ДУГЛАС У. ХАББАРД
РИЧАРД СИРСЕН

КАК ОЦЕНИТЬ РИСКИ В КИБЕРБЕЗОПАСНОСТИ

ЛУЧШИЕ ИНСТРУМЕНТЫ И ПРАКТИКИ

БОМБОРА
ИЗДАТЕЛЬСТВО

КиберБез. Лучшие книги о безопасности в сети

Дуглас Хаббард

Как оценить риски в кибербезопасности. Лучшие инструменты и практики

«Эксмо»

2016

УДК 004.056
ББК 32.973-018.2

Хаббард Д. У.

Как оценить риски в кибербезопасности. Лучшие инструменты и практики / Д. У. Хаббард — «Эксмо», 2016 — (КиберБез. Лучшие книги о безопасности в сети)

ISBN 978-5-04-188104-7

Перед вами руководство по поиску и измерению рисков в кибербезопасности вашей компании. Устаревшим практикам оценки сетевых угроз автор противопоставляет методы, в основе которых лежат математические вычисления и специальные метрики. С помощью набора инструментов, описанных в его книге, вы сможете не только защититься от возможных угроз, но и приобрести новые инструменты для принятия более дальновидных решений по развитию бизнеса. В формате PDF A4 сохранен издательский макет книги.

УДК 004.056
ББК 32.973-018.2

ISBN 978-5-04-188104-7

Содержание

Дуглас У. Хаббард, Ричард Сирсен
Как оценить риски в кибербезопасности. Лучшие инструменты и практики

Посвящение Дугласа Хаббарда:

Моим детям Эвану, Мадлен и Стивену – постоянным источникам вдохновения в моей жизни. А также моей жене, Джанет, за все, что она делает, чтобы дать мне возможность писать, и за то, что она – потрясающий корректор.

Посвящение Ричарда Сирсена:

Всем дамам в моей жизни: Хелене, Каэле, Анике и Бренне. Спасибо за вашу любовь и поддержку как в жизни, так и в написании этой книги. С вами все легко и весело.

Даг и Ричард также хотели бы посвятить эту книгу военнослужащим и сотрудникам правоохранительных органов, специализирующимся в области кибербезопасности.

HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK
Douglas Hubbard, Richard Seiersen, Daniel E. Geer, Stuart McClure

Москва 2023

Предисловие

Нам повезло получить два предисловия от двух ведущих умов в области оценки рисков кибербезопасности: Дэниела Э. Гира – младшего и Стюарта Мак-Клара.

> ***Дэниел Э. Гир – младший,* доктор технических наук**
>
> Дэниел Гир занимается исследованием количественных характеристик безопасности. Его группа в Массачусетском технологическом институте разработала протокол Kerberos, затем было еще несколько стартап-проектов, а сейчас он продолжает работать этой области в качестве руководителя отдела информационной безопасности в компании In-Q-Tel. Дэниел пишет множество работ самого разного объема, и иногда их даже читают. Он инженер-электрик, статистик и человек, уверенный, что в споре рождается истина.

Я с удовольствием рекомендую книгу «Как оценить риски в кибербезопасности. Лучшие инструменты и практики». Тема бесспорно актуальная, я и сам уже долгое время пытаюсь к ней подступиться[1]. Это сложная проблема, и, думаю, будет уместно процитировать бывшего госсекретаря США Джона Фостера Даллеса: «Мерилом успеха выступает не факт наличия сложной проблемы, требующей решения, а то, является ли она той же самой проблемой, что возникла у вас в прошлом году». Данная книга как минимум обещает помочь оставить позади часть старых и сложных проблем.

Практика кибербезопасности – это частично инженерия, а частично логические рассуждения. Главная истина инженерии заключается в том, что проектирование успешно тогда и только тогда, когда сама формулировка проблемы полностью понятна. Основная истина логических рассуждений гласит, что у любых данных есть изъяны, и вопрос в том, можно ли их исправить. И инженерия, и логические рассуждения полагаются на измерения. При достаточно хорошем уровне измерений можно говорить о метриках.

Я называю их метриками потому, что это производные от измерений. Метрика включает в себя измерения, выполняемые для подтверждения текущих решений. Мы с вами, дорогие читатели, занимаемся кибербезопасностью не ради науки, но тем, кто пришел в эту область, имея научный (или философский) интерес, понадобятся измерения для подтверждения теорий. Нам необходимы метрики, полученные на основе достоверных измерений, поскольку в масштабах нашей задачи имеющиеся инструменты требуют усиления. Что ни говори, а игроки не станут играть лучше, если не будет вестись счет.

