисправность оборудования, доступ злоумышленника к оборудованию. Так же необходимо защищать файлы системы, это базы данных, программное обеспечение. Если этого не делать, то у злоумышленника появляется возможность влиять на элементы СЭД, не проникая в систему. К примеру, файлы могут быть скопированы или нарушены злоумышленником в результате сбоя системы или оборудования. [4; 8]

Используя такой метод, можно построить систему, которая будет защищена на всех уровнях.

Угрозы системам электронного документооборота почти одинаково однообразны и можно сделать следующую классификацию:

- угроза целостности – искажение и уничтожение информации, как непреднамеренное, так и умышленное;

- угроза конфиденциальности – это нарушение конфиденциальности, перехват информации, кража информации;

- угроза работоспособности системы – различные угрозы, которые приводят к нарушению или прекращению работы системы. Это атаки злоумышленников, сбои в программном обеспечении, ошибки пользователей.

Любая СЭД должна быть защищена от вышеперечисленных угроз.

Источники угроз СЭД это либо обычные пользователи, либо системные администраторы. Ошибки программного обеспечения. Можно выделить несколько групп:

- пользователи системы;

- администраторы, ИТ-персонал;

- злоумышленники.

Ошибок обычных пользователей системы всегда много. Пользователь системы – это потенциальный злоумышленник, он может сознательно или не сознательно нарушить конфиденциальность информации [1].

Отдельная группа – это администраторы и ИТ-персонал, либо служба информационной безопасности. Данная группа имеет неограниченные возможности, доступ к хранилищам, поэтому данную группу нужно хорошо контролировать и координировать. Они имеют не только большие полномочия, но и высоко квалифицированы в вопросах информационной безопасности. Согласно многим исследованиям, от 70% до 80% потерь – это внутренние атаки. А вот внешние злоумышленники индивидуальны, это могут быть как конкуренты, так и партнеры.[7]

Модели нарушителя в области СЭД (пользователь имеет ограниченные и неограниченные права доступа к СЭД)

Рассмотрим модели нарушителя в СЭД в том случае, когда у пользователя ограниченные и неограниченные права доступа к СЭД.

1. Нарушитель – имеет доступ к Web-интерфейсу (права ограничены).

Атаки: Одна из простейших атак – «отказ в обслуживании». Для того, чтобы это реализовать, злоумышленник может выполнять как атаки на определенного пользователя, так и на всю сеть. При этом злоумышленник может проводить атаки из разряда «раскрытие параметров». К примеру, если нарушитель подключился к сети, то может возникнуть угроза того, что он сможет перехватить пакеты в сети и из данных, которые содержатся в них, сможет определить маску сети, пару IP-MAC – адресов сети, данные о рабочих станциях. Посредством этого открывается возможность атаки типа «нарушение целостности». Последние два вида атак на всю систему невозможны, потому что у нарушителя есть лишь HTTPS –доступ к Web-интерфейсу ЦР, при всем том, на пути между ним и ЦР расположен МСЭ.[6]

Защита:

Для организации защиты от данных атак отделу информационной безопасности необходимо постоянно контролировать новые подключения к сети и проверять сетевой трафик. Помимо всего этого, сеть необходимо конфигурировать так, чтобы нарушитель не смог перехватить пакеты. Если злоумышленник все-таки узнал MAC-адрес и IP-адрес пользователя сети УЦ и зашел с его параметрами в сеть, то у него не должно быть возможности сделать какие-либо действия от имени пользователя. Поэтому, в системе должна присутствовать система аутентификации и идентификации пользователей, чтобы злоумышленник , который узнал физические параметры ЭВМ в сети, не имел возможности ими воспользоваться.

2. Зарегистрированный пользователь (наделен всеми доступными обычному пользователю возможностями: обменом подписанными сообщениями с другими зарегистрированными пользователями, наделен возможностью подтверждать достоверность ЭП, отправлять запросы на выдачу и отзыв сертификата, ключа подписи).

