Введение

Может ли система считаться действительно надежной, если по сути она не является безопасной? И наоборот, можно ли считать ее безопасной, если она ненадежна?

Для успешного проектирования, внедрения и обслуживания систем требуется стремление к обеспечению полного жизненного цикла системы. Это возможно лишь тогда, когда безопасность и надежность являются центральными элементами в архитектуре систем. Но оба эти явления часто считаются второстепенными и учитываются только после появления инцидента, что приводит к дорогостоящим и иногда трудным нововведениям.

Конструктивная информационная безопасность (Security by Design) (https://wiki.owasp.org/index.php/Security_by_Design_Principles) все более важна в мире, где многие продукты имеют выход в Интернет и облачные технологии становятся все более распространенными. Чем больше мы полагаемся на эти системы, тем надежнее они должны быть. Чем больше мы доверяем их безопасности, тем безопаснее они должны быть.

СИСТЕМЫ

В этой книге мы в основном говорим о *системах*, которые подразумевают концептуальный подход к группам компонентов, взаимодействующих между собой для выполнения некоторой функции. В нашем контексте системного проектирования эти компоненты обычно включают в себя части ПО, работающие на процессорах различных компьютеров. Они могут также включать само оборудование и процессы, с помощью которых люди проектируют, внедряют и обслуживают системы. Рассуждать о поведении систем может быть трудно, так как нередко оно бывает сложным и непредсказуемым.

Почему мы написали эту книгу

Мы хотели написать книгу, в которой основное внимание уделяется интеграции безопасности и надежности в жизненный цикл ПО и системы, с тем чтобы рассказать о технологиях и методах, которые защищают системы и обеспечивают их надежность, а также проиллюстрировать, как эти практики взаимодействуют друг с другом. Цель нашей книги — предоставить информацию о разработке,

внедрении и обслуживании систем от профессионалов-практиков, которые специализируются на безопасности и надежности.

Надо сразу признать, что отдельные стратегии, рекомендованные в книге, требуют поддержки инфраструктуры, которой просто может не быть там, где вы сейчас работаете. По возможности мы рекомендуем подходы, подходящие для организаций любого масштаба. Но здесь мы хотели поделиться мыслью о том, как можно развивать и совершенствовать существующие методы обеспечения безопасности и надежности, ведь все члены нашего растущего и квалифицированного сообщества могут многому научиться друг у друга. Надеемся, что другие организации тоже захотят поделиться с сообществом своими успехами и историями. Чем шире наши представления о безопасности и надежности, тем полезнее это будет для профессиональной среды. Инженерия безопасности и надежности все еще быстро развивается. Мы постоянно сталкиваемся с условиями и случаями, которые заставляют нас пересматривать (или в некоторых случаях заменять) ранее беспрекословно принимаемые убеждения.

Для кого предназначена эта книга

Безопасность и надежность — это ответственность каждого, поэтому мы ориентируемся на широкую аудиторию: людей, которые проектируют, внедряют и поддерживают системы. Мы не будем проводить границы между традиционными профессиональными ролями разработчиков, архитекторов, инженеров по обеспечению надежности сайтов (SRE) (https://landing.google.com/sre/sre-book/chapters/introduction/), системных администраторов и инженеров по проектированию безопасности. Хотя некоторые раскрываемые нами темы могут быть более полезны для опытных инженеров, мы приглашаем вас — читателей — примерить на себя разные роли, которых у вас (в настоящее время) нет, и представить, как можно было бы улучшить свои системы.

Мы уверены, что всем стоит задумываться об основах надежности и безопасности с самого начала процесса разработки и интегрировать эти принципы на ранних этапах жизненного цикла системы. Это важнейшая концепция, вокруг которой построен весь материал книги. В отрасли ведется множество дискуссий о том, что специалисты по защите информации все больше похожи на разработчиков ПО, а SR-инженеры и разработчики ПО больше напоминают специалистов по защите информации[1]. Мы приглашаем вас присоединиться к обсуждению.

---

[1] См., например, статью: *Zovi D. D.* Every Security Team is a Software Team Now (www.blackhat.com/us-19/briefings/schedule/index.html#every-security-team-is-a-software-team-now-17280) на Black Hat USA 2019, DevSecOps (https://oreil.ly/_PAzE) на саммите Open Security и аналитическую статью в SANS: *Shackleford D.* A DevSecOps Playbook (https://oreil.ly/Wmcx).

