
Безопасные и надежные СИСТЕМЫ

*Лучшие практики проектирования, внедрения
и обслуживания как в Google*

*Хизер Адкинс, Бетси Бейер, Пол Бланкиншип,
Петр Левандовски, Ана Опра, Адам Стабблфилд*



Санкт-Петербург • Москва • Минск

2025

Выпущено
при поддержке

КРОК

Краткое содержание

Отзывы о книге.....	19
Предисловие Рояла Хансена.....	22
Предисловие Майкла Вайлданера	25
Введение	27

ЧАСТЬ I. ВВОДНЫЕ МАТЕРИАЛЫ

Глава 1. Пересечение безопасности и надежности	38
Глава 2. Виды злоумышленников.....	51

ЧАСТЬ II. ПРОЕКТИРОВАНИЕ СИСТЕМ

Глава 3. Пример из практики: безопасные прокси.....	77
Глава 4. Компромиссные решения при проектировании	83
Глава 5. Принцип наименьших привилегий при проектировании.....	102
Глава 6. Проектирование для понятности.....	136
Глава 7. Проектирование для меняющегося ландшафта.....	172
Глава 8. Проектирование для устойчивости	197
Глава 9. Проектирование для восстановления.....	242
Глава 10. Защита от DoS-атак.....	281

ЧАСТЬ III. ВНЕДРЕНИЕ СИСТЕМ

Глава 11. Пример: проектирование, разработка и поддержка публично доверенного центра сертификации.....	296
Глава 12. Написание кода.....	306
Глава 13. Тестирование	335
Глава 14. Развертывание.....	370
Глава 15. Исследование систем.....	402

ЧАСТЬ IV. ОБСЛУЖИВАНИЕ СИСТЕМ

Глава 16. Планирование аварийных ситуаций.....	435
Глава 17. Антикризисное управление	461
Глава 18. Восстановление и последствия.....	494

ЧАСТЬ V. ОРГАНИЗАЦИЯ И КУЛЬТУРА

Глава 19. Пример из практики: команда безопасности Chrome	524
Глава 20. Понимание ролей и обязанностей.....	535
Глава 21. Формирование культуры безопасности и надежности	554
Заключение.....	583
Приложение. Матрица оценки риска бедствий.....	585
Об авторах.....	588
Иллюстрация на обложке.....	590

Оглавление

Отзывы о книге.....	19
Предисловие Рояла Хансена.....	22
Предисловие Майкла Вайлдпанера.....	25
Введение.....	27
Почему мы написали эту книгу.....	27
Для кого предназначена эта книга.....	28
Примечание о культуре.....	29
Как читать эту книгу.....	29
Условные обозначения, используемые в книге.....	30
Благодарности.....	31
От издательства.....	36
О научном редакторе русскоязычного издания.....	36

ЧАСТЬ I. ВВОДНЫЕ МАТЕРИАЛЫ

Глава 1. Пересечение безопасности и надежности.....	38
О паролях и перфораторах.....	38
Надежность и безопасность: соображения проектирования.....	40
Конфиденциальность, целостность, доступность.....	41
Конфиденциальность.....	41
Целостность.....	41
Доступность.....	42
Надежность и безопасность: общие черты.....	43
Незаметность.....	43
Оценка.....	44
Простота.....	44
Эволюция.....	44
Устойчивость.....	45
От проектирования до использования.....	47
Исследование систем и ведение журналов.....	47

Антикризисное реагирование	48
Восстановление.....	49
Резюме.....	50
Глава 2. Виды злоумышленников.....	51
Мотивация атакующего	52
Профили злоумышленников.....	54
Любители.....	54
Исследователи уязвимостей.....	55
Правительства и правоохранительные органы.....	55
Преступники	60
Автоматизация и искусственный интеллект.....	62
Инсайдеры.....	62
Методы атакующего.....	69
Анализ угроз.....	69
Cyber Kill Chains™.....	70
Тактика, методы и процедуры.....	71
Оценка риска.....	72
Резюме.....	73

ЧАСТЬ II. ПРОЕКТИРОВАНИЕ СИСТЕМ

Глава 3. Пример из практики: безопасные прокси.....	77
Безопасные прокси в производственных средах.....	77
Tool Proxu в Google.....	80
Резюме.....	82
Глава 4. Компромиссные решения при проектировании.....	83
Цели и требования при проектировании.....	84
Функциональные требования.....	84
Нефункциональные требования.....	85
Характеристики в сравнении с эмерджентными свойствами.....	86
Пример: документ о дизайне в Google.....	88
Балансировка требований.....	89
Пример: обработка платежей.....	90
Управление противоречиями и согласование целей.....	95
Пример: микросервисы и фреймворк веб-приложений Google.....	95
Согласование требований к эмерджентным свойствам.....	97