На заре моей карьеры в банке-маркетмейкере состоялась встреча. Руководитель отдела информационной безопасности, в прошлом работавший в отделе внутреннего аудита и не испытывавший радости от назначения на новую должность, был чересчур резок даже по меркам нью-йоркского мира финансов. Свое выступление он начал не то чтобы мягко:

Вы, служба безопасности, настолько глупы, что не можете сказать мне:

- Насколько я в безопасности?
- В большей ли безопасности, чем был в то же время в прошлом году?
- Я трачу достаточное количество денег?
- Каково мое положение по сравнению с другими людьми моего уровня?
- Какие варианты перехода рисков у меня есть?

Двадцать пять лет спустя эти вопросы остаются актуальными. Ответы на них и подобные им можно получить только с помощью измерений. Вот *почему* нужна эта книга.

И даже если мы все согласны с причиной, настоящая ценность книги – в ответе не на вопрос «Почему?», а на вопрос «Как?». *Как* измерить, а затем выбрать нужный метод, *как* делать это последовательно и неоднократно и *как* двигаться вперед от одного метода к другому по мере совершенствования навыков?

Кто-то скажет, что обеспечить кибербезопасность невозможно, если вы столкнетесь с достаточно опытным противником. Так и есть, но это не важно. Наши противники в основном выбирают цели, которые дадут максимальный результат при затраченных усилиях. Это вежливый намек, что у вас, возможно, не получится противостоять самому целеустремленному противнику, для которого цель оправдывает любые средства, но определенно получится сделать так, чтобы другие цели казались гораздо привлекательнее вас. Как я уже говорил, игроки не станут играть лучше, если не будет вестись счет. Вот что предлагает данная книга – способ улучшить вашу игру.

Для этого нужны числа, ведь именно они являются единственными входными данными, как в инженерии, так и в логических рассуждениях. Не слова. И не цветовое кодирование. Если вас заботит собственное благополучие, если вам хочется быть независимыми и знать, каковы ваши позиции, то вы просто обязаны прочесть эту книгу от корки до корки. Ее текст понятен, объяснения просты, а возможность загрузить электронные таблицы не оставляет вам отговорок, чтобы не попытаться.

Убедительно ли я объяснил? Надеюсь, да.

Примечание

1. Daniel Geer, Jr., Kevin Soo Hoo, and Andrew Jaquith, “Information Security: Why the Future Belongs to the Quants,” *IEEE Security & Privacy* 1, no. 4 (July/August 2003): 32–40, geer.tinho.net/ieee/ieee.sp.geer.0307.pdf.

Предисловие

Стюарт Мак-Клар

Стюарт Мак-Клар – генеральный директор компании Cylance, бывший глобальный технический директор компании McAfee, а также ведущий автор серии книг «Секреты хакеров».

В университете профессора постоянно повторяли нам старую максиму: «Нельзя управлять тем, что невозможно измерить». Я, вчерашний подросток, каждый раз все никак не мог уловить ее смысл. Разумеется, на многочисленных занятиях по компьютерным наукам постоянно приходилось совершенствовать математические алгоритмы в программах, но я толком не понимал, как эти попытки количественной оценки могут пригодиться в управлении хоть чем-нибудь вообще, не говоря уже о киберпространстве.

Так я и строил карьеру в области информационных технологий и программирования, пытаясь найти применение своим уникальным талантам. Измерения в киберсфере меня совсем не привлекали, пока я не коснулся кибербезопасности. Мотивацией к поиску фундаментального способа измерить свои действия в области кибербезопасности стал извечный вопрос: «Защищены ли мы от атаки?»

Очевидный ответ на такой банальный, но вполне понятный вопрос: «Нет. Безопасность не бывает стопроцентной». И все же некоторые из вас отвечают так же, как и я временами, когда мне надоедает этот пустой вопрос: «Да, защищены». Почему? Потому, что на нелепые вопросы и ответы нелепые. Как нам в этом убедиться? Без метрик – никак.

По мере становления моей карьеры в области кибербезопасности сначала в компаниях InfoWorld и Ernst & Young, потом в основанной мной компании Foundstone, затем на руководящих должностях в компании McAfee, которая приобрела Foundstone, а сейчас в собственной компании Cylance у меня сформировалось своеобразное понимание старой фразы профессора, что нельзя управлять тем, что невозможно измерить. Пусть истинно объективной метрики не существует, но вполне возможно провести субъективные и локализованные измерения текущего уровня риска и вашего положения относительно вас самих в прошлом и других компаний вашего уровня.

