

УДК 004.42
ББК 32.973
Б43

Б43 Белл Л., Брантон-Сполл М., Смит Р., Бэрд Д.

Безопасность разработки в Agile-проектах. Обеспечение безопасности в конвейере непрерывной поставки / пер. с англ. А. А. Слинкин. – М.: ДМК Пресс, 2018. – 448 с.: ил.

ISBN 978-5-97060-648-3

В большинстве организаций стремительно принимают на вооружение гибкие (agile) методики разработки. Они позволяют своевременно реагировать на изменение условий и значительно снижать стоимость разработки. Однако исторически безопасность и гибкие методики никогда не дружили между собой.

Эта книга поможет вам разобраться в том, что такое безопасность, какие существуют угрозы и на каком языке специалисты-безопасники описывают, что происходит. Вы научитесь моделировать угрозы, измерять степень риска, создавать ПО постоянно помня о безопасности.

Издание будет полезно всем специалистам, в чьи обязанности входит обеспечение информационной и операционной безопасности организаций, разработчикам, применяющие гибкие методы разработки приложений, для которых Scrum и кайдзен не пустые слова.

УДК 004.42
 ББК 32.973

Original English language edition published by O'Reilly Media, Inc. Copyright © 2017 Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. All rights reserved. Russian-language edition copyright © 2017 by DMK Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-1-49193-884-3 (англ.)

© 2017 Laura Bell, Rich Smith, Michael Brunton-Spall, Jim Bird. All rights reserved.

ISBN 978-5-97060-648-3 (рус.)

© Оформление, перевод на русский язык, издание, ДМК Пресс, 2018

Оглавление

Предисловие.....	14
Кому стоит прочитать эту книгу?.....	15
Разработчики, применяющие гибкие методы	15
Специалист по безопасности	16
Специалист по гибким методикам обеспечения безопасности.....	16
О структуре книги	16
Часть 1. Основы	17
Часть 2. Гибкая разработка и безопасность.....	17
Часть 3. Собираем все вместе	17
Графические выделения.....	18
Как с нами связаться	19
Благодарности	19
Глава 1. Начала безопасности.....	21
Не только для технарей.....	24
Безопасность и риск неразделимы.....	24
Уязвимость: вероятность и последствия	24
Все мы уязвимы	25
Не невозможно, просто маловероятно	25
Измерение затрат	26
Риск можно свести к минимуму, но не устранить вовсе	27
Несовершенный мир – трудные решения	27
Знай своего врага	28
Враг найдется у каждого	28
Мотивы, ресурсы, доступ	30
Цели безопасности: защита данных, систем и людей	30
Понимание того, что мы пытаемся защитить.....	30
Конфиденциальность, целостность и доступность.....	30
Неотрицаемость.....	32
Соответствие нормативным требованиям, регулирование и стандарты безопасности.....	32
Типичные заблуждения и ошибки в области безопасности	33
Безопасность абсолютна	33
Безопасность – достижимое состояние	33
Безопасность статична	34
Для безопасности необходимо специальное [вставьте по своему усмотрению: пункт, устройство, бюджет]	34
Начнем, пожалуй	35
Глава 2. Элементы гибких методик.....	36
Сборочный конвейер	36
Автоматизированное тестирование	37

Непрерывная интеграция	41
Инфраструктура как код	42
Управление релизами	44
Визуальное прослеживание	46
Централизованная обратная связь	47
Хороший код – развернутый код	47
Работать быстро и безопасно	48
Глава 3. Революция в методах разработки – присоединяйтесь!	51
Гибкая разработка: взгляд с высоты	51
Scrum, самая популярная из гибких методик	54
Спринты и журналы пожеланий	54
Планерки	56
Циклы обратной связи в Scrum	57
Экстремальное программирование	58
Игра в планирование	58
Заказчик всегда рядом	59
Парное программирование	59
Разработка через тестирование	60
Метафора системы	61
Канбан	61
Канбан-доска: сделать работу видимой	63
Постоянная обратная связь	63
Непрерывное улучшение	64
Бережливая разработка	64
Гибкие методы в целом	66
А как насчет DevOps?	68
Гибкие методики и безопасность	71
Глава 4. Работа с существующим жизненным циклом гибкой разработки	73
Традиционные модели безопасности приложения	73
Ритуалы на каждой итерации	76
Инструменты, встроенные в жизненный цикл	78
Деятельность до начала итераций	79
Инструменты планирования и обнаружения	80
Деятельность после итерации	80
Инструментальные средства в помощь команде	81
Инструменты проверки соответствия нормативным требованиям и аудита	82
Задание контрольного уровня безопасности	82
А что будет при масштабировании?	83
Создание содействующих групп безопасности	83
Создание инструментов, которыми будут пользоваться	84
Методы документирования системы безопасности	85
Сухой остаток	86