Атаки:

Атаки типа «нарушение целостности» пользователь может выполнять запросы на создание и отзыв сертификатов или менять параметры уже существующих. Большой угрозой в таком

случае может быть возможность использования злоумышленником ЭП пользователя. Нарушитель зарегистрирован в ЦР, и его запросы будут проходить в ЦС. Исходя из чего для защиты от возможных атак на УЦ нужно ограничить число одновременных подключений с одного IP-адреса, прекратить соединение пользователей с каким-либо элементом, кроме ЦР а к ЦР разрешить только доступ на просмотр к Web-интерфейсу по протоколу HTTPS.

Защита:

Для того, чтобы сократить возможности нарушителя, который завладел рабочей станцией пользователя , к минимуму, нужно в УЦ запретить автоматическую обработку запросов на выдачу, отзыв или изменение сертификатов с компьютеров пользователей системы. Данные действия с сертификатами нужно осуществлять именно с компонента УЦ –АРМ администратора (АРМА).

Модели нарушителя в области СЭД (нарушитель находится в выделенной сети или пытается захватить автоматизированное рабочее место (АРМ))

1. Нарушитель находится в выделенной сети УЦ

Атаки:

В предоставленной модели нарушитель конфигурировать пакеты и менять адрес отправителя, указывая адрес компонентов системы. Для того, чтобы избежать такие атаки все компоненты системы УЦ должны иметь ЭП, что поспособствует идентификации получаемых пакетов и даст возможность защититься от различных фальсифицированных пакетов.

Защита:

В ЦС должна храниться база данных сертификатов открытых ключей ЭП и закрытые ключи ЭП только зарегистрированных пользователей. Поэтому, прежде чем попасть в ЦС, запрос сначала проходит проверку на соответствие в ЦР. При отправки зарегистрированного лица он передается в ЦС, в противном случае пропускается. Отсюда можно сделать вывод, что в ЦС поступают только те запросы, которые проходят ЦР, поэтому необходимо устанавливать МСЭ перед ЦС, который пропускает только пакеты от ЦР для защиты от потенциальных атак со стороны других компонентов УЦ.[2]

2. Нарушитель захватил АРМ

Атаки:

Нарушитель может создавать запросы на регистрацию новых пользователей, так же может удалять или модифицировать уже существующие профили. Кроме этого, злоумышленник может создавать запросы на создание или отзыв сертификатов, а также может копировать базы данных зарегистрированных пользователей ЦР и базу данных сертификатов.

Защита:

Разумным решением будет разделить полномочия у пользователей. Подразумевается наличие двух пользователей УЦ: администратора УЦ и оператора УЦ. Первый в свою очередь отвечает за настройку ПО УЦ, создание базы данных ЦР и ЦС, может изменять и удалять профили уже зарегистрированных пользователей, а также может отзывать действующие сертификаты.[3] При сбое системы администратор УЦ должен восстановить ее работоспособность, посредством использования резервных копий. Оператор УЦ в свою очередь может создавать пользователей и предоставлять им сертификаты (запросы на выдачу сертификатов). [7]

Модели нарушителя в области СЭД (злоумышленник захватил центр регистрации (ЦР) или центр сертификации (ЦС))

1. Нарушитель захватил ЦР

Атаки:

В таком случае злоумышленник захватил связующим звеном между пользователями системы ЭП и УЦ и владеет большими полномочиями. Благодаря этому он может отключить от сети ЦР, блокировать ЦС и посредством этого прекратить деятельность УЦ. Посредством этого, все действия с ЭП в это время будут трудно реализуемы.

Защита:

Для повышения безопасности в ЦР должна быть предоставлена возможность разграниче-

ния полномочий, а конкретно: должны быть две роли УЦ – оператор ЦР и администратор ЦР. У обоих пользователей должны отсутствовать права на установку или модификацию ПО.

2. Нарушитель захватил ЦР

Осуществление атаки типа «раскрытие параметров» не составляет больших затруднений. Кроме параметров самого ЦР в нем зафиксированы соответствующие сетевые настройки АРМА и ЦС. А вот атаки типа «нарушение целостности» , можно формировать запросы к ЦС напрямую (по сертификатам). К профилям пользователей можно обращаться и менять саму базу данных. Кроме вышеперечисленных действий можно контролировать изменения в системе или же вовсе скопировать базу данных авторизированных пользователей УЦ.