Начальная скорость по сравнению с установившейся скоростью.....	98
Резюме.....	101
Глава 5. Принцип наименьших привилегий при проектировании.....	102
Концепции и терминология.....	103
Наименьшая привилегия.....	103
Сеть с нулевым доверием.....	103
Zero Touch.....	104
Классификация доступа на основе риска.....	104
Лучшие практики.....	106
Небольшие функциональные API.....	106
Механизм аварийного доступа.....	109
Аудит.....	110
Тестирование и минимальные привилегии.....	113
Диагностика отказа в доступе.....	116
Механизмы постепенного отказа и аварийного доступа.....	117
Пример из практики: распределение конфигурации.....	118
POSIX API через OpenSSH.....	119
API обновления ПО.....	120
Пользовательский параметр ForceCommand для OpenSSH.....	120
Пользовательский HTTP-получатель (расширенный).....	121
Пользовательский HTTP-получатель (внутрипроцессный).....	121
Компромиссы.....	121
Структура политик для решений аутентификации и авторизации.....	122
Использование расширенных средств контроля авторизации.....	124
Вложение в широко используемый фреймворк авторизации.....	125
Избегание потенциальных ловушек.....	125
Расширенные средства контроля.....	126
Многосторонняя авторизация (MPA).....	126
Трехфакторная авторизация (3FA).....	127
Бизнес-обоснования.....	130
Временный доступ.....	130
Прокси.....	131
Компромиссы и противоречия.....	132
Повышенная сложность безопасности.....	132
Влияние на сотрудничество и корпоративную культуру.....	132
Качественные данные и системы, влияющие на безопасность.....	132

Влияние на производительность пользователей	133
Влияние на сложность для разработчиков	133
Резюме	134
Глава 6. Проектирование для понятности.....	136
Почему понятность важна?	137
Инварианты системы	138
Анализ инвариантов	139
Ментальные модели.....	140
Проектирование понятных систем.....	142
Сложность и понятность.....	142
Разрушение сложности.....	143
Централизованная ответственность за требования безопасности и надежности.....	144
Архитектура системы	145
Понятные спецификации интерфейса.....	146
Понятные идентификационные данные, аутентификация и контроль доступа.....	149
Границы безопасности.....	155
Проектирование программного обеспечения.....	162
Использование фреймворков приложений для общих требований к сервису.....	162
Понимание сложных потоков данных	163
Рассматриваем удобство использования API.....	167
Резюме	170
Глава 7. Проектирование для меняющегося ландшафта.....	172
Типы изменений безопасности.....	173
Проектирование ваших изменений	173
Архитектурные решения для простых изменений.....	175
Постоянно обновляйте зависимости и регулярно пересобирайте код	175
Частые выпуски с использованием автоматизированного тестирования.....	175
Использование контейнеров.....	176
Использование микросервисов	177
Разные изменения: разные скорости, разные сроки.....	180
Краткосрочное изменение: уязвимость нулевого дня	181
Среднесрочные изменения: улучшение состояния безопасности	185
Долгосрочные изменения: внешнее требование.....	189

Сложности: когда планы меняются	193
Пример: растущая область действия — Heartbleed	194
Резюме	196
Глава 8. Проектирование для устойчивости	197
Принципы проектирования для устойчивости	198
Защита в глубину	199
Троянский конь	199
Анализ Google App Engine	201
Управление деградацией	205
Разделение затрат на сбои	207
Развертывание механизмов реагирования	209
Автоматизируйте ответственно	213
Управление радиусом взлома	215
Разделение по ролям	218
Разделение по местоположению	218
Разделение по времени	223
Области отказов и избыточность	223
Области отказов	224
Типы компонентов	227
Контроль избыточности	230
Непрерывная проверка	232
Основные направления проверки	234
Проверка на практике	235
Практические советы: с чего начать	239
Резюме	241
Глава 9. Проектирование для восстановления	242
От чего мы восстанавливаемся?	243
Случайные ошибки	243
Непреднамеренные ошибки	244
Ошибки программного обеспечения	245
Вредоносные действия	245
Принципы проектирования для восстановления	246
Проектирование должно быть максимально быстрым (в соответствии с политикой)	246
Ограничение зависимости от внешних представлений о времени	251
Откаты — компромисс между безопасностью и надежностью	253
Минимально допустимые номера версий безопасности	257
Использование явного механизма отката	263