Глава 5. Безопасность и требования	87
Учет безопасности в требованиях	87
Гибкие требования: рассказывание историй	89
Как выглядят истории?	89
Условия удовлетворенности	90
Учет историй и управление ими: журнал пожеланий	91
Отношение к дефектам	92
Включение вопросов безопасности в требования	92
Истории, касающиеся безопасности	93
Конфиденциальность, мошенничество, соответствие нормативным требованиям и шифрование	97
Истории, касающиеся безопасности, с точки зрения SAFECode	99
Персоны и антиперсоны безопасности	101
Истории противника: надеваем черную шляпу	103
Написание историй противника	105
Деревья атак	107
Построение дерева атак	108
Сопровождение и использование деревьев атак	109
Требования к инфраструктуре и эксплуатации	110
Сухой остаток	115
Глава 6. Гибкое управление уязвимостями	116
Сканирование на уязвимости и применение исправлений	116
Сначала поймите, что сканировать	117
Затем решите, как сканировать и с какой частотой	118
Учет уязвимостей	119
Управление уязвимостями	120
Как относиться к критическим уязвимостям	124
Обеспечение безопасности цепочки поставок программного обеспечения	125
Уязвимости в контейнерах	127
Лучше меньше, да лучше	127
Как устранить уязвимости по-гибкому	128
Безопасность через тестирование	130
Нулевая терпимость к дефектам	131
Коллективное владение кодом	132
Спринты безопасности, спринты укрепления и хакатоны	133
Долг безопасности и его оплата	135
Сухой остаток	137
Глава 7. Риск для гибких команд	139
Безопасники говорят «нет»	139
Осознание рисков и управление рисками	140
Риски и угрозы	142
Отношение к риску	143

Делать риски видимыми	144
Принятие и передача рисков	145
Изменение контекста рисков	146
Управление рисками в гибких методиках и DevOps	148
Скорость поставки	149
Инкрементное проектирование и рефакторинг	150
Самоорганизующиеся автономные команды	151
Автоматизация	152
Гибкое смягчение риска	152
Отношение к рискам безопасности в гибких методиках и DevOps	155
Сухой остаток	157
Глава 8. Оценка угроз и осмысление атак	159
Осмысление угроз: паранойя и реальность	159
Понимание природы злоумышленников	160
Архетипы злоумышленников	161
Угрозы и цели атаки	164
Разведка угроз	165
Оценка угроз	168
Поверхность атаки вашей системы	169
Картирование поверхности атаки приложения	170
Управление поверхностью атаки приложения	171
Гибкое моделирование угроз	173
Доверие и границы доверия	173
Построение модели угроз	176
«Достаточно хорошо» – и достаточно	176
Думать как противник	179
STRIDE – структурная модель для лучшего понимания противника	180
Инкрементное моделирование угроз и оценка рисков	181
Оценка рисков в самом начале	181
Пересмотр угроз при изменении проекта	182
Получение выгоды от моделирования угроз	183
Типичные векторы атак	185
Сухой остаток	186
Глава 9. Построение безопасных и удобных для пользования систем	188
Проектируйте с защитой от компрометации	188
Безопасность и удобство пользования	189
Технические средства контроля	190
Сдерживающие средства контроля	190
Средства противодействия	191
Защитные средства контроля	191
Детекторные средства контроля	192
Компенсационные средства контроля	192