Защита:

У оператора присутствуют все нужные ему полномочия для полноценного функционирования ЦР, права подписывать запросы на выпуск сертификатов, создание новых и т.д. Но опять же у него нет прав удаления базы данных пользователей, создание новых таблиц, вывода таблиц полностью на экран, изменение и просмотра списка сертификатов и секретных ключей ЦР, все того, чем владеет администратор ЦР.

3. Нарушитель захватил ЦС

Атаки:

Одна из самых простых атак, атака типа «отказ в обслуживании» - изменение сетевых настроек или выключение сетевого интерфейса, посредством чего происходит полная остановка всей системы ЭП. Так же может произойти удаление базы данных сертификатов открытых ключей и секретных ключей.

Злоумышленник сможет обнаружить состав самого ЦС, и сетевые параметры ЦР и, вероятно, версию ОС И ПО ЦР. Одними из самых опасных атак являются атаки типа «нарушение целостности». У нарушителя есть доступ к базе данных ЦС, то есть он может изменять базу. Сделав копию системы от может выполнять действия от имени пользователя ЭП.

Защита:

Необходимо ввести разграничение полномочий по ролям путем создания двух ролей УЦ: оператора ЦС и администратора ЦС. Оператор УЦ имеет возможность создавать новые учетные записи и право их изменять. Администратор ЦС имеет права на создание и удаление баз данных, но у него нет прав на добавление новых записей, но есть преимущество изменять их.

У одной и другой роли должны отсутствовать права на установку ПО, и права на вывод содержимого базы данных.

Ниже представлены комментарии к моделям нарушителя.

1. Обеспечение сохранности документов.

Каждая СЭД, которая претендует на звание «защищенной» должна как минимум иметь механизм защиты от базовых угроз: обеспечение сохранности документов, протоколирование действий пользователей.

СЭД должна обеспечивать сохранность документов от потери и порчи, а так же должна иметь способность их быстрого восстановления. Статистика такова, что 45% случаев потери важных данных исходят из физических причин таких как поломка аппаратуры, а 35% объясняется ошибками пользователей и менее 20% - это вредоносные программы и злоумышленники.[10]

Взять, к примеру, СЭД, которые используют базы данных Microsoft SQL Server или Oracle, имеют предпочтение использовать средства резервного копирования от разработчика СУБД. Другие же системы имеют свои подсистемы резервного копирования, которые разработаны самим производителем СЭД. Также сюда следует включить способность восстановления не только данных, но и самой системы в случае ее искажения, повреждения.[5]

1. Обеспечение безопасного доступа.

Этот пункт постоянно все понимают под безопасностью СЭД, тем самым постоянно ограничивают понятие безопасности систем. Безопасный доступ к информации, находящейся внутри СЭД осуществляется посредством аутентификации и разграничением прав пользователя.

В данном пункте следует акцентировать внимание на методах аутентификации. Один из самых популярных методов – парольный. Самый действенный способ аутентификации – имуще-

ственный, это различные USB-ключи, смарт-карты.

Одним из самых надежных методов проведения идентификации и последующей аутентификации способ – это биометрический (отпечаток пальца, сканирование сетчатки глаза, голос).

Еще один из главных параметров аутентификации –количество учитываемых факторов. Многофакторность.

2. Разграничения прав пользователей и конфиденциальность.

В каждой системе обязано быть разграничение прав пользователя и чем детальнее, тем эффективнее. Возможно, потребуется больше времени на настройку, но в результате мы получим наиболее защищенную систему.

Большим плюсом для конфиденциальности данных имеют криптографические методы защиты данных. Их использование не дает нам нарушить конфиденциальность документов, даже в случае, если документ попал в руки стороннего лица. Не нужно забывать, что каждый криптографический алгоритм имеет такое свойство как криптостойкость, у любой защиты есть предел. [8]

Помимо всего вышесказанного, не нужно забывать об организационных мерах защиты. Насколько бы криптография не была сильна, ничто не помешает третьему лицу просмотреть информацию, стоя за плечом человека, у которого есть доступ.

