# СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ДОКУМЕНТООБОРОТА ОРГАНИЗАЦИИ

**Е.В. Чернышова,** *канд. техн. наук, доцент*
**С.С. Тупицина,** *студент*
**Воронежский государственный университет инженерных технологий**
**(Россия, г. Воронеж)**

*DOI: 10.24411/2500-1000-2020-10941*

***Аннотация.*** *На сегодняшний день существуют различные программные продукты, которые направлены на решение задачи защиты электронного документооборота в организации. Однако большинство из них являются платными, что не всегда позволяет использовать их в небольшой организации, или же они содержат ограниченный функционал, что не позволяет их использовать для всеобъемлющей защиты информации. Поэтому проведенные в работе анализ и совершенствование защищенного документооборота позволят более детально понять суть и принципы организации защищенного документооборота, как в Российской Федерации, так и за ее пределами, а разработанная система позволит обеспечить комплексную защиту персональных данных организации.*

***Ключевые слова:*** *система защиты персональных данных, информационная безопасность.*

Разработка частной модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных (ИСПДн) и проектирования системы защиты персональных данных (СЗПДн), включает в себя: построение предварительного перечня угроз безопасности персональных данных (с учетом рассматриваемой модели нарушителя); определение вероятности реализации угроз (для каждой угрозы из предварительного перечня); определение опасности угроз (для каждой угрозы из предварительного перечня); определение актуальности угроз (для каждой угрозы из предварительного перечня); описание возможных мер противодействия (технических или организационных) угрозам (для актуальных угроз).

Таблица. Совершенствование информационной безопасности персональных данных (коэффициент вероятности реализации угрозы рассчитывается по формуле: Y=(Y1+Y2)/20, где Y1 уровень исходной защищенности, а Y2 – вероятность реализации угрозы)

| Тип угроз безопасности ПДн | Исходный уровень защищенности (Y1) | Вероятность реализации угрозы (Y2) | Коэффициент вероятности реализации угрозы (Y) | Возможность реализации | Опасность |
|---|---|---|---|---|---|
| Угрозы от утечки по техническим каналам | | | | | |
| 1.1. Угрозы утечки акустической информации | 5 | 5 | 0,5 | средняя | средняя |
| 1.2. Угрозы утечки видовой информации | 5 | 5 | 0,5 | средняя | средняя |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 5 | 0 | 0,25 | низкая | низкая |
| 2. Угрозы несанкционированного доступа к информации. | | | | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | | | | | |

| Тип угроз безопасности ПДн | Исходный уровень защищенности (Y1) | Вероятность реализации угрозы (Y2) | Коэффициент вероятности реализации угрозы (Y) | Возможность реализации | Опасность |
|---|---|---|---|---|---|
| 2.1.1. Кража ПЭВМ | 5 | 0 | 0,25 | низкая | низкая |
| 2.1.2. Кража носителей информации | 5 | 5 | 0,5 | средняя | средняя |
| 2.1.3. Кража ключей и атрибутов доступа | 5 | 0 | 0,25 | низкая | низкая |
| 2.1.4.Кражи,модификации уничтожения информации | 5 | 0 | 0,25 | низкая | низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | 5 | 5 | 0,5 | средняя | средняя |
| 2.1.6.Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ | 5 | 0 | 0,25 | низкая | низкая |
| 2.1.7.Несанкционированное отключение средств защиты | 5 | 2 | 0,35 | средняя | средняя |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). | | | | | |
| 2.2.1. Действия вредоносных программ (вирусов) | 5 | 2 | 0,35 | средняя | средняя |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | 5 | 5 | 0,5 | средняя | средняя |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | 5 | 0 | 0,25 | низкая | средняя |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | | | | |
| 2.3.1. Утрата ключей и атрибутов доступа | 5 | 0 | 0,25 | низкая | низкая |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | 5 | 5 | 0,5 | средняя | средняя |
| 2.3.3. Непреднамеренное отключение средств защиты | 5 | 10 | 0,75 | высокая | высокая |
| 2.3.4. Выход из строя аппаратно-программных средств | 5 | 5 | 0,5 | средняя | средняя |
| 2.3.5. Сбой системы электроснабжения | 5 | 5 | 0,5 | средняя | средняя |
| 2.3.6. Стихийное бедствие | 5 | 10 | 0,75 | высокая | высокая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей | | | | | |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | 5 | 0 | 0,25 | низкая | низкая |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | 5 | 0 | 0,25 | низкая | низкая |
| 2.5.Угрозы несанкционированного доступа по каналам связи. | | | | | |
| 2.5.1.Угроза «Анализ сетево- | 5 | 0 | 0,25 | низкая | низкая |

