

ЭЛЕКТРОНИКИ

А.И. БЕЛОУС, В.А. СОЛОДУХА

Основы
кибербезопасности.
Стандарты,
концепции, методы
и средства
обеспечения



ТЕХНОСФЕРА

Содержание

Предисловие.....	12
Введение.....	18
Глава 1. Киберпреступность и кибертерроризм.....	23
1.1. Кибертерроризм	23
1.1.1. Кибертерроризм – определение, способы реализации кибертерактов	23
1.1.2. Краткая история кибертерроризма	25
1.1.3. Основные направления кибертерроризма	26
1.1.4. Кибертерроризм как форма гибридной войны	36
1.1.4.1. Кибертерроризм и политический терроризм	36
1.1.4.2. Перспективы кибертерроризма	37
1.2. Киберпреступность	39
1.2.1. Классификация типов киберпреступлений согласно Конвенции Совета Европы	39
1.2.2. Основные виды киберпреступлений, представленные в Конвенции Совета Европы.....	39
1.2.3. Классификация арсенала используемого киберпреступниками «кибероружия»	40
1.2.4. Стандарты кибербезопасности	40
1.3. О возможности международного соглашения об ограничении распространения кибероружия	41
1.4. Особенности организации и функционирования системы киберзащиты НАТО.....	44
1.4.1. Концептуальный подход НАТО к организации киберзащиты.....	44
1.4.2. Кибератаки против НАТО и членов альянса.....	45
1.4.3. Основные оперативные киберструктуры НАТО	45
1.5. Киберпреступления и киберпреступники – классификация, методы «работы» и способы защиты.....	47
1.5.1. Классификация киберпреступников.....	47
1.5.2. Классификация компьютерных преступлений по Интерполу.....	48
1.5.3. Детализированный алгоритм типовой кибератаки.....	50
1.5.4. «Залив денег на карту быстро и без предоплаты» – тонкости профессий заливщика, рефорда и ботовода	54
1.5.5. Пример эффективного расследования киберпреступлений: взлет и падение русскоязычного хакера Fxmsp	59
1.5.5.1. Компания Group-IB – расследование и предотвращение киберпреступлений как важный компонент кибербезопасности	59
1.5.5.2. Аналитический отчет Group-IB «Fxmsp: невидимый бог сети»	60
1.5.6. Легализация бизнеса по разработке шпионских программ как новая угроза кибербезопасности	63

1.5.6.1. Hacking Team – разработка и продажа шпионских программ для государственных организаций.....	63
1.5.6.2. Уникальный эпизод – открытый отчет хакера, взломавшего защиту компании Hacking Team	66
1.5.7. К вопросу о практике «технического симбиоза» кибермошенников и государственных спецслужб	69
1.6. Этичные хакеры и хактивисты – мифы и реалии.....	70
1.6.1. Этичный хакинг – что это такое?	70
1.6.2. Наиболее известные группировки хактивистов.....	73
1.6.3. Манифесты хактивиста Phineas Fisher	75
1.6.4. Этика общечеловеческая и этика хакерская – «почувствуйте разницу!	76
Глава 2. Концепции, методы и средства применения кибероружия.....	85
2.1. Краткая история развития кибероружия.....	85
2.1.1. Основные эпизоды из предыстории развития кибероружия	85
2.1.2. Изменение видов киберугроз за период с 1980 по 2010 г.	91
2.2. Методологические принципы классификации кибероружия.....	94
2.2.1. Введение в проблему, классификация типов кибероружия.....	94
2.2.2. Виды информационных атак	102
2.2.3. Способы внедрения в состав информационных ресурсов противника вредоносных программ	102
2.2.4. Классификация основных видов кибервоздействий	104
2.2.5. Классификация основных видов кибервоздействий	110
2.2.6. Удаленные сетевые атаки как наиболее распространенные типы кибервоздействий	118
2.2.7. Примеры реализации кибервоздействий с использованием метода удаленных сетевых атак	121
2.3. Проблемы идентификации исполнителей и заказчиков кибератак	122
2.3.1. Введение в проблему	122
2.3.2. Зачем нужна идентификация источника кибератаки.....	124
2.3.3. Основные проблемы решения задачи идентификации источника кибератаки	126
2.3.4. Основные индикаторы (признаки), используемые при определении источников кибератак	127
Глава 3. Типовые уязвимости в системах киберзащиты.....	132
3.1. Уязвимости в микросхемах.....	132
3.2. Уязвимости в криптографических алгоритмах (стандартах)	135
3.3. Преднамеренные уязвимости в шифровальном оборудовании	138
3.4. Уязвимости программного обеспечения информационных систем	139
3.4.1. Классификация, термины и определения типовых уязвимостей программного обеспечения	139
Классификация уязвимостей программного обеспечения	141
3.4.2. Риски использования уязвимых программ	143