Измерение рисков кибербезопасности, существующих в организации, – задача и без того нетривиальная, а когда требуется проводить количественные измерения вместо субъективных и качественных оценок, она становится даже пугающей.

В конечном счете для нас, специалистов в области безопасности, главными являются вопросы «С чего начать?» и «Как измерить эффективность и отдачу в сфере кибербезопасности?». Ответить на них возможно только с помощью количественных показателей. До сих пор область кибербезопасности с трудом поддавалась измерению. Помню, когда впервые спросили мое мнение о программе измерения риска безопасности, я ответил что-то вроде: «Нельзя измерить то, что не выражено количественно».

Авторы данной книги начали определять структуру и подбирать алгоритмы и метрики для того, что долгое время казалось невозможным или, по крайней мере, бесполезным в нашей сфере, – для измерения рисков безопасности. Наши измерения могут быть несовершенны, но мы можем определить набор стандартных метрик, обоснованных и поддающихся количественному измерению, а затем использовать те же самые показатели день за днем, чтобы убедиться, что ситуация улучшается. В этом и заключается главная ценность определения и применения набора показателей безопасности. Не надо быть совершенными. Надо всего лишь с чего-то начать и сравнивать свои показатели с теми, что были днем ранее.

Благодарности

Благодарим за помощь в написании книги:
Джека Джонса
Джека Фройнда
Джима Липкиса
Томаса Ли
Кристофера «Кипа» Бона
Скотта Стрэнски
Томаса Гирнюса
Джея Якобса
Сэма Сэвиджа
Тони Кокса
Майкла Мюррея
Патрика Хейма
Чен-Пин Ли
Майкла Сардарызадеха
Стюарта Мак-Клара
Рика Рэнкина
Антона Мобли
Винни Лю
Команду SIRA.org
Дэни Гира
Дэна Розенберга

Особая благодарность Бонни Норман и Стиву Абрахамсону за дополнительное редактирование.

Об авторах

Дуглас Хаббард – создатель метода прикладной информационной экономики и основатель компании Hubbard Decision Research. Он является автором одной из самых продаваемых на английском языке книг по статистике предприятий «Как измерить все, что угодно. Оценка стоимости нематериального в бизнесе»[1] (How to Measure Anything: Finding the Value of «Intangibles» in Business), а также книг The Failure of Risk Management: Why It's Broken and How to Fix It («Провал концепции управления рисками: Почему она не работает и как это исправить») и Pulse: The New Science of Harnessing Internet Buzz to Track Threats and Opportunities («Пульс: отслеживание угроз и возможностей в информационном шуме»). Его книги используются для обучения по многим дисциплинам в крупных университетах, они переведены на восемь языков, а их продажи превысили 100 000 копий. Опыт консультирования Хаббарда в области количественных характеристик анализа решений и проблем измерения насчитывает в общей сложности 27 лет и охватывает самые разные сферы, в том числе фармацевтику, страхование, банковское дело, коммунальный сектор, кибербезопасность, посредничество для развивающихся стран, горнодобывающую отрасль, федеральное правительство и правительства штатов, развлекательные СМИ, военное снабжение и промышленность. Статьи Хаббарда опубликованы в ряде периодических изданиях, среди которых *Nature, The IBM Journal of R&D, Analytics, OR/MS Today, InformationWeek* и *CIO Magazine.*

Ричард Сирсен – исполнительный директор по технологиям с почти 20-летним опытом работы в области информационной безопасности, управления рисками и разработки продуктов. В настоящее время является генеральным директором по вопросам кибербезопасности и конфиденциальности в компании GE Healthcare. Много лет назад, до начала карьеры в сфере технологий, он получил классическое музыкальное образование, если точнее, по курсу гитары. Сейчас Ричард живет с семьей в районе залива Сан-Франциско, все его родные тоже играют на струнных инструментах. В свободное время, которого немного, он медленно, но верно работает над получением степени магистра наук по прогностической аналитике в Северо-Западном университете США. Рассчитывает успеть до пенсии, после чего, по его мнению, будет неплохо снова заняться игрой на гитаре.

[1] М.: Олимп-Бизнес, 2009.

Введение

Почему эта книга и почему сейчас?

Представленная книга – первое продолжение серии, начатой другой очень успешной книгой Дугласа Хаббарда «Как измерить все, что угодно. Оценка стоимости нематериального в бизнесе». Для будущих книг этого цикла рассматривались темы вроде «Управление проектами» или определенные сферы деятельности, например здравоохранение. Требовалось лишь выбрать хорошую идею из длинного списка вариантов.