3. Обеспечение подлинности документов.

На сегодняшний день одним из главных и почти единственных предлагаемых на рынке продуктом для обеспечения подлинности документов является электронная подпись. Принцип работы которой основан на технологиях шифрования с ассиметричным ключом.

Многие производители СЭД уже имеют встроенные в свои системы средства для использования ЭП, как к примеру система Directum или система Евфрат-Документооборот. Такому содействию с ЭП способствовало и появление закона о ЭП (№63-ФЗ от 06.04.11г.), в котором электронная подпись стала иметь юридическую силу наравне с собственноручной подписью. [4]

4. Протоколирование действий пользователей – один из самых важных пунктов в защите электронного документооборота. Его грамотное использование в системе позволит проконтролировать все незаконные действия и отыскать злоумышленника. Такая функция обязательно должна быть в самой СЭД. Помимо всего, дополнительно можно использовать ресурсы сторонних разработчиков, а именно Microsoft или Oracle, в которых есть все необходимые средства для защиты. Кроме того, не нужно забывать о функционале операционных систем по протоколированию действий пользователей.

Заключение

Главная проблема при организации защиты системы электронного документооборота это далеко не технические средства, а лояльность пользователей. При попадании документа пользователю автоматически нарушается конфиденциальность данного документа по отношению к пользователю. Техническими средствами в данном случае тяжело как-либо предотвратить утечку документа через данного пользователя. Ключевые средства защиты в данном случае – это организационные меры по ограничению доступа к конфиденциальной информации и работы с самим пользователем.

СЭД отечественных разработчиков можно поделить на две группы – ориентированные на коммерческое использование и использование в государственных структурах. Это совсем не означает, что их использование нацелено только на что-то конкретное, некоторые системы зачастую используются как в государственных структурах, так и в коммерческих. Любая из данных групп имеет свою особенность, даже не только в самой технологии организации документооборота, делопроизводства, но и в системах защиты.

Одно из основных отличий в системах защиты – это алгоритмы, которые используются в шифровании и в ЭП. Почти все системы имеют парольную аутентификацию и разграничения доступа пользователей. Многие из них имеют также способность интеграции с Windows- аутентификацией, что позволяет пользоваться дополнительными инструментами аутентификации , которые поддерживает Windows. Не все из перечисленных пунктов имеют свою криптографическую

защиту, будь то шифрование или ЭП. Во многих продуктах это возможно реализовать только с помощью дополнительных средств разработчиков.

Подход к защите электронного документооборота должен быть комплексным. Нужно со всех сторон оценивать предполагаемые угрозы и риски СЭД и возможный ущерб от реализованных угроз. Также немаловажны моменты защиты аппаратных средств системы, защиты сетевой среды, в которой работает система, защита каналов передачи данных и сетевого оборудования. Комплекс организационных мер имеет огромную роль на каждом уровне защиты, но его, к сожалению, часто упускают из вида, несмотря на проведенный инструктаж и подготовку рядового персонала к работе с конфиденциальной информацией.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Барченков А.И. Документоведение и защита конфиденциальной информации. Учеб.пособие.-СПб.:Изд-во: СПбГПУ, 2003.-154с.

2. Белов С.П. Подготовка к внедрению систем электронного документооборота. Монография. –М.: Мир науки, 2016.-210с. –ISBN 978-5-9907048-9-3.

3. Бобылева М.П Управленческий документооборот: от бумажного к электронному. М.: Издательский дом МЭИ.-2010.-296с.

4. Васильева А.С., Власова О.А. Информационное обеспечение управления малым предприятием//Решетниковские чтения: материалы XXI Междунар.науч.практич.конф./ Красноярск с.315-316

5. Давыденко Е.А. Конфиденциальное делопроизводство: учебное пособие/ Издательство Нижневартовский гос.ун-т.2013

6. Куняев Н.Н., Демушкин А.С., Фабричнов А.Г. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник/ под общ.ред Н.Н. Куняева. М.: Логос, 2011.