Архитектура безопасности.....	193
Безопасность без периметра.....	193
Предполагайте, что система скомпрометирована.....	196
Сложность и безопасность.....	197
Сухой остаток.....	199
Глава 10. Инспекция кода в интересах безопасности	200
Зачем нужна инспекция кода?	200
Типы инспекций кода	202
Формальные инспекции.....	202
Метод утенка, или Проверка за столом	202
Парное программирование (и программирование толпой)	203
Дружественная проверка	204
Аудит кода	204
Автоматизированная инспекция кода.....	205
Какой подход к инспекции оптимален для вашей команды?.....	205
Когда следует инспектировать код?	206
До фиксации изменений.....	206
Контрольно-пропускные проверки перед релизом	207
Посмертное расследование.....	207
Как проводить инспекцию кода.....	208
Применяйте наставление по кодированию	208
Контрольные списки для инспекции кода.....	209
Не делайте этих ошибок	210
Инспектируйте код небольшими порциями	211
Какой код следует инспектировать?	212
Кто должен инспектировать код?.....	214
Сколько должно быть инспекторов?	215
Каким опытом должны обладать инспекторы?	216
Автоматизированная инспекция кода.....	217
Разные инструменты находят разные проблемы	219
Какие инструменты для чего подходят.....	221
Приучение разработчиков к автоматизированным инспекциям кода.....	224
Сканирование в режиме самообслуживания.....	226
Инспекция инфраструктурного кода	228
Недостатки и ограничения инспекции кода.....	229
Для инспекции нужно время.....	230
Разобраться в чужом коде трудно.....	231
Искать уязвимости еще труднее	231
Внедрение инспекций кода на безопасность	233
Опирайтесь на то, что команда делает или должна делать	233
Рефакторинг: поддержание простоты и безопасности кода	235
Базовые вещи – вот путь к безопасному и надежному коду.....	236
Инспекция функций и средств контроля, относящихся к безопасности.....	238

Инспекция кода на предмет угроз от инсайдеров	239
Сухой остаток	241
Глава 11. Гибкое тестирование безопасности	244
Как производится тестирование в гибких методиках?	244
Кто допускает ошибки, тот побежден	246
Пирамида гибкого тестирования	247
Автономное тестирование и TDD	249
Последствия автономного тестирования для безопасности системы	250
Нам не по пути успеха	251
Тестирование на уровне служб и средства BDD	253
Gauntlt («придирайся к своему коду»)	253
BDD-Security	254
Заглянем под капот	254
Приемочное тестирование	256
Функциональное тестирование и сканирование безопасности	256
Краткое пособие по ZAP	257
ZAP в конвейере непрерывной интеграции	259
Совместное использование BDD-Security и ZAP	260
Трудности, возникающие при сканировании приложений	262
Тестирование инфраструктуры	265
Проверка правил оформления	267
Автономное тестирование	267
Приемочное тестирование	267
Создание автоматизированного конвейера сборки и тестирования	269
Ночная сборка	270
Непрерывная интеграция	270
Непрерывная поставка и непрерывное развертывание	271
Экстренное тестирование и инспекция	272
Передача в эксплуатацию	273
Рекомендации по созданию успешного автоматизированного конвейера	274
Место тестирования безопасности в конвейере	274
Место ручного тестирования в гибких методиках	276
Как добиться, чтобы тестирование безопасности работало в гибких методиках и DevOps?	278
Сухой остаток	280
Глава 12. Внешние инспекции, тестирование и рекомендации	282
Почему нужны внешние инспекции?	283
Оценка уязвимости	286
Тестирование на проникновение	287
Команда красных	291
Вознаграждение за обнаружение ошибок	293
Как работает программа вознаграждения	293

Подготовка к программе вознаграждения за найденные ошибки	294
А вы уверены, что хотите запустить программу вознаграждения?	299
Инспекция конфигурации	303
Аудит безопасности кода	303
Криптографический аудит	304
Выбор сторонней компании	306
Опыт работы с продуктами и организациями, похожими на ваши	307
Активная исследовательская работа и повышение квалификации	307
Встречи с техническими специалистами	308
Оценка результатов оплаченной работы	308
Не тратьте чужое время попусту	309
Проверка найденных проблем	309
Настаивайте на устраивающей вас форме результатов	310
Интерпретируйте результаты в контексте	310
Подключайте технических специалистов	310
Измеряйте улучшение со временем	310
Храните сведения о состоявшихся инспекциях и ретроспективном анализе и делитесь результатами	311
Распределяйте устранение проблем между командами, чтобы способствовать передаче знаний	311
Время от времени ротлируйте оценщиков или меняйте местами тестировщиков	311
Сухой остаток	312
Глава 13. Эксплуатация и безопасность	314
Укрепление системы: настройка безопасных систем	315
Нормативно-правовые требования к укреплению	317
Стандарты и рекомендации, относящиеся к укреплению	318
Проблемы, возникающие при укреплении	319
Автоматизированное сканирование на соответствие нормативным требованиям	321
Подходы к построению укрепленных систем	322
Автоматизированные шаблоны укрепления	324
Сеть как код	325
Мониторинг и обнаружение вторжений	327
Мониторинг с целью организации обратной связи	328
Использование мониторинга приложений в интересах безопасности	328
Аудит и протоколирование	330
Проактивное и реактивное обнаружение	333
Обнаружение ошибок во время выполнения	334
Оборона во время выполнения	336
Обеспечение безопасности в облаке	336
RASP	337
Реакция на инциденты: подготовка к взлому	340
Тренируйтесь: учения и команда красных	340

