

# СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ</b> . . . . .	11
<b>ГЛАВА 1. ЗАЩИТА ОТ ИНФОРМАЦИОННЫХ АТАК — ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ</b> . . . . .	16
1.1. Автоматизированная система — объект защиты от информационных атак . . . . .	16
1.2. Уязвимости — ахиллесова пята автоматизированных систем . . . . .	21
1.2.1. Уязвимости «buffer overflow» . . . . .	25
1.2.2. Уязвимости «SQL injection» . . . . .	29
1.2.3. Уязвимости «format string» . . . . .	32
1.2.4. Уязвимости «Directory traversal» . . . . .	33
1.2.5. Уязвимости «Cross Site Scripting» . . . . .	34
1.2.6. Уязвимости программных реализаций стека TCP/IP . . . . .	35
1.2.7. Уязвимости протоколов стека TCP/IP . . . . .	36
1.3. Жизненный цикл информационной атаки . . . . .	38
1.3.1. Стадия рекогносцировки . . . . .	40
1.3.2. Стадия вторжения и атакующего воздействия . . . . .	48
1.3.3. Стадия дальнейшего развития атаки . . . . .	56
1.4. Последствия информационных атак . . . . .	58
<b>ГЛАВА 2. СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК И ИХ ФУНКЦИОНАЛЬНЫЕ ЗАДАЧИ</b> . . . . .	64
2.1. Существующие методы и средства защиты от информационных атак . . . . .	64
2.1.1. Средства криптографической защиты информации . . . . .	66
2.1.2. Средства разграничения доступа пользователей к информационным ресурсам АС . . . . .	71
2.1.3. Средства межсетевое экранирования . . . . .	73
2.1.4. Средства анализа защищенности автоматизированных систем . . . . .	76
2.1.5. Средства антивирусной защиты . . . . .	77
2.1.6. Средства защиты от спама . . . . .	78
2.1.7. Средства контентного анализа . . . . .	79
2.2. Системы обнаружения атак и история их развития . . . . .	80
2.3. Функциональная ниша систем обнаружения атак . . . . .	87
<b>ГЛАВА 3. СБОР ИСХОДНОЙ ИНФОРМАЦИИ СИСТЕМАМИ ОБНАРУЖЕНИЯ АТАК</b> . . . . .	93
3.1. Источники информации для систем обнаружения атак . . . . .	93
3.2. Сетевые датчики систем обнаружения атак . . . . .	100
3.3. Хостовые датчики систем обнаружения атак . . . . .	107

3.4. Сопоставление функциональных возможностей сетевых и хостовых датчиков . . . . .	112
3.5. Защита датчиков систем обнаружения атак от воздействий злоумышленников . . . . .	115
<b>ГЛАВА 4. МЕТОДЫ ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ АТАК . . .</b>	<b>118</b>
4.1. Классификация методов выявления атак . . . . .	118
4.2. Сигнатурные методы обнаружения атак . . . . .	120
4.3. Поведенческие методы выявления атак . . . . .	133
<b>ГЛАВА 5. ПРОТИВОДЕЙСТВИЕ ВЫЯВЛЕННЫМ ИНФОРМАЦИОННЫМ АТАКАМ . . . . .</b>	<b>145</b>
5.1. Пассивные методы реагирования на атаки . . . . .	145
5.1.1. Оповещение администратора безопасности о выявленных атаках . . . . .	146
5.1.2. Запись сведений об обнаруженной атаке в информационное хранилище системы . . . . .	150
5.1.3. Вывод предупреждающего сообщения . . . . .	151
5.2. Активные методы реагирования на атаки . . . . .	151
5.2.1. Блокирование ТСП-соединения, по которому реализуется атака . . . . .	151
5.2.2. Блокирование учетных записей пользователей . . . . .	152
5.2.3. Блокирование рабочей станции пользователя . . . . .	153
5.2.4. Блокирование приложения, являющегося источником атаки . . . . .	153
5.2.5. Блокирование сетевых атак посредством взаимодействия с межсетевыми экранами . . . . .	153
5.2.6. Изменение конфигурации коммуникационного оборудования АС . . . . .	156
5.2.7. Изолирование объекта атаки . . . . .	158
5.2.8. Предотвращение информационных атак . . . . .	158
5.2.9. Активное подавление источника атаки . . . . .	163
5.3. Реализация дополнительных методов реагирования СОА . . . . .	163
5.3.1. Использование механизма запуска внешних программ . . . . .	163
5.3.2. Использование специализированных сценарных языков . . . . .	164
5.4. Политика реагирования на инциденты безопасности . . . . .	164
<b>ГЛАВА 6. ОБЗОР СУЩЕСТВУЮЩИХ СИСТЕМ ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ АТАК . . . . .</b>	<b>169</b>
6.1. Системы обнаружения сетевых атак . . . . .	169
6.1.1. Система «Radware DefensePro» . . . . .	169
6.1.2. Система «ISS RealSecure» . . . . .	172
6.1.3. Система «ISS Proventia» . . . . .	175
6.1.4. Система «Juniper Networks IDP» . . . . .	178
6.1.5. Система «Cisco IDP 4200» . . . . .	181
6.1.6. Система «Symantec SNS 7100» . . . . .	184
6.1.7. Система «Snort» . . . . .	186
6.1.8. Система «Форпост» . . . . .	188
6.2. Системы обнаружения внутренних атак злоумышленников . . . . .	190
6.2.1. Система «InfoWatch Net Monitor» . . . . .	190
6.2.2. Система «Insider» . . . . .	193