3.4.3. Уязвимости систем информационной безопасности	172
3.4.4. Переполнение буфера как опасная уязвимость	178
3.5. Уязвимости в автомобилях	185
3.5.1. Из истории автомобильных вирусов	185
3.5.2. Hackable – уязвимости автомобилей для кибератак	186
3.6. Уязвимости бортового оборудования воздушных судов и робототехнических комплексов	190
3.6.1. Уязвимости комплексов с беспилотными летательными аппаратами	190
3.6.2. Функциональные модели построения робототехнических комплексов военного назначения с повышенной киберзащитой	196
3.6.2.1. Основные принципы организации киберзащиты РТК	196
3.6.2.2. Модель угроз безопасности информации и функциональной устойчивости РТК	199
3.6.2.3. Построение модели системы защиты информации и контроля целостности КВС путем идентификации ПАВ на их элементы	202
3.6.3. Концепции обеспечения кибербезопасности бортового оборудования воздушных судов	205
3.6.3.1. Тенденции развития информационной архитектуры воздушных судов	205
3.6.3.2. Инциденты, угрозы и уязвимости безопасности на борту воздушного судна	208
3.6.3.3. Основные направления обеспечения кибербезопасности воздушного судна	211
3.7. Методы выявления программных уязвимостей	217
3.7.1. Виды сертификационных испытаний	217
3.7.2. Виды тестирования безопасности кода	218
3.7.3. Типовая статистика выявления уязвимостей в программном обеспечении	220
3.8. Five-Level Problem – пути снижения уязвимостей критических информационных систем	224
Глава 4. Антивирусные программы и проактивная антивирусная защита	228
4.1. Антивирусные программы	228
4.1.1. Стандартные компоненты антивирусной защиты	229
4.1.2. Основные требования к антивирусным программам	231
4.1.3. Основные характеристики антивирусных программ	232
4.1.4. Классификация и принципы работы антивирусных программ	233
4.1.5. Краткий обзор антивирусных программ	234
4.1.6. Полезные практические рекомендации пользователям от разработчиков антивирусного программного обеспечения	237

4.2. Проактивная антивирусная защита – функции и возможности	239
4.2.1. Поведенческий контроль (Behavior Control)	239
4.2.2. Режимы работы поведенческого контроля	240
4.2.3. Использование песочницы (Sandbox) как изолированной программной среды	241
4.2.4. Потенциально опасные действия и процедуры (Potentially Dangerous Actions and Techniques)	242
4.2.5. Управление компонентами (Component control)	246
4.2.6. Защита переносных мультимедийных устройств (Removable Media Protection)	246
4.2.7. Самозащита (Self-protection)	247
4.3. Иммунный подход к защите информационных систем	247
4.3.1. К проблеме уязвимости операционных систем	247
4.3.2. Цифровые иммунные системы как перспективный инструмент сетевой защиты	249
4.3.3. KasperskyOS – первая российская операционная система с кибериммунитетом	253
4.3.4. Киберфизические иммунные системы	258
4.3.5. Биометрическая система кибербезопасности Darktrace	261
Глава 5. Кибершпионаж, киберразведка и киберконтрразведка	264
5.1. Классификация, способы и объекты кибершпионажа	264
5.1.1. Классификация кибершпионажа	264
5.1.2. Способы осуществления кибершпионажа	265
5.1.3. Объекты кибершпионажа	266
5.1.4. Основные источники угрозы кибершпионажа	266
5.2. Киберразведка и контрразведка: цели, задачи, методы работы	267
5.2.1. Общая информация о киберразведке	267
5.2.2. Стратегическая киберразведка как способ управление рисками	270
5.2.3. Основные цели и задачи киберконтрразведки	272
5.2.4. Специфические требования к новому поколению специалистов по информационной и кибербезопасности	274
5.3. Структура и основные функции главного управления киберразведки США	276
5.4. Ежегодные отчеты управления контрразведки США о киберугрозах	278
5.5. Расследование кибератак как высокоприбыльный бизнес и инструмент политической борьбы	284
5.6. Автоматизация процессов киберразведки с помощью Threat Intelligence Platform	287
5.6.1. Основные этапы алгоритма реализации Threat Intelligence	287
5.6.2. Стандартный цикл процесса киберразведки TI	290
5.6.3. Коммерческие платформы Threat Intelligence	292
5.6.4. Некоммерческие (Open source) Threat Intelligence Platform	300