Риски кибербезопасности идеально подходили для книги новой серии. Тема чрезвычайно актуальна и изобилует проблемами измерений, решить которые часто представляется невозможным. Также нам она кажется крайне важной как для отдельного человека (ведь мы пользуемся платежными системами, у нас есть медицинские карты, данные клиентов, интеллектуальная собственность и т. д.), так и для экономики в целом.

Другим фактором, повлиявшим на выбор темы, стало появление подходящего соавтора. Так как Даг Хаббард – специалист по методам измерения – не может одновременно быть экспертом в любом из потенциальных ответвлений серии, он планировал найти соавтора, который хорошо разбирался бы в конкретной заданной тематике. Хаббарду повезло встретить энтузиаста-добровольца Ричарда Сирсена, имеющего многолетний опыт работы на самых высоких должностях в области управления кибербезопасностью в нескольких крупнейших организациях.

Итак, актуальность, сложность в проведении измерений, широкая и постоянно растущая целевая аудитория и наличие достойного соавтора сделали кибербезопасность идеальным вариантом.

О чем эта книга?

Несмотря на то что книга посвящена рискам кибербезопасности, у нее все же много общего с первым изданием серии «Как измерить все, что угодно», включая рассмотрение следующих вопросов:

- Как принимать наилучшие решения в случаях, когда вы не уверены в настоящем и будущем?
- Как снизить неопределенность даже в тех случаях, когда кажется, что данные недоступны или что цели измерения двусмысленны и неосязаемы?

В частности, в этой книге предлагается альтернатива набору глубоко укоренившихся методов оценки рисков, которые в настоящее время широко используются в сфере кибербезопасности, но не имеют в своей основе математических вычислений или научных методов. С нашей точки зрения, такие методы лишь мешают принятию решений по проблеме, что становится критически важной. И мы утверждаем, что методы, основанные на реальных доказательствах улучшения принимаемых решений, не только практичны, но уже применялись для широкого круга одинаково сложных проблем, в том числе и в кибербезопасности. Мы покажем, что можно начать с простых приемов, а затем развить их до необходимого уровня и при этом избежать проблем, присущих матрицам и шкалам риска. Так что не останется причин тотчас же не перейти на использование более эффективных методов.

Чего следует ожидать

Следует ожидать, что постепенно эффективность принимаемых решений повысится, что будет отражено количественно. В частности, это коснется ключевых решений, принимаемых в ситуации с высокой долей неопределенности, последствия которых при неверном выборе могут быть катастрофическими. Мы считаем, что безопасность охватывает все эти проблемы.

Читателям не обязательно быть экспертами по управлению рисками или кибербезопасности. Методы, применяемые нами в сфере безопасности, можно использовать и во многих других областях. Хотя, конечно, мы надеемся, что наши методики помогут прежде всего специалистам в сфере кибербезопасности более успешно строить защиту и разрабатывать ее стратегии. А также мы надеемся, что благодаря книге многие руководители начнут лучше осознавать риски безопасности и принимать более эффективные решения.

Подходит ли мне эта книга?

Если вы хотите быть уверены, что эта книга для вас, ниже описана целевая аудитория, на которую мы ориентировались.

• Вы – специалист, принимающий решения и стремящийся повысить число верно принятых важных решений (так чтобы это можно было проверить *количественно*).

• Вы – специалист по безопасности, желающий усовершенствовать свою стратегию борьбы со злоумышленниками.

• Вы не относитесь ни к одной из названных категорий, но хотите лучше понять область кибербезопасности и/или управления рисками, используя доступные количественные методы.

Профессиональные количественные аналитики могут пропустить разделы, посвященные исключительно анализу. Профессиональные хакеры могут не читать разделы о безопасности. Мы часто будем рассматривать хорошо знакомые вам области с новой точки зрения или, наоборот, повторять очевидное, поэтому читайте так, как будет удобнее.

Одних технологий недостаточно

Нам необходимо реже проигрывать в борьбе с преступниками. Или хотя бы проигрывать элегантнее, а восстанавливаться быстрее. Многие считают, что для этого нужны более совершенные технологии. Они требуют больше инноваций от поставщиков в области безопасности, даже несмотря на то что частота нарушений при этом не сокращается. На наш взгляд, для успешного противостояния угрозам безопасности нужно что-то не менее (а может, и более) важное, чем инновационные технологии. И под этим «что-то» подразумевается более эффективный способ количественного рассмотрения рисков.