Когда мы говорим «вы» в книге, мы подразумеваем читателя, независимого от конкретной работы или уровня опыта. Эта книга бросает вызов традиционным представлениям о ролях специалистов. Она направлена на то, чтобы вы могли нести ответственность за безопасность и надежность на протяжении всего жизненного цикла продукта. Не нужно стараться использовать все методы, описанные здесь, в ваших конкретных обстоятельствах. Вместо этого мы советуем возвращаться к этой книге на разных этапах карьеры или по мере развития вашей организации. Помните, что идеи, которые на первый взгляд не казались ценными, могут получить новое значение.

Примечание о культуре

Для применения широко распространенных передовых практик, которые мы рекомендуем в книге, нужен определенный уровень культуры, способствующей таким изменениям. Мы считаем, что, выбирая технологию, которой вы будете пользоваться, важно учитывать культуру вашей организации. Тогда вы сможете сосредоточиться как на безопасности, так и на надежности, чтобы любые внесенные вами изменения были постоянными и жизнеспособными. По нашему мнению, организации, которые не осознают важность безопасности и надежности, должны измениться, а перестройка культуры самой организации часто требует предварительных инвестиций.

Мы включили в книгу лучшие технические практики и подкрепили их данными. Но невозможно включить лучшие культурные практики, основанные на данных. Хотя в этой книге предлагаются подходы, которые, как мы думаем, другие могут адаптировать или обобщить, каждая организация имеет особую и уникальную культуру. Мы рассматриваем работу Google в рамках своей культуры, но это может не иметь ничего общего с культурой вашей организации. Вместо этого мы рекомендуем извлечь подходящие вам практики из рекомендаций, которые мы включили в эту книгу.

Как читать эту книгу

Хоть книга и содержит множество примеров, это не сборник рецептов. Мы описываем истории Google и индустрии в целом, а также делимся тем, что узнали за эти годы. Все примеры инфраструктуры разные, поэтому некоторые предлагаемые нами решения вам нужно будет адаптировать. Часть из них вообще могут не подходить вашей организации. Мы стараемся предоставить вам высокоуровневые принципы и практические решения, которые вы сможете применить в соответствии с вашей уникальной средой.

Начните с глав 1 и 2, а затем можете читать главы, которые вас больше всего интересуют. Многие главы начинаются с предисловия или краткого обзора, в котором изложено следующее.

- Формулировка проблемы.
- На каком этапе жизненного цикла разработки ПО стоит применять описанные принципы и практики.
- Пересечения и/или компромиссы между надежностью и безопасностью, которые необходимо учитывать.

В каждой главе темы, как правило, упорядочены от фундаментальных до самых сложных. Углубленный анализ и специализированные темы мы обозначаем значком с изображением аллигатора.

В этой книге много инструментов или методов, которые считаются в профессиональной среде хорошими практиками. Не каждая идея подойдет для вашего конкретного случая использования, поэтому сначала оцените требования своего проекта и проектные решения, адаптированные к вашему конкретному ландшафту рисков.

Несмотря на то что это книга для самостоятельной работы, вы найдете ссылки на издания Site Reliability Engineering (https://landing.google.com/sre/sre-book/toc/index.html) и The Site Reliability Workbook (https://landing.google.com/sre/workbook/toc/), где эксперты из Google описывают, как именно надежность влияет на проектирование сервисов. Чтение этих книг может дать более глубокое понимание некоторых концептов, но читать их необязательно.

Мы надеемся, что вам понравится наша книга и что некоторая информация на этих страницах поможет вам повысить надежность и безопасность ваших систем.

Условные обозначения, используемые в книге

В этой книге используются следующие типографские условные обозначения.

Курсив

Курсивом выделены новые термины.

Рубленый шрифт

Используется, чтобы отмечать URL-адреса, адреса электронной почты, элементы интерфейса.

`Моноширинный шрифт`

Используется для листингов программ, а также внутри текста для выделения элементов программ, таких как имена переменных, функций, баз данных, типов данных, переменных окружения, инструкций и ключевых слов. Им также выделены имена и расширения файлов.

`Полужирный моноширинный шрифт`

Выделяет команды или другой текст, который пользователь должен ввести самостоятельно.

