

УДК 007
ББК 32.81
Т65

Рецензенты:

И.А. Лазарев — доктор технических наук, профессор, академик МАН ИПТ, заслуженный деятель науки и техники РФ;

В.М. Глуценко — доктор экономических наук, профессор, академик МАН ИПТ.

Т65 **Трайнев, Владимир Алексеевич.**

Системный подход к обеспечению информационной безопасности предприятия (фирмы) : монография / В.А. Трайнев. — 5-е изд. — Москва : Издательско-торговая корпорация «Дашков и К°», 2022. — 332 с.

ISBN 978-5-394-05035-0.

В монографии изложен системный подход к построению комплексной защиты информационной системы предприятия (фирмы). Рассмотрены принципы и предпосылки обеспечения информационной безопасности предприятия (фирмы); характеристики угроз и анализ уязвимостей системы; требования к системе защиты.

Описывается подход к построению комплексной защиты интегрированной информационной системы предприятия (фирмы) с применением отечественных средств защиты.

Для специалистов, проектирующих информационные системы и средства их защиты, а также научных работников и студентов вузов.

Основу данной монографии составляют материалы учебного пособия
«Информационная безопасность предприятия»
(авторы А.А. Садердинов, В.А. Трайнев, А.А. Федулов).

ISBN 978-5-394-05035-0

© Трайнев В.А., Садердинов А.А.,
 Федулов А.А., 2018

© ООО «ИТК «Дашков и К°», 2018

Оглавление

Введение	4
Принятые сокращения	6
1. Основные принципы и предпосылки обеспечения информационной безопасности предприятия	7
1.1. Основные принципы обеспечения информационной безопасности предприятия	7
1.2. Предпосылки и цели обеспечения информационной безопасности предприятия	10
2. Политика информационной безопасности	13
2.1. Политика информационной безопасности России	13
2.2. Описание трехуровневой политики информационной безопасности	17
3. Характеристика угроз информационной безопасности	21
3.1. Классификация угроз	21
3.2. Примеры составов преступлений, в области информационного обеспечения предприятий, определяемые УК РФ.	21
3.3. Источники угроз	23
3.4. Наиболее распространенные угрозы в интегрированной информационной системе управления предприятием	24
3.5. Угрозы при взаимодействии интегрированной информационной системы управления предприятием с Internet	27
4. Анализ уязвимости информационных систем и оценка рисков	31
4.1. Уязвимость информационных систем	31
4.2. Классификация сетевых атак	32
4.3. Проблемы безопасности локальных вычислительных сетей и интегрированных информационных систем управления предприятием	44
4.4. Распределенное хранение файлов	51
4.5. Удаленные вычисления	52
4.6. Топологии и протоколы	52
4.7. Службы обмена сообщениями	53
4.8. Оценка рисков	53
5. Требования по обеспечению комплексной системы информационной безопасности	54
5.1. Требования по обеспечению информационной безопасности корпоративной информационной системы предприятия.	54

5.2. Требования к программно-аппаратным средствам	55
5.3. Требования к подсистеме идентификации и аутентификации:	55
5.4. Требования к подсистеме управления доступом	56
5.5. Требования к подсистеме протоколирования аудита	57
5.6. Требования к подсистеме защиты повторного использования объектов	58
5.7. Требования к защите критичной информации	58
5.8. Требования к средствам обеспечения целостности:	59
5.9. Требования к средствам управления ИБ	60
5.10. Требования к Межсетевому Экрану	61
6. Принципы построения систем информационной безопасности	67
6.1. Принципы и правила построения информационной системы предприятия	67
6.2. Принципы построения системы санкционированного доступа к ресурсам	72
6.3. Принципы построения подсистемы защиты интег- рированной комплексной информационной системы управления предприятием от угроз, исходящих из Internet.....	74
6.4. Службы и механизмы защиты	75
6.5. Идентификация и аутентификация	76
6.6. Управление доступом	79
6.7. Конфиденциальность данных и сообщений	82
6.8. Целостность данных и сообщений	83
6.9. Контроль участников взаимодействия	84
6.10. Регистрация и наблюдение	85
7. Структура защиты информации в интегрированной информационной системе управления предприятием	87
7.1. Структурная схема системы защиты информации интегрированной информационной системы управ- ления предприятием	87
7.2. Основные функции уровней защиты информации интегриро- ванной информационной системы управления предприятием	90
8. Отечественные и зарубежные программно-технические средства защиты информации в интегрированных инфор- мационных системах управления предприятием	94
8.1. Системы разграничения доступа (полномочий)	94
8.2. Электронный замок «Соболь»	94
8.3. Идентификация и аутентификация пользователей.	96

8.4. Регистрация попыток доступа к ПЭВМ.	96
8.5. Контроль целостности программной среды и запрет загрузки со съемных носителей.....	97
8.6. Возможности по администрированию	98
8.7. Криптографическое устройство eToken электронный замок eToken.....	98
8.8. Системы биометрической аутентификации.....	101
8.9. Решения по обеспечению безопасности корпоративной сети	103
8.10. Применение средств антивирусной защиты	104
8.11. Применение средств межсетевого экранирования	111
8.12. Защита на основе маршрутизатора с листами доступа.....	114
8.13. Защита внутренних информационных ресурсов корпоративной сети	114
8.14. Межсетевой экран PIX Firewall.....	117
8.15. WatchGuard Firebox System	121
8.16. Централизованное управление защитой	122
8.17. Схема децентрализованной защиты корпоративных серверов	124
8.18. Применение средств контроля электронной почты	127
8.19. Средство контроля и разграничения доступа к web	132
8.20. Сканирование электронной почты с помощью MIMESweeper for Domino.....	142
8.21. Применение средств контроля и регистрации событий безопасности	145
8.22. Создание виртуальных частных сетей (VPN)	169
8.23. Система централизованного управления RealSecure Site Protector	182
8.24. Оснащение объекта техническими средствами защиты и контроля информации	186
9. Система защиты информации в SAP R/3	198
9.1. Служба безопасности SAP R/3	198
9.2. Подключение ядра шифрования фирмы CryptoPro к компонентам mySAP.com через модифицированный MSNC-адаптер	199
9.3. Создание центра сертификации Windows 2000 на базе криптографического ядра фирмы CryptoPro	202
9.4. Настройка служб безопасности R/3	206
9.5. Задачи администрирования системы R/3.....	211

10. Сертификация информационных систем	214
10.1. Основные характеристики технических средств защиты от несанкционированного доступа	214
10.2. Требования по защите информации от несанк- ционированного доступа для автоматизированных систем	215
10.3. Требования к автоматизированным системам защиты третьей группы	215
10.4. Требования к автоматизированным системам защиты второй группы	220
10.5. Требования к автоматизированным системам защиты первой группы	226
10.6. Требования по защите информации от несанкциони- рованного доступа для средств вычислительной техники	248
10.7. Требования к межсетевым экранам. Показатели защищенности межсетевых экранов	266
11. Направления работ по созданию систем комплексной защиты информационной системы предприятия	278
11.1. Организация работ по защите от несанкциониро- ванного доступа ИИСУП	280
11.2. Классификация интегрированных информацион- ных систем управления предприятием	280
11.3. Система компьютерной безопасности	282
11.4. Оснащение объекта техническими средствами противодействия экономическому шпионажу и защи- ты речевой информации	288
11.5. Этапы проведения работ по обеспечению инфор- мационной безопасности предприятия	294
Приложение. Терминологический словарь	296
Литература	322