Новые инструменты для тех, кто принимает решения

Нам нужны специалисты, которые последовательно принимали бы оптимальные решения благодаря повышению качества анализа, а также знали бы, как справляться с неопределенностью перед лицом надвигающейся катастрофы. Чтобы этого достичь, требуется инструментарий, элементы которого иногда называют современными модными терминами, такими как прогностическая аналитика, но в целом он включает в себя и науку о принятии решений, и анализ решений, и даже надлежащим образом применяемую статистику.

Как устроена эта книга

Первая часть закладывает основу для рассуждения о неопределенности в области безопасности. Здесь сформулированы определения таких понятий, как безопасность, неопределенность, измерения и управление риском, а также объясняется опасность неправильного их понимания. Нами будет обоснована необходимость более совершенного подхода к измерению риска кибербезопасности и, если уж на то пошло, к измерению эффективности самого анализа рисков кибербезопасности. Кроме того, мы познакомим читателей с весьма простым количественным методом, который может послужить отправной точкой, даже если вам очень не нравится все сложное.

Во второй части подробно раскрывается последовательность шагов для реализации очень простой количественной модели. Мы опишем, как усложнить эту модель и использовать даже минимальное количество данных для ее совершенствования.

Наконец, в третьей части речь пойдет о том, что необходимо для внедрения рассмотренных методов на практике. А кроме того, мы обсудим влияние данной книги на всю «экосистему» кибербезопасности, в том числе на организации по стандартизации и поставщиков.

Часть I. Почему для оценки риска в сфере кибербезопасности необходимы более эффективные инструменты измерения

Глава 1. Самая нужная «заплатка» в кибербезопасности

Ничто так не обманчиво, как слишком очевидные факты.
А. Конан Дойл. Тайна Боскомской долины[2]

После 11 сентября 2001 года усиление мер безопасности вылилось в тщательные досмотры в аэропортах, черные списки пассажиров, появление воздушных маршалов и уничтожение лагерей подготовки террористов. Однако всего 12 лет спустя ФБР стало придавать особое значение совсем другой возникшей проблеме: киберугрозам. Директор ФБР Джеймс Б. Коми, давая 14 ноября 2013 года[1] показания в Комитете Сената США по внутренней безопасности и правительственным делам, заявил:

> …мы ожидаем, что в будущем ресурсы, предназначенные для борьбы с киберугрозами, окажутся равны или даже превысят ресурсы, выделяемые на борьбу с терроризмом.

К такому смещению приоритетов нельзя не отнестись серьезно. Сколько организаций в 2001 году, готовясь противостоять угрозам, которые они считали основными в то время, могли бы представить себе, что киберугрозы не только сравняются с более традиционными террористическими угрозами, но и превзойдут их по степени опасности? А сейчас, на момент написания книги, это уже воспринимается как данность.

Следует признать, что люди, не имеющие отношения к миру кибербезопасности, могут подумать, что ФБР сеет семена страха, неуверенности и сомнений, преследуя политические цели. Но источников страха, неопределенности и сомнений, кажется, уже и так немало, зачем же тогда выделять киберугрозы? Для экспертов по кибербезопасности, разумеется, все вполне очевидно. Мы находимся под ударом, и ситуация, безусловно, станет еще хуже, прежде чем наступит перелом к лучшему.

Ресурсы при этом все еще ограничены. Поэтому специалисты в области кибербезопасности должны уметь эффективно определять отдачу от снижения риска. Неважно, удастся ли точно ее рассчитать, достаточно оценить, является ли выбранная стратегия защиты более рациональным вариантом распределения ресурсов, чем другие. Проще говоря, необходимо измерить и выразить в денежном эквиваленте риск и его снижение. Для этого специалистам не помешает инструкция по распределению ограниченных ресурсов для противодействия все возрастающим киберугрозам и использованию этих ресурсов для оптимального снижения степени риска. Поэтому здесь будут рассмотрены методы:

- измерения самих методов оценки риска;
- измерения степени снижения риска с помощью конкретного метода защиты, контроля, смягчения последствий или стратегии (использование более эффективных методов, как говорилось в предыдущем пункте);

[2] Пер. М. Бессараб.

• постоянного и измеримого повышения эффективности применяемых подходов за счет использования более продвинутых методов, которые читатели смогут взять на вооружение, когда будут готовы.

Давайте теперь уточним, чем наша книга не является. В ней не говорится о технической стороне безопасности. Если вам нужна книга об «этичном взломе», вы обратились не по адресу. Здесь не будет обсуждений, как добиться переполнения стека, обойти алгоритмы шифрования или внедрить SQL-код. Если подобные вопросы и будут подниматься, то только в контексте рассмотрения их как параметров в модели рисков.