Знайте свое предполагаемое состояние, вплоть до байтов.....	267
Проектирование для тестирования и непрерывной проверки.....	274
Экстренный доступ.....	275
Контроль доступа.....	276
Связь.....	277
Привычки респондентов.....	278
Неожиданные преимущества.....	279
Резюме.....	280
Глава 10. Защита от DoS-атак.....	281
Стратегии атаки и защиты.....	282
Стратегия атакующего.....	282
Стратегия защитника.....	283
Проектирование для защиты.....	284
Защищаемая архитектура.....	284
Защищаемые сервисы.....	286
Предотвращение атак.....	287
Мониторинг и оповещение.....	287
Постепенная деградация.....	288
Система защиты от DoS.....	288
Стратегический ответ.....	290
Борьба с внутренними атаками.....	291
Поведение пользователя.....	291
Поведение клиента при повторных попытках.....	293
Резюме.....	293

ЧАСТЬ III. ВНЕДРЕНИЕ СИСТЕМ

Глава 11. Пример: проектирование, разработка и поддержка публично доверенного центра сертификации.....	296
Общие сведения о публично доверенных центрах сертификации.....	296
Зачем нам нужен доверенный ЦС.....	298
Создать или купить?.....	298
Вопросы проектирования, реализации и обслуживания.....	299
Выбор языка программирования.....	300
Сложность в сравнении с понятностью.....	301
Защита сторонних компонентов и компонентов с открытым исходным кодом.....	302

Тестирование.....	303
Устойчивость набора ключей ЦС	304
Проверка данных	304
Резюме.....	305
Глава 12. Написание кода.....	306
Основы обеспечения безопасности и надежности.....	307
Преимущества использования фреймворков	308
Пример: фреймворк для серверов RPC	310
Распространенные уязвимости безопасности.....	314
Уязвимости SQL-внедрений: TrustedSqlString.....	316
Предотвращение XSS: SafeHtml	318
Уроки оценки и создания фреймворков	320
Простые, безопасные, надежные библиотеки для общих задач	321
Стратегия внедрения	322
Простота — залог безопасного и надежного кода	324
Избегайте многоуровневого вложения	324
Устранение «запахов» YAGNI.....	325
Погашение технического долга	326
Рефакторинг.....	327
Безопасность и надежность по умолчанию.....	328
Выберите правильные инструменты.....	328
Использование строгих типов	330
Очистка кода.....	333
Резюме.....	334
Глава 13. Тестирование	335
Модульное тестирование.....	336
Написание эффективных модульных тестов	337
Когда писать модульные тесты	337
Как модульное тестирование влияет на код	339
Интеграционное тестирование	340
Написание эффективных интеграционных тестов.....	341
Динамический анализ программ.....	342
Нечеткое тестирование	345
Как работают механизмы фаззинга	347
Написание эффективных драйверов фаззинга	351
Пример фаззера	352
Непрерывное нечеткое тестирование	356

Статический анализ программ.....	357
Инструменты автоматической проверки кода	359
Интеграция статического анализа в рабочий процесс.....	364
Абстрактная интерпретация	366
Формальные методы.....	368
Резюме.....	369
Глава 14. Развертывание.....	370
Концепции и терминология	371
Модель угроз.....	373
Лучшие практики.....	375
Сделайте рецензирование обязательным.....	375
Автоматизируйте	376
Проверяйте не только людей, но и артефакты	377
Относитесь к настройкам как к коду	378
Защита в соответствии с моделью угроз	380
Расширенные стратегии смягчения угроз	382
Бинарное происхождение	383
Что указывать в бинарном происхождении	383
Политики развертывания на основе происхождения	386
Верифицируемые сборки	388
Пункты контроля развертывания	394
Проверки после развертывания	396
Практические советы	397
Двигайтесь небольшими шагами	397
Предоставьте информативные сообщения об ошибках	397
Убедитесь в однозначности происхождения.....	398
Создавайте однозначные политики.....	399
Добавьте механизм аварийного доступа при развертывании.....	399
Пересмотр защиты в соответствии с моделью угроз	400
Резюме	400
Глава 15. Исследование систем.....	402
От отладки до исследования.....	403
Пример: временные файлы	403
Методы отладки	405
Что делать, если вы зашли в тупик	414
Совместная отладка: способ обучения	419
Чем отличаются исследования безопасности от отладки	420

Сбор подходящих и полезных записей журналов	422
Сделайте журналы неизменяемыми	422
Примите во внимание конфиденциальность	423
Определите, какие журналы безопасности нужно сохранить	424
Бюджет на ведение журнала	429
Надежный и безопасный доступ при отладке	430
Надежность	430
Безопасность	431
Резюме.....	432

