

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Secreta ad utilitatem



Секретно для пользы

№ 13

По-настоящему безопасной
можно считать лишь систему,
которая выключена, замурована
в бетонный корпус, заперта
в помещении со свинцовыми
стенами и охраняется вооруженным
караулом, однако и в этом случае
сомнения не оставят меня.

Ю. Спаффорд

А. Ю. Даниленко

БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Технология защиты
электронных
документов



URSS

А. Ю. Даниленко

БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

**Технология защиты
электронных
документов**



URSS
МОСКВА

ББК 22.18 30–5–05 32.811 32.817 32.973–02 65.050

Даниленко Андрей Юрьевич

Безопасность систем электронного документооборота: Технология защиты электронных документов. — М.: ЛЕНАНД, 2015. — 232 с.
(Основы защиты информации. № 13.)

Всякий раз, когда заходит разговор об обмене информацией в электронной форме, будь это платежи через Интернет, почта или переписка в Скайпе, рано или поздно возникает тема безопасности информации. Если же мы говорим об электронном документообороте, то есть о движении электронных документов, совместной работе с ними, принятии решений на их основе, набор вопросов существенно возрастает. Например:

- ✓ Что такое юридическая значимость электронного документа и как ее обеспечить?
- ✓ Как обеспечить конфиденциальность информации?
- ✓ Можно ли быть уверенными в неизменности данных, содержащихся в нашем документе, если мы сами их не модифицировали?
- ✓ Имеет ли смысл шифровать электронные документы, и если да, то как это делать?
- ✓ Какова роль электронных подписей при работе с такими системами?
- ✓ Можем ли мы доверять данной информационной системе свою информацию, а если можем, то почему?
- ✓ И вообще, что такое электронный документ?

Обсуждению этих и многих других вопросов, связанных с электронными документами и работой с ними, посвящена предлагаемая книга.

Формат 60×90/16. Печ. л. 14,5. Зак. № ИП-93.

Отпечатано в ООО «ЛЕНАНД».

117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISBN 978–5–9710–2114–8

© ЛЕНАНД, 2015

16725 ID 198564



Все права защищены. Никакая часть настоящей книги не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, а также размещение в Интернете, если на то нет письменного разрешения владельца.

ОГЛАВЛЕНИЕ

Используемые сокращения	9
Введение.....	10
1 Обеспечение информационной безопасности АИС различного назначения	12
1.1 Понятие информационной безопасности	12
1.2 Подходы к обеспечению ИБ	13
1.2.1 Теоретический подход	13
1.2.2 Нормативный подход.....	13
1.2.3 Практический подход	14
1.3 Применяемые СЗИ.....	15
1.3.1 Идентификация и аутентификация.....	15
1.3.2 Управление доступом	16
1.3.3 Протоколирование и аудит.....	18
1.3.4 Криптографические механизмы.....	19
1.4 Критерии оценки надежных компьютерных систем	20
1.5 Безопасность общесистемного и прикладного ПО.....	22
1.6 Математические модели политики безопасности.....	31
1.6.1 Дискреционная модель управления доступом.....	31
1.6.2 Мандатная модель	32
1.6.3 Рольное управление доступом.....	35
1.6.4 Распределенные системы.....	36
1.6.5 Каналы утечки информации.....	37
1.7 Безопасность СЭДО.....	38

2 Особенности СЭДО-ЗИ.....	43
2.1 Необходимые определения.....	43
2.1.1 Электронный документ.....	43
2.1.2 Система электронного документооборота.....	44
2.1.3 Система электронного документооборота в защищенном исполнении.....	44
2.1.4 Объекты защиты АИС	45
2.2 Функциональные особенности	45
2.2.1 Источник появления проблем	46
2.2.2 Управление доступом	46
2.2.3 Бесконтрольное размножение	48
2.2.4 Перемещение документов	49
2.3 Математическое моделирование работы СЭДО-ЗИ.....	50
2.3.1 Модель работы пользователя СЭДО	50
2.3.1.1 Пути оптимизации работы сервера СЭДО.....	53
2.3.2 Обнаружение вторжений	54
2.3.3 Оценка возможного ущерба от действий нарушителей.....	58
2.3.4 Модель безопасности жизненного цикла документа	61
2.3.4.1 Дискреционная модель	62
2.3.4.2 Мандатная модель	65
2.3.4.3 Динамический контроль прохождения документов.....	67
2.3.5 Поиск наименее затратного пути в графе	70
2.4 Особенности атак на СЭДО-ЗИ.....	73
2.4.1 Атаки с использованием свойств алгоритмов хэширования	74
2.4.2 Атаки с подбором пароля	76
2.4.2.1 Атака подмены пользователя при входе в систему	76
2.4.2.2 Атака подмены пользователя, вошедшего в систему	79
2.4.3 Атаки типа «Отказ в обслуживании»	80
2.4.4 Атака легитимного пользователя.....	82
2.4.4.1 Описание механизма атаки.....	82