И все же не разочаровывайтесь, если вы являетесь техническим специалистом. Мы обязательно затронем детали аналитики применительно к безопасности. Взглянем на них с позиции аналитика или руководителя, пытающегося сделать наилучший выбор в контексте возможных потерь в будущем. А пока давайте оценим масштаб имеющейся проблемы, рассмотрим, как решаем ее сейчас, и наметим направление для улучшений, изложенных в остальной части книги.

Глобальная поверхность атаки

Государства, организованная преступность, хактивистские группировки и инсайдеры хотят заполучить наши секреты, наши деньги и нашу интеллектуальную собственность, а некоторые мечтают о нашем полном уничтожении. Звучит драматично? Что ж, если мы верно поняли, ФБР рассчитывает потратить на защиту нас от киберугроз столько же или больше, чем на защиту от тех, кто превращает самолеты, машины, скороварки и даже людей в бомбы. Так как вы читаете эту книгу, то, вероятно, уже осознаете серьезность ситуации. Тем не менее разъясним этот момент еще раз, хотя бы для того, чтобы помочь тем, кто уже разделяет данную точку зрения, доказывать свою правоту остальным.

Общемировое исследование рабочей силы в области информационной безопасности, проведенное в 2015 году с участием более 14 000 специалистов по вопросам безопасности, из которых 1800 являлись федеральными служащими, показало, что мы не просто несем потери, мы отступаем:

> Учитывая объем усилий, потраченных за последние два года на повышение готовности федеральных систем к обеспечению безопасности, и общую позицию государства в вопросах безопасности, мы ожидали увидеть очевидный прогресс. Данные же показали, что на самом деле был сделан шаг назад.
>
> *(ISC)[2] о результатах исследования, 2015 год*[3]

Данные из других источников подтверждают этот мрачный вывод. Страховой рынок Соединенного Королевства, Лондонский Ллойд, подсчитал, что кибератаки обходятся миру в 400 млрд долл. в год[4]. В 2014 году был скомпрометирован 1 млрд записей с личными данными пользователей, из-за чего журнал *Forbes* назвал его «годом взлома данных»[5]. К сожалению, название, вероятно, было дано преждевременно: ситуация запросто может ухудшиться.

Более того, основатель и глава компании XL Catlin, крупнейшего страховщика Лондонского Ллойда, заявил, что кибербезопасность – «самый большой и серьезный системный риск», с которым ему приходилось сталкиваться за 42 года работы в сфере страхования[6]. Потенциальные уязвимости широко используемого программного обеспечения, взаимосвязанный доступ к сети у компаний, поставщиков и клиентов, а также возможность осуществления масштабных скоординированных атак могут сильно повлиять не только на отдельную крупную компанию вроде Anthem, Target или Sony. Представители XL Catlin допускают вероятность одновремен-

ного воздействия на множество крупных организаций, которое скажется на всей экономике. По их мнению, если в течение короткого промежутка времени поступят обращения с несколькими значительными страховыми претензиями, то страховщикам будет не по силам покрыть все расходы.

Что вызывает такой резкий рост числа взломов и почему ожидается увеличение их количества? Все дело в поверхности атаки (attack surface). Обычно под ней понимают совокупность всех уязвимостей информационной системы. Поверхность атаки раскрывает ценную информацию ненадежным источникам. Не нужно быть профессионалом в области безопасности, чтобы это понять. У вашего дома, банковского счета, семьи, личности есть поверхность атаки. Если вы пользуетесь защитой от кражи личных данных, предоставляемой федеральным служащим или клиентам компаний Home Depot, Target, Anthem и Neiman Marcus, то получаете вы ее благодаря поверхности атаки, ведь эти компании поместили цифровые сведения о вас в зоне досягаемости преступников. Прямо или косвенно этому способствовал интернет. Перемены произошли быстро и без ведома всех заинтересованных сторон (организаций, служащих, клиентов или граждан).

Различные определения поверхности атаки описывают пути входа и выхода из системы, ее средства защиты, а иногда ценность имеющихся в системе данных[7, 8]. В одних случаях термином обозначают поверхность атаки системы, а в других – поверхность атаки сети, но все эти определения слишком узкие даже для одной конкретной компании. Поэтому можно выделить поверхность атаки предприятия, которая включает не только все системы и сети в данной организации, но и воздействие третьих лиц. Речь идет обо всех в экосистеме предприятия, в том числе основных клиентах, поставщиках и, возможно, государственных учреждениях. Напомним, что в случае взлома компании Target источником уязвимости стала компания – поставщик систем отопления, вентиляции и кондиционирования воздуха.

