

Кибербезопасность главные принципы

Обновленные стратегии и тактики

Рик Ховард



Санкт-Петербург • Москва • Минск

2025

Краткое содержание

Об авторе	12
О научных редакторах	13
Благодарности	15
Предисловие. Кто мы такие	18
Введение	20
От издательства	27
Глава 01. Базовые принципы	28
Глава 02. Стратегии	54
Глава 03. Нулевое доверие	67
Глава 04. Предотвращение реализации убийственной цепочки вторжения (kill chain)	120
Глава 05. Обеспечение устойчивости	188
Глава 06. Прогнозирование рисков	230
Глава 07. Автоматизация	272
Глава 08. Подведение итогов	298
Рекомендованная литература	305

Оглавление

Об авторе	12
О научных редакторах	13
Благодарности	15
Предисловие. Кто мы такие	18
Введение	20
Для кого предназначена книга	20
О чем пойдет речь	22
Значения используемых терминов	23
Кибербезопасность	23
Профессионалы в области кибербезопасности	23
Организации	23
Проект Cybersecurity Canon Project	24
Сайт книги	24
Дорожная карта	25
От издательства	27
Глава 01. Базовые принципы	28
Обзор главы	28
Что такое базовые принципы	29
Предыдущие исследования базовых принципов кибербезопасности	32
Атомарный базовый принцип кибербезопасности	37
Является ли триада КЦД абсолютным первичным принципом?	39
Является ли патчинг абсолютным базовым принципом?	41
Является ли защита от вредоносного ПО абсолютным первичным принципом?	43
Является ли реагирование на инциденты абсолютным первичным принципом?	44
Является ли соблюдение правил фреймворков безопасности абсолютным первичным принципом?	45
Является ли соблюдение нормативных требований абсолютным первичным принципом?	48
Атомарный первичный принцип кибербезопасности	49
Заключение	52

Глава 02. Стратегии	54
Обзор главы	54
Разница между стратегиями и тактиками	55
Основные стратегии реализации программы защиты информации, базирующейся на первичном принципе	56
Обзор стратегии нулевого доверия	57
Обзор стратегии предотвращения реализации убийственной цепочки вторжения	60
Обзор стратегии обеспечения устойчивости	62
Обзор стратегии прогнозирования рисков	63
Обзор стратегии автоматизации	65
Заключение	66
Глава 03. Нулевое доверие	67
Обзор главы	67
Актуальность стратегии нулевого доверия: случай с Эдвардом Сноуденом ..	68
Концепция нулевого доверия переоценена рынком, но... ..	70
Кибергигиена, эшелонированная защита и защита периметра: нулевое доверие до появления одноименной концепции	72
Рождение концепции нулевого доверия	73
Нулевое доверие — это философия, а не продукт	75
Базовая реализация стратегии нулевого доверия	77
Логическая и микросегментация	78
Управление уязвимостями: тактика нулевого доверия	79
Управление уязвимостями как разведывательная задача	82
Использование спецификаций программного обеспечения: тактика нулевого доверия	85
Сходство автомобильного производства с методологией DevOps	86
Коммерческое ПО — это ПО с открытым исходным кодом	87
Цепочка поставок ПО и первичные принципы кибербезопасности	87
Актуальные стандарты SBOM	89
Директива президента	90
Три инструмента для снижения рисков, связанных с цепочкой поставок ..	90
Светлое будущее SBOM	91
Управление идентификацией: тактика нулевого доверия	92
Компоненты IAM: IGA, PIM и PAM	98
Единый вход: тактика нулевого доверия	99
Процесс OAuth	100
Процесс SAML	102
Двухфакторная аутентификация: тактика нулевого доверия	104
Виды двухфакторной аутентификации	105
Насколько безопасна двухфакторная аутентификация	107
Будущее двухфакторной аутентификации	109