5.7. Методологические особенности отбора и подготовки специалистов в области киберразведки и киберконтрразведки	303
5.7.1. Состояние и тенденции развития кибервойск.....	303
5.7.2. Методология отбора и подготовки специалистов для противостояния в киберпространстве на примере израильского секретного подразделения 8200	307
5.7.2.1. Подразделение 8200 – история создания, функции и задачи	307
5.7.2.2. Методология отбора и подготовки специалистов для подразделения 8200.....	309
5.7.2.3. Стратегическое международное сотрудничество с Израилем в сфере кибербезопасности	311
5.7.2.4. Особенности израильских кибервойск.....	312
5.7.3. Отечественный специалист по киберразведке – профессия будущего	313
Глава 6. Особенности обеспечения кибербезопасности конечных точек инфраструктурных систем	316
6.1. Тенденции развития киберугроз, направленных на конечные точки инфраструктурных систем.....	316
6.2. Тенденция роста бесфайловых (fileless) атак	320
6.3. Рост ущерба от атак на конечные точки	321
6.4. Мировой рынок EDR-решений	322
6.5. Основные платформы Endpoint Detection and Response.....	324
6.5.1. Gartner	324
6.5.2. Платформы Forrester	326
6.5.3. Платформа The Radicati Group	328
Глава 7. Основные направления обеспечения кибербезопасности	331
7.1. Базовые термины и определения кибербезопасности	332
7.2. Редтайминг и блютайминг – «красные», «голубые» и другие «разноцветные» команды	333
7.2.1. Введение в проблему	333
7.2.2. Концепции и сценарии «цветного противостояния»	335
7.2.3. Имитация целевых атак как оценка безопасности. Кимеручения в формате Red Teaming.....	339
7.3. Охота за угрозами как «проактивный метод» киберзащиты.....	345
7.3.1. Общая характеристика подхода ThreatHunting	345
7.3.2. Основные игроки на рынке Threat Hunting.....	349
7.3.3. Стандартные инструменты для организации проактивного поиска.....	351
7.4. База знаний MITRE ATT&CK	355
7.4.1. Парадигма построения базы знаний ATT&CK. Введение в проблему.....	355
7.4.2. Краткое описание проектов, использующих MITRE ATT&CK.....	360



7.5. SIEM как важный элемент в архитектуре киберзащиты	366
7.5.1. Основные цели и задачи SIEM	366
7.5.2. Корреляция как процесс сопоставления событий и логов.....	368
7.5.3. Дополнительные функции SIEM	372
7.5.4. Сравнительный анализ характеристик наиболее популярных SIEM-систем	375
7.5.4.1. Методологические принципы сравнительного анализа	375
7.6. Магический квадрант Gartner – что это такое?	378
Глава 8. Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	383
8.1. Тенденции развития и особенности цифровизации промышленных инфраструктур	383
8.1.1. Особенности цифрового управления промышленными инфраструктурами	383
8.1.2. Основные угрозы безопасности цифрового производства.....	386
8.1.3. Эволюция парадигмы информационной безопасности производства	388
8.1.4. Основные уязвимости промышленных информационно- коммуникационных систем.....	389
8.2. Оценка рисков безопасности в энергетических системах	393
8.2.1. Киберугрозы и промышленные информационно- коммуникационные технологии	393
8.2.2. Сбор и обработка информации	395
8.2.3. Оценка рисков	395
8.2.4. Принятие решений и реализация действий	396
8.2.5. Типовые сценарии процесса анализа рисков для электроэнергетической системы	396
8.2.5.1. Сбор и обработка информации.....	396
8.2.5.2. Оценка рисков в электроэнергетической отрасли	398
8.3. Стандарты и методы обеспечения кибербезопасности электроэнергетических инфраструктур	405
8.3.1. Стандарты безопасности – общие критерии и подходы	405
8.3.2. Стандарты американского общества приборостроителей (ISA)	410
8.3.3. Стандарты международной организации по стандартизации (ISO)	411
8.3.4. Стандарты национального института стандартов и технологий (NIST)	413
8.3.4.1. Специальные публикации NIST 800.....	413
8.3.4.2. Руководство по обеспечению безопасности промышленных систем управления (ICS) (NIST 800-82)	413
8.3.4.3. Руководство по управлению рисками для ИТ-систем (NIST 800-30)	414