Пожалуй, общая поверхность атаки, охватывающая всех граждан, потребителей и правительства, является своего рода глобальной поверхностью атаки: совокупным набором рисков кибербезопасности во всех системах, сетях и организациях. И с этим набором рисков мы сталкиваемся постоянно при оплате покупок банковской картой, просмотре сайтов в интернете, получении медицинских пособий или даже просто работая. Эта глобальная поверхность атаки – макроуровневое явление, возникновение которого обусловлено по меньшей мере четырьмя макроуровневыми причинами: увеличением числа пользователей по всему миру, разнообразием пользователей в мире, ростом числа обнаруженных и эксплуатируемых уязвимостей из расчета на каждый визит в сеть каждого пользователя, а также более тесным сетевым взаимодействием между организациями, что приводит к риску «каскадного отказа».

• *Увеличение числа пользователей сети Интернет.* Число интернет-пользователей во всем мире выросло в шесть раз за период с 2001 по 2014 год (от 500 млн до 3 млрд). Может быть неочевидно, что количество пользователей является параметром в некоторых поверхностях атаки, но есть другие показатели поверхности атаки, касающиеся ценности цели, которая частично связана с количеством пользователей (например, получение доступа к большему числу личных записей)[9]. Кроме того, в мировом масштабе увеличение числа интернет-пользователей действует как важный мультипликатор для остальных факторов.

• *Число заходов каждого пользователя на онлайн-ресурсы.* Разнообразие вариантов использования интернета, общее время, проведенное в сети, использование банковских карт и различных услуг, требующих хранения персональных данных для автоматизированных переводов средств, – все эти показатели постоянно растут. Для каждого человека. По всему миру. Например, с 2001 года число одних только веб-сайтов росло в пять раз быстрее, чем количество пользователей, достигнув к 2014 году 1 млрд. Устройства с выходом в интернет – еще один потенциальный способ использования Всемирной паутины даже без непосредственного участия человека. Согласно одному из прогнозов компании Gartner об интернете вещей, «количе-

ство подключенных к интернету устройств в 2015 году должно было вырасти на 30 % по сравнению с 2014-м и составить 4,9 млрд, а к 2020-му – достичь 25 млрд»[10]. Ключевой проблемой здесь является отсутствие согласованной системы безопасности в этих разработках. Консультативный комитет по связи в системе национальной безопасности (NSTAC) определил, что «осталось совсем небольшое окно, пока еще можно обеспечить функционирование интернета вещей таким образом, чтобы максимизировать безопасность и минимизировать риски, но это окно быстро закрывается. Если страна этого не сделает, ей придется бороться с последствиями в течение нескольких поколений»[11].

• *Рост числа уязвимостей.* Естественным следствием двух предыдущих факторов является увеличение количества способов использования таких возможностей со злым умыслом. Это происходит из-за роста количества систем и устройств с потенциальными уязвимостями, даже если число уязвимостей в одном устройстве не увеличивается. В любом случае будет расти количество *обнаруженных* уязвимостей, отчасти потому, что все больше людей их активно ищет и использует. И все чаще среди них встречаются хорошо организованные и хорошо финансируемые группы, работающие на различные государства.

• *Возможность крупного каскада взломов.* Все больше крупных организаций отмечают, что при более тесном взаимодействии эффективность работы повышается. Тот факт, что компанию Target взломали через ее поставщика, повышает вероятность того, что одна и та же атака может затронуть несколько организаций. У компаний вроде Target множество поставщиков, а у некоторых из них, в свою очередь, есть множество крупных корпоративных и правительственных клиентов. Составить карту связей такой киберэкосистемы практически невозможно, ведь для этого все задействованные организации должны будут разгласить конфиденциальную информацию. Вот почему для данного фактора не существует общепринятых метрик, которые можно было бы использовать, как в трех предыдущих случаях. Но есть подозрения, что большинство крупных организаций отделены друг от друга всего одним или двумя уровнями связей.

Кажется разумным, что в перечисленных четырех тенденциях более ранние усиливают последующие. В таком случае риск возникновения крупного каскада взломов может увеличиваться быстрее, чем происходит рост первых двух факторов.

