

Оглавление

Введение.....	13
От издательства.....	13
Часть I. Введение в инсайдерские угрозы	14
Глава 1. Экосистема внутренних нарушителей.....	15
Суть проблемы.....	16
Классификация инсайдеров.....	17
Итоги	22
Глава 2. Классификация инсайдерских угроз	23
Угроза утечки конфиденциальной информации	24
Обход средств защиты от утечки конфиденциальной информации.....	24
Кража конфиденциальной информации по неосторожности	25
Нарушение авторских прав на информацию.....	25
Мошенничество	26
Нецелевое использование информационных ресурсов компании....	26
Саботаж ИТ-инфраструктуры.....	26
Рейтинг опасности инсайдерских угроз	27
Итоги	29
Глава 3. Самые громкие инсайдерские инциденты	30
Утечка интеллектуальной собственности из Lockheed Martin	33
Утечка из Министерства по делам ветеранов США	34
Саботаж в UBS PaineWebber	34
Кража клиентской базы японского сотового оператора KDDI.....	35
Инсайдеры в крупнейшем британском банке HSBC	36
База данных потребительских кредитов российских банков	36
ИИИ	
<u>Оглавление</u>	
База данных неблагонадежных заемщиков банка «Первое ОБК»....	37
Утечка базы данных белорусского сотового оператора Velcom	37
Утечка из сингапурского филиала Citibank.....	38

Утечка интеллектуальной собственности из Acme Tele Power.....	38
Итоги	39
Часть II. Нормативная совместимость	40
Глава 4. Нормативные акты корпоративного управления	41
Глава 5. Федеральный закон «О персональных данных»	44
Основные положения	47
Требования к безопасности персональных данных	49
Ответственность за нарушения закона	50
Критические даты.....	50
Итоги	51
Глава 6. Стандарт Банка России по ИБ	53
Общие сведения	54
Основные положения	55
Стимулы к внедрению стандарта	57
Обязательность стандарта	60
Итоги	61
Глава 7. Соглашение Basel II	62
Основные положения	63
Три столпа Basel II.....	64
Структура операционных рисков в рамках Basel II	65
Связь Basel II со стандартом Банка России по И Б	66
Методология измерения операционных рисков	67
Влияние Basel II на конкурентоспособность банка	69
Репутационные риски в рамках Basel II	71
Итоги	72
Глава 8. Корпоративное управление	73
Современное корпоративное управление	74
От корпоративного управления к внутреннему контролю	75

Нормативные акты корпоративного управления.....	76
Стимулы к внедрению нормативного акта корпоративного управления	78
Требования к внутреннему контролю	81
Итоги	85
Глава 9. Кодекс корпоративного поведения ФСФР.....	86
Корпоративное управление и внутренний контроль	87
Основные положения.....	89
Принцип внутреннего контроля	90
Обязательный характер Кодекса ФСФР	91
Важность Кодекса ФСФР для российского бизнеса.....	91
Итоги	93
Глава 10. Американский закон SOX	94
Анализ требований закона SOX.....	96
Основные положения закона SOX	97
Анализ требований к системе внутреннего контроля	100
Итоги	101
Часть III. Проблема утечки конфиденциальной информации.....	103
Глава 11. Аналитический взгляд на проблему утечек	104
Портрет респондентов	105
Угрозы ИБ в России.....	108
Внутренние угрозы ИБ	110
Утечка конфиденциальной информации	112
Нормативное регулирование	115
Средства защиты	116
Открытый вопрос	120
Итоги	120
Глава 12. Методы оценки эффективности в сфере защиты информации от утечек	122
Ключевые выводы исследования.....	123
Какие отрасли страдают от утечек.....	124

Масштаб и структура убытков	125
Последствия утечек.....	127
Расходы шаг за шагом	129
Итоги	131
Глава 13. Организационные меры защиты.....	133
Проблема организационных мер.....	134
Собственно организационные меры	135
Психологические меры	135
Права локальных пользователей.....	136
Стандартизация ПО	136
Специфические решения.....	137
Работа с кадрами	137
Внутрикорпоративная нормативная база	138
Хранение физических носителей.....	139
Система мониторинга работы с конфиденциальной информацией... 139	
Аутсорсинг хранения информации.....	140
Итоги	141
Глава 14. Службы обмена мгновенными сообщениями и инсайдеры	142
Общие выводы исследования	143
Отношение пользователей к интернет-пейджерам.....	144
Отношение ИТ-профессионалов к интернет-пейджерам.....	148
Итоги	151
Глава 15. Нелояльные сотрудники. Инсайдеры и компьютерный саботаж.....	153
Введение в понятие «корпоративный саботаж»	154
Последствия корпоративных диверсий.....	155
Портрет типичного саботажника	158
Что не так с ребятами из ИТ	160
Деструктивная активность саботажников	160
Как выявить диверсанта	161
Итоги	* 163