Посмертный анализ без поисков виновного: обучение на инцидентах безопасности.....	342
Защита сборочного конвейера	344
Укрепление инфраструктуры сборки.....	346
Выяснение того, что происходит в облаке.....	346
Укрепление инструментов непрерывной интеграции и поставки.....	347
Ограничение доступа к диспетчерам конфигурации	349
Защита ключей и секретов.....	349
Ограничение доступа к репозиториям	349
Безопасный чат	350
Просмотр журналов	351
Использование серверов-фениксов для сборки и тестирования.....	351
Мониторинг систем сборки и тестирования	352
Шшш... секреты должны храниться в секрете.....	352
Сухой остаток.....	355
Глава 14. Соответствие нормативным требованиям	357
Соответствие нормативным требованиям и безопасность.....	358
Различные подходы к законодательному регулированию.....	361
PCI DSS: подход на основе правил	362
Надзор за целостностью и соблюдением требований: подход на основе результатов	366
Какой подход лучше?.....	367
Управление рисками и соответствие нормативным требованиям.....	367
Прослеживаемость изменений	369
Конфиденциальность данных.....	370
Как соответствовать нормативным требованиям, сохраняя гибкость.....	372
Истории о соответствии и соответствие в историях.....	373
Больше кода, меньше писанины.....	374
Прослеживаемость и гарантии непрерывной поставки	376
Управление изменениями при непрерывной поставке	379
Разделение обязанностей	381
Встраивание соответствия нормативным требованиям в корпоративную культуру	383
Как доставить удовольствие аудитору	384
Как быть, когда аудиторы недовольны	386
Сертификация и аттестация.....	387
Непрерывное соответствие и взломы	387
Сертификация не означает, что вы в безопасности.....	388
Сухой остаток.....	388
Глава 15. Культура безопасности	390
Важность культуры безопасности.....	391
Определение «культуры».....	391
Тяни, а не толкай.....	391

Выстраивание культуры безопасности	392
Принципы эффективной безопасности	393
Содействуй, а не блокируй	395
Прозрачная безопасность	399
Не ищите виноватых	401
Масштабировать безопасность, усиливать фланги	405
Кто – не менее важно, чем как	407
Продвижение безопасности	408
Эргобезопасность	410
Информационные панели	412
Сухой остаток	417
Глава 16. Что такое гибкая безопасность?	418
История Лауры	418
Не инженер, а хакер	418
Твое дитя – уродец, и ты должен чувствовать себя виноватым	419
Поменьше говори, побольше слушай	420
Давайте двигаться быстрее	420
Создание круга поклонников и друзей	421
Мы невелички, но нас много	421
История Джима	422
Вы можете вырастить собственных экспертов по безопасности	422
Выбирайте людей, а не инструменты	424
Безопасность должна начинаться с качества	425
Соответствие нормативным требованиям может стать повседневной практикой	426
История Майкла	426
Знания о безопасности распределены неравномерно	429
Практическим специалистам нужно периодически проходить повышение квалификации	430
Аккредитация и гарантии отмирают	430
Безопасность должна содействовать делу	431
История Рича	431
Первый раз бесплатно	432
А это может быть не просто хобби?	433
Прозрение	433
С компьютерами трудно, с людьми еще труднее	434
И вот мы тут	435
Сведения об авторах	436
Об иллюстрации на обложке	438
Предметный указатель	439