7. Кулешов С.И. Особенности защиты электронного документооборота// Актуальные вопросы обеспечения информационной безопасности: научно – практическая конференция. Белгород.

8. Никитина Т.П. Электронные системы управления документооборотом. Учеб.пособие.- Ярославль.:МУБиНТ, 2012г.-204с.

9. Романов Д.А. Правда об электронном документообороте.-М.:Альт-Пресс, 2014г.-219с.

10. Автоматизация делопроизводства и документооборота на предприятии. Основы национального делопроизводства. [электронный ресурс]. – URL: http://www.directum.ru/339091.aspx (дата обращения 07.02.2020)

11. Защита систем электронного делопроизводства. [электронный ресурс] URL: http://www.ixbit.com/soft/sed.shtml.(дата обращения 02.02.2020)

REFERENCES

1. Barchenkov A.I. Documentation and protection of confidential information. Textbook.-SPb.: Publishing House: SPbSPU, 2003.-154s.

2. Belov S.P. Preparation for the implementation of electronic document management systems. Monograph. –M.: World of Science, 2016.-210s. –ISBN 978-5-9907048-9-3.

3. Bobyleva MP Management workflow: from paper to electronic. M .: Publishing house MEI.-2010.-296s.

4. Vasiliev A.S., Vlasova O.A. Information support for small business management // Reshetnikov Readings: Materials of the XXI International Scientific Practical Conference / Krasnoyarsk p. 315-316

5. Davydenko EA Confidential office work: a training manual / Publishing house Nizhnevartovsk gos.un-t. 2013

6. Kunyaev N.N., Demushkin A.S., Fabrichnov A.G. Confidential record keeping and secure electronic document management: textbook / ed.

7. Kuleshov S.I. Features of protection of electronic document management // Actual issues of ensuring information security: a scientific and practical conference. Belgorod.

8. Nikitina T.P. Electronic document management systems. Textbook.- Yaroslavl.: MUBiNT, 2012.-204s

9. Romanov D.A. The Truth About Electronic Document Management.-M.: Alt-Press, 2014.-219s..

10. Automation of paperwork and workflow at the enterprise. Fundamentals of national office work. [electronic resource]. - URL: http://www.directum.ru/339091.aspx (accessed 07.02.2020)

11. Protection of electronic record keeping systems. [electronic resource] URL: http://www.ixbit.com/soft/sed.shtml.(released on 02.02.2020)

Информация об авторах

Семенова Анна Александровна – магистрант кафедры ИСиЗИ, Иркутский государственный университет путей и сообщений, г. Иркутск, e-mail: anna.siemienova.1996@mail.ru.

Глухов Николай Иванович – директор центра информационной безопасности транспортной инфраструктуры, к.э.н., доцент кафедры ИСиЗИ, Иркутский государственный университет путей и сообщений, г. Иркутск, e-mail: gni1953@mail.ru.

Authors

Semenova Anna Aleksandrovna – graduate student of the Department of ISIS, Irkutsk State University of Railwais and Communication, Irkutsk, e-mail: anna.siemienova.1996@mail.ru.

Glukhov Nikolay Ivanovich – Director of the Center for Information Security of Transport Infrastructure Ph.D., Associate Professor of the Department of ISIS, Irkutsk State University of Railways and Communications, Irkutsk, e-mail: gni1953@mail.ru.

Для цитирования

Семенова А.А., Глухов Н.И. Анализ уязвимостей современных систем электронного документооборота // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №2(7). – С. 32-38 – DOI: 10.26731/2658-3704.2020.2(7).32-38 – Режим доступа: http://ismm-irgups.ru/toma/27-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.06.2020)

For citations

Semenova A.A., Glukhov N.I. Analysis of vulnerabiliti of modern electronic documentation systems // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2020. No. 2(7). P. 32-38. DOI: 10.26731/2658-3704.2020.2(7).32-38 [Accessed 01/06/20]