2.4.4.2	Предпосылки ее возможности.....	83
2.4.4.3	Возможности обнаружения и предотвращения.....	84
2.5	Особенности применения СЗИ.....	85
2.5.1	Структура механизмов безопасности АИС.....	85
2.5.2	Подходы к обеспечению безопасности ОС и СУБД.....	87
2.5.3	Каналы утечки информации в случае СЭДО-ЗИ.....	88
2.5.4	Идентификация и аутентификация.....	89
2.5.5	Управление доступом	91
2.5.5.1	Дискреционное управление доступом.....	92
2.5.5.2	Ролевое управление доступом.....	94
2.5.5.3	Мандатное разграничение доступа.....	95
2.5.6	Максимальное ограничение распространения информации	97
2.5.7	Максимальное сокращение количества копий	99
2.5.8	Уничтожение электронных документов.....	100
2.5.9	Резервное копирование.....	101
2.5.10	Ограничение прав административного персонала.....	102
2.5.11	Ограничение использования административных учетных записей пользователей.....	103
2.5.12	Печать документов.....	103
2.5.13	Протоколирование	105
2.5.14	Криптографические механизмы.....	108
2.5.15	Контроль целостности объектов системы.....	110
2.5.16	Шифрование	111
2.5.17	Электронная подпись.....	112
2.5.18	Передача документов между подразделениями.....	116
2.5.19	Взаимодействие с внешними системами	116
2.5.20	Межсетевое экранирование и антивирусная защита	117
2.6	Организационно-технические меры.....	117
2.7	Особенности СЭДО-ЗИ в случае применения облачных технологий.....	121
2.7.1	Преимущества облачных технологий.....	123

2.7.2	Недостатки облачных технологий и пути их преодоления.....	124
2.7.3	Возможные задачи для решения с применением облачных технологий в случае небольших предприятий.....	126
2.7.4	Безопасность обработки данных облачными сервисами.....	127
2.7.5	Система электронного документооборота на основе облачной инфраструктуры.....	130
2.8	Юридическая значимость электронных документов.....	131
2.8.1	Понятие юридической значимости.....	131
2.8.2	Возможность и перспективы реализации юридически значимого электронного документооборота.....	131
2.9	Выводы по главе.....	134
3	Проектирование и разработка СЭДО-ЗИ.....	135
3.1	Обследование.....	135
3.1.1	Область деятельности организации.....	136
3.1.2	Характеристики обрабатываемой информации.....	136
3.1.3	География фирмы.....	137
3.1.4	Организационная структура фирмы.....	138
3.1.5	Бизнес-процессы в фирме.....	140
3.1.6	Общая архитектура АИС.....	141
3.2	Формирование политики безопасности.....	144
3.2.1	Политика безопасности АИС.....	144
3.2.1.1	Модель угроз.....	144
3.2.1.2	Модель нарушителя.....	144
3.2.1.3	Описание политики управления доступом.....	145
3.2.2	Политика безопасности СЭДО-ЗИ.....	147
3.2.2.1	Формализованное описание политики безопасности.....	147
3.2.2.2	Политика безопасности ПК «Евфрат».....	153
3.3	Архитектура СЭДО-ЗИ.....	171
3.3.1	Функциональная архитектура.....	171

3.3.1.1	Базы данных	171
3.3.1.2	Сервер системы	172
3.3.1.3	Клиентские АРМ	172
3.3.1.4	Обработка содержательной информации.....	174
3.3.1.5	Просмотр и редактирование метаданных	174
3.3.1.6	Средства администрирования	174
3.3.1.7	Средства настройки СЭДО.....	176
3.3.1.8	Протоколирование.....	177
3.3.2	Архитектура СЗИ	178
3.3.2.1	Локализация СЗИ	178
3.3.2.2	Взаимодействие СЗИ ОС, СУБД и СЭДО-ЗИ.....	180
3.3.3	Взаимодействие с другими АИС	183
3.3.3.1	Возможные алгоритмы взаимодействия	183
3.3.3.2	Обеспечение информационной безопасности	184
3.4	Особенности процесса разработки СЭДО-ЗИ.....	184
3.5	Выводы по главе	188
4	Промышленная система электронного документооборота	190
4.1	Общий функционал	190
4.1.1	Общее описание	190
4.1.2	Документы	191
4.1.3	Функциональные обязанности пользователей.....	192
4.1.4	Схема обработки документов.....	193
4.1.5	Контроль исполнения документов.....	194
4.1.6	Обмен сообщениями между пользователями	196
4.1.7	Уведомления и напоминания	197
4.1.8	Обмен документами между серверами	197
4.2	Встроенные средства защиты информации.....	198
4.2.1	Идентификация и аутентификация.....	198
4.2.2	Управление доступом	199
4.2.2.1	Электронные документы	199

4.2.2.2	Письма внутренней почтовой системы	200
4.2.2.3	Поручения	200
4.2.3	Протоколирование	201
4.2.4	Шифрование сетевого трафика	201
4.2.5	Электронно-цифровая подпись	201
4.3	Встроенные механизмы настройки	202
4.3.1	Дизайнер форм электронных документов	202
4.3.2	Дизайнер маршрутов	203
4.4	Особенности реализации	204
4.4.1	Клиентские АРМ	204
4.4.2	Сервер системы	204
4.4.2.1	Сервер приложений	204
4.4.2.2	Сервисы Inproc и Outproc	205
4.5	Система Ника	207
4.6	Выводы по главе	210
Заключение		212
Список литературы		213