`Курсивный моноширинный шрифт`

Выделяет текст, который должен быть заменен значениями, введенными пользователем, или значениями, определяемыми контекстом.

Этот элемент обозначает общее примечание.

Этот значок указывает на углубленный анализ.

Благодарности

Эта книга — результат энтузиазма и щедрого вклада около 150 человек, включая авторов, технических писателей, руководителей отделов и рецензентов из инженерных, юридических и маркетинговых отделов, которые охватывают 18 часовых поясов в Северной и Южной Америке, Европе и Азиатско-Тихоокеанском регионе. Мы хотели бы поблагодарить всех, кто еще не внесен в список для каждой главы.

В качестве лидеров безопасности в Google и SRE Гордон Чаффи, Роял Хансен, Бен Латч, Сунил Потти, Дэйв Ренсин, Бенджамин Трейнор Слосс и Майкл Вайлдпанер были кураторами проекта в Google. Их вера в проект, который фокусируется на интеграции безопасности и надежности непосредственно в жизненный цикл программного обеспечения и системы, была важна для выпуска книги.

Эта книга никогда не вышла бы без стремления и преданности Аны Опреа. Она распознала ценность этой идеи, инициировала ее в Google, поделилась ею с лидерами SRE и безопасности и организовала огромный объем работы, необходимой для ее реализации.

Мы хотели бы выразить признание людям, которые внесли свой вклад, предоставив данные с их обсуждением и рассмотрением.

- Глава 1: Фелипе Кабрера, Перри Циник и Аманда Уокер.
- Глава 2: Джон Асанте, Шейн Хантли и Майк Койвунен.
- Глава 3: Амайя Букер, Михал Чапинский, Скотт Дайер и Райнер Волафка.
- Глава 4: Фелипе Кабрера, Дуглас Колиш, Питер Дафф, Кори Хардман, Ана Опреа и Сергей Симаков.
- Глава 5: Поль Гуглиельмино и Мэттью Сакс.
- Глава 6: Дуглас Колиш, Поль Гуглиельмино, Кори Хардман, Сергей Симаков и Питер Вальчев.
- Глава 7: Адам Бахус, Брэндон Бейкер, Аманда Бурридж, Грег Касл, Петр Левандовски, Марк Лодато, Дэн Лоренк, Дамиан Меншер, Анкур Рати, Даниэль Реболледо Сампер, Миче Смит, Сампат Шринивас, Кевин Стадмейер и Аманда Уокер.
- Глава 8: Пьер Бурдон, Перри Циник, Джим Хиггинс, Август Хубер, Петр Левандовски, Ана Опреа, Адам Стабблфилд, Сет Варго и Тоби Вайнгартнер.
- Глава 9: Ана Опреа и Дж. К. ван Винкель.
- Глава 10: Золтан Егид, Петр Левандовски и Ана Опреа.
- Глава 11: Хизер Адкинс, Бетси Бейер, Ана Опреа и Райан Сливи.
- Глава 12: Дуглас Колиш, Феликс Грёберт, Кристоф Керн, Макс Люббе, Сергей Симаков и Питер Вальчев.
- Глава 13: Дуглас Колиш, Даниэль Фабиан, Адриен Куныш, Сергей Симаков и Дж. К. ван Винкель.
- Глава 14: Брэндон Бейкер, Макс Люббе и Федерико Скринци.
- Глава 15: Оливер Барретт, Пьер Бурдон и Сандра Райчевич.
- Глава 16: Хизер Адкинс, Джон Асанте, Тим Крейг и Макс Люббе.
- Глава 17: Хизер Адкинс, Йохан Берггрен, Джон Ланни, Джеймс Неттесхайм, Аарон Петерсон и Сара Смоллетт.
- Глава 18: Йохан Берггрен, Мэтт Линтон, Майкл Синно и Сара Смоллетт.
- Глава 19: Абхишек Арья, Уилл Харрис, Крис Палмер, Карлос Пизано, Эдриенн Портер Фелт и Джастин Шух.
- Глава 20: Ангус Кэмерон, Даниэль Фабиан, Вера Хаас, Роял Хансен, Джим Хиггинс, Август Хубер, Артур Янк, Майкл Яноско, Майк Койвунен, Макс

Люббе, Ана Опреа, Эндрю Поллок, Лора Посей, Сара Смоллетт, Питер Вальчев и Эдуардо Вела Нава.