| Тип угроз безопасности ПДн | Исходный уровень защищенности (Y1) | Вероятность реализации угрозы (Y2) | Коэффициент вероятности реализации угрозы (Y) | Возможность реализации | Опасность |
|---|---|---|---|---|---|
| го трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: | | | | | |
| 2.5.1.1. Перехват за пределами с контролируемой зоны | 5 | 5 | 0,5 | средняя | средняя |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | | 0 | 0,25 | низкая | низкая |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | 5 | 10 | 0,75 | высокая | высокая |
| 2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | 5 | 10 | 0,75 | высокая | высокая |
| 2.5.3.Угрозы выявления паролей по сети | 5 | 0 | 0,25 | низкая | низкая |
| 2.5.4.Угрозы навязывание ложного маршрута сети | 5 | 0 | 0,25 | низкая | низкая |
| 2.5.5.Угрозы подмены доверенного объекта в сети | 5 | 0 | 0,25 | низкая | низкая |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 5 | 5 | 0,5 | средняя | средняя |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | 5 | 5 | 0,5 | средняя | средняя |
| 2.5.8.Угрозы удаленного запуска приложений | 5 | 10 | 0,75 | высокая | высокая |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | 5 | 5 | 0,5 | средняя | средняя |

Разработка модели нарушителя. По сфере воздействия на компанию, потенциальных нарушителей можно разделить на внутренних и внешних. Под внутренними нарушителями подразумеваются сотрудники компании, имеющие физический и/или логический доступ к ресурсам ИС (программно-техническим и/или информационным). Подразумеваются физические лица, не являющиеся сотрудниками компании, но имеющие физический и/или логический доступ к ресурсам ИС (программно-техническим и/или информационным), в том числе лица, получившие доступ незаконным способом.

Внутренних нарушителей в зависимости от способа, полномочий доступа к подсистемам ИС компании и уровня квалификации можно подразделить на шесть категорий: обслуживающий персонал, пользователь ИС, удаленные пользователи ИС, администраторы, технический персонал, программисты.

Инженерно-технические меры по защите информации. В целях защиты кабинета для совещаний от утечки информации актуально следующее предложение: так как проникновение злоумышленника возможно через дверь в кабинет, необходимо создать защитный рубеж. Для этого на дверь из коридора в кабинет устанавливается

магнитоконтактный извещатель типа ИО-104-4. Этот извещатель обеспечивает замыкание и размыкание контактов геркона при приближении магнита к геркону на расстояние не более 10 мм контакты и удалении более 45 мм.

Учитывая небольшую площадь кабинета для совещаний, целесообразно применять или пассивные оптико-электронные извещатели или активные волновые с регулируемой мощностью излучения. Выгодно установить комбинированный извещатель «Сокол-2», совмещающий пассивный инфракрасный и радиоволновой принципы обнаружения. Он обеспечивает дальность действия: минимальную – 3-5 м, максимальную – 12 м. Он может крепиться к стене или на потолке, имеет высокую помехоустойчивость.

Целесообразно установить локальные извещатели для охраны компьютера. Для защиты информации в компьютере от физического контакта его со злоумышленником и хищения информации путём копирования или изъятия винчестера в качестве извещателя можно использовать ёмкостной извещатель «Пик».

Для прекращения функционирования оптического канала утечки информации «окно кабинета – окно противоположного жилого дома» можно применить следующие меры: шторы на окна; жалюзи; тонированные плёнки на стёклах.

Для защиты от утечки речевой информации в кабинете для совещаний необходимо существенно повысить звукоизоляцию дверей как наиболее слабого звена в акустической защите и стены.

В качестве меры, повышающей энергетическое скрытие речевой информации в кабинете для совещаний, на стенах можно укрепить виброакустические излучатели акустического генератора помех «Барон».

Для исключения утечки информации через батареи и трубы отопления перед батареями устанавливают резонансные экраны в виде деревянных перегородок с отверстиями, или используются виброакустические преобразователи прибора «Барон».

Для исключения возможности функционирования скрыто установленного диктофона применяем средство «Бубен». В целях подавления сотовых сигналов во время конфиденциальных совещаний в кабинете для совещаний необходимо предусмотреть генератор шума «Аллигатор 100+4G LTE», с помощью которого возможно подавить сигнал 3G и 4G сети. Необходимо установить средство подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд».