Программно-определяемый периметр: тактика нулевого доверия	110
Программно-определяемый периметр становится новой моделью.	112
Причины провала проектов с нулевым доверием	115
Заключение	118
Глава 04. Предотвращение реализации убийственной цепочки вторжения (kill chain)	120
Обзор главы	121
Зарождение новой идеи	121
Документ компании Lockheed Martin, посвященный концепции убийственной цепочки	122
Модель убийственной цепочки.	124
Мотивация противника: преобразование кибервойны в низкоуровневый киберконфликт	127
Убийственная цепочка Lockheed Martin — это здорово, но...	129
Модели убийственной цепочки.	130
Фреймворк MITRE ATT&CK	131
Модель Diamond Министерства обороны США	134
Некоторые соображения по поводу атрибуции	137
Количество плейбуков активных противников	140
Три кита киберразведки: концепция убийственной цепочки, база знаний ATT&CK и модель Diamond	141
Развертывание SOC-центров: тактика предотвращения реализации убийственной цепочки вторжения	142
Оркестрация стека безопасности: тактика предотвращения реализации убийственной цепочки вторжения	148
Операции киберразведки как путешествие	170
Операции «красной»/«синей»/«фиолетовой» команды: тактика предотвращения реализации убийственной цепочки вторжения	171
Обмен разведданными: тактика предотвращения реализации убийственной цепочки вторжения	175
Заключение	186
Глава 05. Обеспечение устойчивости	188
Обзор главы	188
Что такое устойчивость	189
Примеры устойчивости	190
ИТ-устойчивость и ИБ-устойчивость	192
Устойчивость и планы по ее обеспечению	192
Выпас котов: матрицы распределения ответственности	196
Как следует задуматься об устойчивости	200
Антикризисное управление: тактика обеспечения устойчивости	201
RSA Security: пример антикризисных коммуникаций	202
Equifax: пример антикризисных коммуникаций	204

Ожидаемые результаты	206
Руководители — занятые люди: используйте их время эффективно	207
Резервное копирование: тактика обеспечения устойчивости	209
Резервное копирование как стратегия защиты от программ-вымогателей	211
Вариант 1. Платформы для централизованного резервного копирования содержимого всех островов данных	214
Вариант 2. Децентрализованные системы для однократного резервного копирования	214
Вариант 3. DevOps (DevSecOps) для каждого приложения	215
Как попасть в Карнеги-холл? Надо практиковаться!	216
Шифрование: тактика обеспечения устойчивости	216
Данные в состоянии покоя и данные в движении	218
Тактика шифрования, основанная на базовом принципе кибербезопасности, является рекурсивной	220
Реагирование на инциденты: тактика обеспечения устойчивости	222
Руководства NIST по обеспечению кибербезопасности и реагированию на инциденты	225
Техническая сторона реагирования на инциденты	226
Заключение	229
Глава 06. Прогнозирование рисков	230
Обзор главы	230
Суперпрогнозирование, оценки Ферми и «черные лебеди»	232
Сверхспособности суперпрогнозиста	234
Люди не думают в терминах вероятности, но им следует это делать	235
Скрывается ли Усама бен Ладен в бункере?	236
Оценки Ферми являются достаточно хорошими	238
«Черные лебеди» и устойчивость	239
Изменение мнения	241
Правило Байеса: еще один способ размышления о рисках кибербезопасности	243
Теорема Байеса	243
Использование байесовского подхода для победы над немцами во Второй мировой войне	247
Применение теоремы Байеса для прогнозирования рисков кибербезопасности	252
Практический пример прогнозирования рисков с помощью теоремы Байеса	253
Минутку, а что насчет меня?	258
Как учитывать новые данные	262
Анализ по схеме «изнутри наружу»: первичные принципы	264
Анализ по схеме «изнутри наружу»: корпорация Contoso	265

Анализ по схеме «изнутри наружу»: стратегии, основанные на базовом принципе кибербезопасности.	267
Что теперь? Укладывается ли уровень риска в допустимый диапазон? . . .	269
Заключение	271
Глава 07. Автоматизация.	272
Обзор главы	272
Важность автоматизации системы безопасности	273
Ранняя история развития философий разработки программного обеспечения	274
Agile бросает вызов	276
Когда мы задумались о безопасности?	276
Разработка инфраструктуры.	277
DevSecOps: важнейшая тактика автоматизации	279
Что случилось с ИБ-сообществом	280
DevSecOps движется в верном направлении.	281
DevSecOps как стратегия, основанная на базовом принципе кибербезопасности	282
Напоследок об автоматизации как стратегии	283
Обеспечение соответствия нормативным требованиям: тактика, базирующаяся на первичном принципе кибербезопасности и пронизывающая все стратегии	284
Индустрия комплаенса	285
Две комплаенс-категории: разрешения и штрафы	286
Вероятность существенного ущерба в результате несоблюдения нормативных требований.	287
Является ли соблюдение нормативных требований тактикой, основанной на базовом принципе кибербезопасности?	290
Хаос-инженерия для автоматизации и обеспечения устойчивости	291
История развития хаос-инженерии.	293
Какое отношение хаос-инженерия имеет к автоматизации и обеспечению устойчивости	294
Заключение	296
Глава 08. Подведение итогов	298
Обзор главы	298
Нулевое доверие	301
Предотвращение реализации убийственной цепочки вторжения.	302
Обеспечение устойчивости	302
Прогнозирование рисков	303
Автоматизация.	303
Заключение	304
Рекомендованная литература	305