- Глава 21: Дэвид Чаллонер, Артур Янк, Кристоф Керн, Майк Койвунен, Костя Серебряный и Дейв Вайнштейн.

Мы также хотели выразить особую благодарность Андрею Силину за его руководство на протяжении всего периода работы над книгой.

Следующие рецензенты предоставили ценную информацию и отзывы, которые весьма помогли нам: Хизер Адкинс, Кристин Бердан, Шоди Данаи Армстронг, Мишель Даффи, Джим Хиггинс, Роб Манн, Роберт Морлино, Ли-Анн Малхолланд, Дейв О'Коннор, Чарльз Проктор, Оливия Пуэрта, Джон Риз, Панкадж Рохатги, Бриттани Стагнаро, Адам Стабблфилд, Тодд Андервуд и Миа Ву. Особая благодарность Дж. К. ван Винклю за проверку целостности книги.

Мы также благодарны следующим авторам, которые поделились опытом и ресурсами: Аве Катушка, Кенту Кавахара, Кевину Молду, Дженнифер Петофф, Тому Саплу, Салиму Вирджи и Мерри Йен.

Внешний обзор от Эрика Гросса помог нам найти хороший баланс между новизной и практическими советами. Мы очень ценим его помощь, а также содержательные отзывы, которые мы получили от рецензентов: Блейка Биссета, Дэвида Н. Бланк-Эдельмана, Дженнифер Дэвис и Келли Шортридж. Детальные обзоры следующих людей сделали каждую главу лучше ориентированной на целевую аудиторию: Курт Андерсен, Андреа Барберио, Ахил Бехл, Алекс Блевитт, Крис Блоу, Джош Бранхам, Анджело Файлла, Тони Годфри, Марко Гуэрри, Эндрю Хоффман, Стив Хафф, Дженнифер Янеско, Эндрю Калат, Томас А. Лимончелли, Аллан Лиска, Джон Луни, Найл Ричард Мерфи, Лукаш Сиудут, Дженнифер Стивенс, Марк ван Хольштейн и Витсе Венема.

Особенно мы хотим поблагодарить Шилайе Нукала и Пола Бланкиншипа, которые помогли командам технических писателей, поделившись своими знаниями в SRE и безопасности.

Наконец, мы хотели бы поблагодарить следующих авторов, которые работали над содержанием, не вошедшим в эту книгу: Хизер Адкинс, Амайю Букер, Пьера Бурдон, Алекса Брэмли, Ангуса Кэмерона, Дэвида Чаллонера, Дугласа Колиша, Скотта Дира, Фануэля Гриаба, Феликса Грёберта, Рояла Хансена, Джима Хиггинса, Августа Хубера, Криса Ханта, Артура Янка, Майкла Яноско, Хантера Кинга, Майка Койвунена, Сюзанну Ландерс, Роксану Лоза (Roxana Loza), Макса Люббе, Томаса Мауфера, Шилайю Нукала, Ану Опреа, Массимилиано Полетто, Эндрю Поллока, Лауру Посей, Сандру Райчевич, Фатиму Ривера, Стивена

Роддиса, Джули Сарацино, Дэвида Сейдмана, Фермина Серна, Сергея Симакова, Сару Смоллетт, Йохана Страмфер, Питера Вальчев, Сайруса Везуна, Джанет Вонг, Якуба Вармуза, Энди Уорнера и Дж. К. ван Винкля.

Спасибо команде O'Reilly Media — Вирджинии Уилсон, Кристен Браун, Джону Девинсу, Коллин Лобнер и Никки Макдональд — за их помощь и поддержку в реализации этой книги. Спасибо Рэйчел Хэд за фантастический опыт редактирования!

Наконец, основная команда книги хотела бы лично поблагодарить следующих людей.