ЧАСТЬ IV. ОБСЛУЖИВАНИЕ СИСТЕМ

Глава 16. Планирование аварийных ситуаций.....	435
Определение «бедствия».....	436
Стратегии динамического реагирования на бедствия	436
Анализ риска катастроф.....	438
Создание команды реагирования на происшествия	439
Определение членов команды и их ролей.....	439
Создание устава команды	441
Создание моделей серьезности и приоритетов	442
Определите рабочие параметры для привлечения IR-команды.....	443
Разработка планов реагирования	444
Создание подробных инструкций	446
Убедитесь в наличии механизмов доступа и обновления	446
Предварительная подготовка людей и систем.....	447
Настройка систем.....	447
Обучение	448
Процессы и процедуры	450
Тестирование систем и планов реагирования	450
Аудит автоматизированных систем	451
Проведение ненавязчивых настольных упражнений.....	452
Тестирование реагирования в производственных средах.....	454
Тестирование красных команд	456
Оценка ответов.....	457
Примеры из опыта Google	458
Тест с глобальным воздействием.....	458
Тестирование DiRT при экстренном доступе	459
Отраслевые уязвимости.....	459
Резюме.....	460

Глава 17. Антикризисное управление	461
Это кризис или нет?	462
Сортировка инцидента	463
Компрометации и ошибки	465
Управление инцидентом	466
Первый шаг: не паникуйте!	466
Начинаем реагировать	467
Создаем команды по реагированию на инцидент	468
Операционная безопасность	470
Жертвуем хорошим OpSec для большего блага	472
Процесс расследования	473
Сохранение контроля над инцидентом	477
Распараллеливание действий	477
Передача обязанностей	479
Командный дух	482
Коммуникация	483
Недопонимание	483
Уклонение от ответа	484
Встречи	484
Информирование нужных людей с правильными уровнями детализации	486
Объединяем все вместе	488
Сортировка инцидента	488
Объявление о происшествии	488
Коммуникация и операционная безопасность	488
Начало инцидента	489
Передача обязанностей	490
Обратная передача обязанностей	490
Информирование пользователей и исправление	491
Завершение реагирования	492
Резюме	493
Глава 18. Восстановление и последствия	494
Логистика восстановления	496
Сроки восстановления	498
Планирование восстановления	499
Определение объема восстановления	499

Соображения по восстановлению.....	500
Чек-листы восстановления	506
Запуск восстановления.....	507
Изоляция активов (карантин).....	508
Повторная сборка системы и обновление программного обеспечения	509
Очистка данных.....	510
Данные для восстановления.....	511
Учетные данные и замена секретов.....	512
Действия после восстановления	515
Постмортемы.....	516
Примеры.....	517
Скомпрометированные облачные экземпляры	517
Крупномасштабная фишинговая атака.....	519
Целенаправленная атака, требующая сложного восстановления	520
Резюме.....	522

ЧАСТЬ V. ОРГАНИЗАЦИЯ И КУЛЬТУРА

Глава 19. Пример из практики: команда безопасности Chrome	524
Возникновение и развитие команды	524
Безопасность — командная ответственность	528
Помогаем пользователям безопасно перемещаться в Интернете	530
Скорость имеет значение.....	531
Проектирование для защиты в глубину	531
Будьте открыты и вовлекайте сообщество	532
Резюме.....	533
Глава 20. Понимание ролей и обязанностей.....	535
Кто отвечает за безопасность и надежность	536
Роли специалистов	537
Что такое экспертиза в безопасности.....	539
Сертификаты и образование.....	540
Интеграция безопасности в организацию	541
Внедрение специалистов и команд по безопасности.....	544
Пример: внедрение безопасности в Google.....	545
Специальные команды: синие и красные	548
Внешние исследователи.....	551
Резюме.....	553

НАУКОВАЯ БІБЛІОТЕКА

Беларускага нацыянальнага
тэхнічнага ўніверсітэта

1014858

Глава 21. Формирование культуры безопасности и надежности	554
Определение здоровой культуры безопасности и надежности	556
Культура безопасности и надежности по умолчанию	556
Культура рецензирования	557
Культура осведомленности	559
Культура согласия	563
Культура неизбежности	564
Культура рационального использования	566
Изменение культуры с помощью хорошей практики	568
Согласуйте цели проекта и поощрения участников	569
Уменьшайте опасения с помощью механизмов снижения риска	569
Обеспечьте подстраховку	571
Повышайте производительность и удобство использования	572
Поощряйте общение и прозрачность	574
Развивайте эмпатию	575
Убедите руководство	576
Поймите, как принимаются решения	577
Обоснуйте причину для изменения	578
Расставляйте приоритеты	580
Эскалация и решение проблем	581
Резюме	581
Заключение	583
Приложение. Матрица оценки риска бедствий	585
Об авторах	588
Иллюстрация на обложке	590