6.2.3. Система «Урядник» . . . . .	195
6.2.4. Система «DeviceLock» . . . . .	197
<b>ГЛАВА 7. ПРОБЛЕМА ВЫБОРА СИСТЕМЫ ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ АТАК . . . . .</b>	<b>200</b>
7.1. Факторы выбора систем обнаружения атак . . . . .	201
7.2. Надежность и отказоустойчивость СОА . . . . .	208
7.3. Тестирование систем обнаружения атак . . . . .	218
<b>ГЛАВА 8. ОСОБЕННОСТИ ВНЕДРЕНИЯ И ЭКСПЛУАТАЦИИ СИСТЕМ ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ АТАК В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ПРЕДПРИЯТИЯ . . . . .</b>	<b>225</b>
8.1. Внедрение системы обнаружения атак . . . . .	225
8.1.1. Обследование автоматизированной системы . . . . .	226
8.1.2. Разработка технического проекта по внедрению системы обнаружения атак . . . . .	227
8.1.3. Обучение персонала . . . . .	228
8.1.4. Пусконаладочные работы, опытная эксплуатация и испытания системы . . . . .	230
8.2. Комплексное использование системы обнаружения атак с другими средствами защиты . . . . .	231
8.2.1. Решение по защите Интернет-портала . . . . .	231
8.2.2. Решение по защите Интранет-портала . . . . .	236
8.2.3. Решение по защите почтовой системы от вирусов, атак и спама . . . . .	240
8.2.4. Решение по защите от утечки конфиденциальной информации . . . . .	241
8.2.5. Решение по организации защищенного доступа пользователей к ресурсам сети Интернет . . . . .	246
8.2.6. Решение по комплексному мониторингу информационной безопасности автоматизированной системы . . . . .	250
<b>ГЛАВА 9. НОРМАТИВНО-ПРАВОВАЯ ОСНОВА ЗАЩИТЫ ОТ ИНФОРМАЦИОННЫХ АТАК . . . . .</b>	<b>255</b>
9.1. Обзор российского законодательства в области информационной безопасности . . . . .	255
9.2. Обзор международных стандартов в области информационной безопасности . . . . .	262
9.3. Стандарты в области обнаружения информационных атак . . . . .	268
9.4. Особенности использования «критериев оценки безопасности информационных технологий» (ISO 15408) для систем обнаружения атак . . . . .	273
<b>ГЛАВА 10. ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ИНФОРМАЦИОННЫХ АТАК . . . . .</b>	<b>282</b>
<b>ЗАКЛЮЧЕНИЕ . . . . .</b>	<b>294</b>
<b>СПИСОК СОКРАЩЕНИЙ . . . . .</b>	<b>296</b>
<b>ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ . . . . .</b>	<b>299</b>

<b>ПРИЛОЖЕНИЕ. ПРИМЕР ПРОФИЛЯ ЗАЩИТЫ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ АТАК</b> . . . . .	308
П. 1. Введение . . . . .	308
П. 1.1. Идентификация ПЗ . . . . .	308
П. 1.2. Аннотация ПЗ . . . . .	309
П. 1.3. Соглашения . . . . .	309
П. 1.4. Термины и определения . . . . .	310
П. 1.5. Структура ПЗ . . . . .	311
П. 2. Описание объекта оценки . . . . .	312
П. 3. Среда безопасности ОО . . . . .	312
П. 3.1. Предположения безопасности . . . . .	312
П. 3.2. Угрозы . . . . .	313
П. 3.3. Политика безопасности организации . . . . .	314
П. 4. Цели безопасности . . . . .	315
П. 4.1. Цели безопасности для ОО . . . . .	315
П. 4.2. Цели безопасности для среды . . . . .	315
П. 5. Требования безопасности . . . . .	316
П. 5.1. Функциональные требования . . . . .	316
П. 5.2. Требования доверия к безопасности . . . . .	324
П. 6. Обоснование . . . . .	330
П. 6.1. Логическое обоснование целей безопасности . . . . .	331
П. 6.2. Обоснование требований безопасности . . . . .	335
П. 6.3. Обоснование удовлетворения всем зависимостям . . . . .	339
<b>ЛИТЕРАТУРА</b> . . . . .	340
<b>ОБ АВТОРЕ</b> . . . . .	359