От Хизер Аджинс

Меня часто спрашивают, как Google всегда остается безопасным. Если отвечать вкратце, то разнообразные качества его людей — это основа способности Google обеспечивать свою безопасность. Я уверена, что за всю свою жизнь не найду большего числа работающих в одной команде защитников Интернета, чем люди из Google. Хочу выразить особенную благодарность Уиллу, моему замечательному мужу, моей маме (Либби), папе (Майку) и брату (Патрику), а также Аполлону и Ориону. Спасибо моей команде и коллегам в Google за то, что они терпели мои пропуски во время написания этой книги, и за их стойкость перед лицом устрашающих злоумышленников; Эрику Гроссу, Биллу Кофрану, Урсу Хёльцле, Роялу Хансену, Виталию Гуданцу и Сергею Брину за их руководство, обратную связь и периодическое поднятие брови за последние 17 с лишним лет, моим дорогим друзьям и коллегам (Мерри, Максу, Сэму, Ли, Сиобану, Пенни, Марку, Джесс, Бену, Рене, Джеку, Ричу, Джеймсу, Алексу, Лиаму, Джейн, Томиславу и Натали), особенно r00t++, за их поддержку. Спасибо, доктор Джон Бернхардт, за то, что вы многому меня научили; простите, что я так и не получила степень!

От Бетси Бейер

Бабушке, Эллиотту, тете Е и Джоан, которые вдохновляют меня каждый день. Вы все мои герои! Кроме того, Даззи, Хаммеру, Кики, Мини и Салиму, которые помогли мне стать такой фанатичной писательницей и человеком, каким я являюсь.

От Пола Бланкиншипа

Прежде всего хочу поблагодарить Эрин и Миллера, на чью поддержку я полагаюсь, и Мэтта и Ноа, которые никогда не перестают меня смешить. Я хочу выразить свою благодарность моим друзьям и коллегам в Google — особенно техническим писателям, которые борются с концепциями и языком и которые должны одновременно быть экспертами *и* защитниками наивных

пользователей. Огромная благодарность остальным авторам этой книги — я восхищаюсь вами и уважаю каждого из вас. То, что мое имя ассоциируется с вашими, — большая честь для меня.

От Сюзанны Ландерс

Всем авторам этой книги: я не могу выразить, насколько важно для меня быть частью этого путешествия! Я не была бы там, где я нахожусь сегодня, без нескольких особенных людей: без Тома — он помог мне в самый нужный момент; Кирилла — он научил меня всему, что я знаю сегодня; Ханнеса, Майкла и Петра — они пригласили меня присоединиться к самой удивительной команде в истории (Semper Tuti — всегда в безопасности!). Всем, кто зовет меня на кофе (вы знаете, кого я имею в виду!). Жизнь была бы невероятно скучной без вас. Вербене, которая, вероятно, повлияла на формирование меня самой больше, чем кто-либо другой, и, самое главное, любви всей моей жизни — за твою безоговорочную поддержку и наших самых удивительных и замечательных детей. Я не знаю, чем я заслужила всех вас, но я сделаю для вас все возможное.

От Петра Левандовски

Всем, кто делает мир лучше, чем он был до их прихода. Моей семье за безусловную любовь. Моей партнерше за то, что разделила свою жизнь с моей, к лучшему или к худшему. Друзьям за радость, которую они приносят в мою жизнь. Коллегам за то, что они были определенно лучшей частью моей работы. Моим наставникам за их постоянное доверие. Я не был бы соавтором этой книги без их поддержки.

От Аны Опреа

Малышу, который родится, когда книга выйдет из типографии. Спасибо моему мужу Фабиану, который поддержал меня и позволил поработать над этой и многими другими вещами. Я благодарна, что мои родители, Ика и Ион, понимают, что я нахожусь далеко. Этот проект — доказательство того, что не может быть никакого прогресса без открытой, конструктивной обратной связи. Я смогла руководить работой над созданием книги только благодаря опыту, накопленному в последние годы, благодаря моему менеджеру Яну и всей команде разработчиков. И последнее, но не менее важное: хочу выразить свою благодарность сообществу поддержки BSides: Мюнхен и MUC:SEC, которые были созидающим местом и откуда я постоянно черпаю знания.

От Адама Стабблфилда

Спасибо моей жене, моей семье и всем моим коллегам и наставникам за эти годы.

От издательства

Мы выражаем огромную благодарность компании «КРОК» за помощь в работе над русскоязычным изданием книги и их вклад в повышение качества переводной литературы.

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

О научном редакторе русскоязычного издания

Анна Белых — старший инженер-разработчик в компании КРОК. Участвовала в проектировании и разработке высоконагруженных информационных систем разных масштабов и с применением различных архитектурных решений. Занимается вопросами производительности серверной (бэкенд) части информационных систем.