Глава 16. Управление изменениями в ИТ-инфраструктуре.....	165
Служба ИБ в структуре современной организации	167
Управление ИТ-изменениями в современной организации	169
Итоги.....	172
Часть IV. Выбор средства защиты	174
Глава 17. Многоуровневый подход к защите от утечек.....	175
Введение в защиту от утечек.....	176
Законодательные факторы, стимулирующие развитие ILD&P	177
Технологические факторы, стимулирующие развитие ILD&P	179
Рост использования интернет-пейджинга и пиринга в корпоративной среде.....	180
Крупные утечки конфиденциальных данных.....	180
Решения в сфере ILD&P.....	181
Итоги.....	184
Глава 18. Новая парадигма внутренней ИТ-безопасности	186
Каналы утечки	187
Уровни контроля.....	188
Режимы защиты.....	190
Канальная защита	190
Периметральная парадигма	192
Канальная защита против периметральной	192
Итоги.....	194
Глава 19. Средства защиты	196
Системы выявления и предотвращения утечек	197
Средства внутреннего контроля	199
Системы сильной аутентификации (ЗА)	201
Предотвращение нецелевого использования ИТ-ресурсов.....	203
Архивирование корпоративной корреспонденции.....	204
Итоги.....	205

Глава 20. Выбор программного средства защиты	206
Authentica ARM Platform	207
InfoWatch Enterprise Solution	209
«Дозор-Джет».....	211
Onigma Platform.....	213
PC Acme	214
Digital Guardian.....	215
Итоги.....	217
Глава 21. Выбор программно-аппаратного средства защиты	219
Компания InfoWatch.....	221
Компания Tizor.....	224
Компания Proofpoint	225
Компания Tablus	226
Компания Hackstrike	227
Компания Oakley Networks	228
Итоги.....	229
Глава 22. Защита от утечек через сменные носители	230
Zami MAS.....	231
Advanced Systems International USB Lock.....	233
InfoWatch Net Monitor и Device Monitor.....	235
SecurITZlock	238
SmartLine DeviceLock.....	239
Итоги.....	241
Часть V. Проблемы на пути внедрения защиты от утечек	243
Глава 23. Юридические аспекты	244
Постановка проблемы.....	245
Внешние угрозы.....	247
Внутренние угрозы	247
Итоги.....	249

Оглавление	
Глава 24. Трудности контентной фильтрации	251
«Дозор» и «Дозор-Джет»	253
Clearswift MIMESweeper	253
InfoWatch Enterprise Solution	255
Symantec Gateway Security	256
Сравнение функциональности продуктов	256
Сравнение архитектуры решений	259
Архивирование почты	260
Итоги	261
Глава 25. Проблемы корпоративного управления правами (ERM)	263
Microsoft RMS	264
InfoWatch Enterprise Solution	268
Сравнительный анализ	273
Итоги	274
Часть VI. Архивирование электронной корреспонденции	276
Глава 26. Нормативные акты в сфере архивирования почты	277
Соглашение Basel II	280
Стандарт ИБ от Центробанка	280
ФЗ «Об архивном деле в Российской Федерации»	281
Директива Евросоюза о сохранении данных	282
Закон SOX	282
Правила Комиссии по ценным бумагам США	283
Закон HIPAA	283
Итоги	284
Глава 27. Сценарии использования централизованных архивов	285
Расследование инцидентов ИБ	286
Решение проблемы резервного копирования	287

Решение задач бизнеса	287
Итоги	289
Глава 28. «Каменный век» в России	290
Архивирование корреспонденции на практике	291
Стимулы к использованию центральных архивов.....	292
Требования к системам архивирования	295
Архивирование интернет-данных.....	297
Планы российских компаний	298
Итоги	299
Глава 29. Пример: почтовый архив против инсайдера	300
Партнерство InfoWatch и LETA IT-company.....	301
Причины внедрения	302
Последствия внедрения.....	302
Итоги	303
Часть VII. Примеры внедрения.....	305
Глава 30. «ГидроОГК» защищается от утечек	306
До внедрения.....	307
Выбор системы.....	308
Предпроект	309
После внедрения.....	310
Итоги	312
Глава 31. Внешторгбанк защищает конфиденциальную информацию	313
До внедрения.....	314
Выбор решения	315
После внедрения.....	317
Итоги	318