Для защиты документов, создаваемых в системе электронного документооборота сформировать электронную цифровую подпись (ЭЦП). Также не обходимо установить антивирус «Касперский» на все компьютеры.

Выбор системы электронного документооборота. Для закрытых акционерных обществ выгоднее всего выбрать документооборот Е1 Евфрат, так как он дает возможность в значительной степени повысить эффективность деятельности как организации в целом, так и отдельных сотрудников, снизить время обработки и согласования документов, повысить исполнительскую дисциплину, упростить процесс поиска документов и устранить проблему их утери, снизить затраты на ведение архива, повысить безопасность работы с информацией, а также вывести бизнес на новый уровень оперативности, гибкости и мобильности.

В отличие от большинства конкурентов, платформа Е1 от начала до конца – продукт собственной разработки. Такое качество придает платформе Е1 гибкость и возможность оперативной адаптации к меняющимся условиям рынка, особенностям и изменениям законодательства, формирования конкурентной цены как для коробочного решения, так и для проектных внедрений. Е1 спроектирован и реализован таким образом, чтобы полностью исключить процесс программирования при внедрении системы, её настройке и последующей эксплуатации. От штатного администратора компании любого размера и структуры не требуется никаких специальных знаний или высокой квалификации для запуска и обслуживания Е1.

Благодаря целому комплексу уникальных технологических возможностей, помощи, опыту, которыми может поделиться Cognitive Technologies с организациями, начинающими использовать E1, использовать систему легко и просто.

Вывод. Быстрота внедрения не влияет на качество и уникальные технологии системы - E1 позволяет гибко управлять неструктурированными и слабоструктурированными бизнес-процессами, которые все больше проникают в жизнь современной организации. Такой подход, называемый dynamic case management, наиболее актуален сегодня, как необходимый элемент быстрого реагирования на возникающие события в процессе операционной деятельности организации.

**Библиографический список**

1. Нормирование требований к характеристикам программных систем защиты информации / Скрыпников А.В., Хвостов В.А., Чернышова Е.В., Самцов В.В., Абасов М.А. // Вестник Воронежского государственного университета инженерных технологий. – 2018. – Т. 80. № 4 (78). – С. 96-110.

2. Обоснование закономерностей и расчёт параметров для распределения степени вершин безмасштабной сети / Скрыпников А.В., Чернышова Е.В., Прокофьев О.Е. // Материалы международной научно-практической конференции «Вопросы образования и науки». – Научный альманах (Тамбов, 31 мая 2016 г.). – 2016. – № 5-3 (19). – С. 156-160.

3. Построение дискретной макро-модели для безмасштабной сети / Скрыпников А.В., Чернышова Е.В., Прокофьев О.Е. // Материалы II международной научно-практической конференции «Инновационные подходы и современная наука». – Киев: Центр научных публикаций, 2016. – С. 128-132.

4. Риск-модели процесса реализации целенаправленных атак с использованием технологий ROOTKIT / Чернышова Е.В., Колпакова Т.А., Каширо П.А., Золотухина У.В. // В сборнике: стандартизация, управление качеством и обеспечение информационной безопасности в перерабатывающих отраслях АПК и машиностроении. – 2016. С. 404-409

5. Эталонное моделирование критически важных объектов информатизации при комплексном обеспечении их информационной безопасности / Дубровин А.С., Лютова Т.В., Чернышова Е.В. // В сборнике: Современные инструментальные системы, информационные технологии и инновации, сборник научных трудов XII-ой Международной научно-практической конференции: в 4-х томах. Ответственный редактор: Горохов А.А. – 2015. – С. 64-68.

## IMPROVEMENT OF THE ORGANIZATION'S DOCUMENT CIRCULATION SYSTEM

**E.V. Chernyshova,** *Candidate of Technical Sciences, Associate Professor*
**S.S. Tupicina,** *Student*
**Voronezh State University of Engineering Technologies**
**(Russia, Voronezh)**

***Abstract.*** *Today, there are various software products that are aimed at solving the problem of protecting electronic document flow in an organization. However, most of them are paid, which does not always allow them to be used in a small organization, or they contain limited functionality, which does not allow them to be used for comprehensive information protection. Therefore, the analysis and improvement of secure document circulation carried out in this work will allow us to understand in more detail the essence and principles of organizing secure document circulation, both in the Russian Federation and abroad, and the developed system will provide comprehensive protection of the organization's personal data.*

***Keywords:*** *personal data protection system, information security.*