8.3.4.4. Руководство по обработке инцидентов в сфере компьютерной безопасности (NIST 800-61)	415
8.3.5. Стандарты Североамериканской корпорации по надежности электроснабжения (NERC)	416
8.3.6. Подходы к обеспечению кибербезопасности в Англии.....	420
8.3.7. Концептуальные подходы к обеспечению кибербезопасности в Нидерландах	425
8.3.7.1. Национальный консультативный центр по критическим инфраструктурам (NAVI).....	425
8.3.7.2. Стратегия национальной безопасности Нидерландов.....	426
8.3.7.3. Руководство по методике оценки национальных рисков (NRA).....	427
8.4. Концепции, методы и формы обеспечения защиты секретной информации в критических инфраструктурах США.....	431
8.4.1. Общие принципы построения системы защиты секретной информации	431
8.4.2. Особенности организации процедуры допуска к секретной информации руководителей организаций-подрядчиков.....	433
8.4.3. Особенности проведения процедуры собеседования с руководителями подрядчиков	434
8.4.4. Процедура оформления допуска персонала к секретным документам.....	435
8.4.5. Срок действия допуска к секретной работе	436
8.4.6. Особенности организации процедур проверок (аудитов) подрядчиков	436
8.4.7. Особенности обучения правилам обеспечения режима секретности	438
8.4.8. Классификационное руководство CG-SS-3	438
8.4.9. Особенности процедуры организации допуска на секретный объект	439
8.4.10. Как и где обеспечивается доступ к секретной информации (специальные зоны).....	440
Глава 9. Кибербезопасные микросхемы как аппаратная база киберзащищенных АСУТП	444
9.1. Термины и определения	444
9.2. От классической «пирамиды производственной безопасности» к «пирамиде кибербезопасности»	445
9.3. Основы проектирования кибербезопасной электронной аппаратуры для АСУТП критических инфраструктур	450
9.3.1. Введение в проблему	450
9.3.2. Анализ кибербезопасности этапов проектирования современных микросхем	454
9.3.3. Потенциальные агенты (организаторы) кибератак с использованием аппаратных троянов в микросхемах	460



9.3.4. Основные методы проектирования кибербезопасной электронной аппаратуры	461
9.4. Использование опыта проектирования безопасного программного обеспечения при проектировании кибербезопасных микросхем	463
9.4.1. Основные различия между разработкой безопасных микросхем и разработкой безопасных программ	463
9.4.2. Особенности обеспечения жизненного цикла разработки безопасного программного обеспечения.....	464
9.4.3. Основные методы безопасного проектирования микросхем для ответственных применений	465
9.4.3.1. Этапы безопасного проектирования микросхем	465
9.4.3.2. Описание моделей угроз.....	466
9.4.3.3. Прослеживаемость в микросхеме	467
9.4.3.4. Цикл обнаружения	468
9.5. Современные технологии контроля безопасности в микроэлектронике	470
9.5.1. Введение в проблему	470
9.5.2. Эволюция классической парадигмы проектирования микросхем ответственного назначения	472
9.5.3. Место и роль технологий контроля безопасности в современной микроэлектронике	473
9.6. Основные алгоритмы (пути) внедрения «зараженных» микросхем в технические объекты вероятного противника.....	476