Какова наша исходная и очевидная гипотеза? Поверхность атаки и взломы коррелируют. Если это так, самое страшное еще впереди. Мы движемся к историческому росту поверхности атаки и, следовательно, взлому, который затмит все случавшееся до сих пор. С учетом этого комментарии директора ФБР и заявления страховщиков Лондонского Ллойда нельзя считать паникерскими. Даже после таких мощных взломов, каким подверглись компании Target, Anthem и Sony, полагаем, «Большого взлома» мы еще не видели.

Ответ на киберугрозу

Ситуация кажется безвыходной, поскольку успех в бизнесе зависит от открытости. Банковские операции, покупки, медицинское обслуживание и даже трудоустройство связаны с раскрытием данных. Чтобы проводить транзакции, приходится сообщать свои данные, а чем активнее бизнес, тем больше поверхность атаки.

Когда данные открыты, на вас могут обратить внимание и повлиять неожиданными и злонамеренными способами. В целях защиты специалисты по кибербезопасности пытаются «укрепить» системы, т. е. удалить все несущественное, включая программы, пользователей, данные, привилегии и уязвимости. Укрепление сокращает поверхность атаки, но не устраняет ее. Однако даже такое частичное сокращение поверхности атаки требует значительных ресурсов, и, согласно текущим тенденциям, потребность в них будет только расти.

В целом внимание руководителей к рискам кибербезопасности возросло, а за вниманием следуют ресурсы. Советы директоров начинают задавать вопросы вроде «Взломают ли нас?», «Лучше ли мы, чем Sony?» или «Тратим ли мы достаточно на защиту от актуальных рисков?». Эти вопросы в итоге приводят к тому, что в некоторых компаниях вводится должность руководителя отдела информационной безопасности. Впервые она появилась в списке журнала *Fortune* (Fortune 100) более 20 лет назад, но с тех пор не было особого роста количества людей, занимающих эту должность. Журнал *CFO Magazine* признал, что еще в 2008 году должность руководителя отдела информационной безопасности посчитали бы «излишней»[12]. Фактически крупные компании еще только начинают озадачиваться вопросом найма первых руководителей отдела информационной безопасности, и многие – лишь после того, как подвергнутся крупному взлому. К моменту написания этой книги компания Target наконец-то наняла руководителя отдела информационной безопасности[13], то же самое сделала и компания JPMorgan, после того как ее взломали[14].

Корпорации не только задают перечисленные выше вопросы и создают руководящие должности для специалистов по информационной безопасности, но и демонстрируют готовность (возможно, меньшую, чем хотелось бы специалистам по кибербезопасности) выделять серьезные ресурсы на решение этой проблемы.

• Сразу после терактов 11 сентября ежегодный рынок кибербезопасности в США составлял 4,1 млрд долл.[15] К 2015 году бюджет министерства обороны США, выделяемый на информационные технологии, вырос до 36,7 млрд долл.[16]

• Это без учета 1,4 млрд долл. инвестиций в стартапы, занимающиеся кибербезопасностью[17].

• Бюджеты, выделяемые на кибербезопасность, растут примерно в два раза быстрее, чем бюджеты сферы информационных технологий в целом[18].

И как же организации используют новую руководящую должность и приток денег на обеспечение кибербезопасности? В основном они ищут уязвимости, выявляют атаки и устраняют нарушения. Конечно, размер поверхности атаки и объем уязвимостей, атак и нарушений означает, что организациям приходится делать трудный выбор. Не все удается исправить, остановить, восстановить и т. д., значит, обязательно будут определенные приемлемые (допустимые) потери. В документах часто не указано, какие риски являются приемлемыми, а когда они все же расписаны, формулировки обычно обтекаемы и не поддаются количественной оценке. Их нельзя толком использовать в расчетах для определения обоснованности тех или иных расходов.

В отношении уязвимостей это привело к появлению так называемого управления уязвимостями, а в плане атак – к управлению событиями, связанными с безопасностью, которое еще обобщенно называют управлением безопасностью. Совсем недавно добавилась «разведка угроз» и, соответственно, новое словосочетание «управление угрозами». Все они относятся к сфере тактических решений в области безопасности, в то время как руководителю необходимо представление о дальнейших действиях. Так каким образом осуществляется управление безопасностью? Как расставляются приоритеты распределения значительных, но ограниченных ресурсов при расширении списка уязвимостей? Другими словами, как организации принимают решения по кибербезопасности, связанные с распределением ограниченных ресурсов для борьбы с такими неопределенными и растущими рисками?

Безусловно, важную роль здесь играет профессиональное чутье, что не редкость в управленческой деятельности. Но при более систематическом подходе подавляющее большинство организаций, озабоченных проблемой кибербезопасности, прибегает к определенному методу подсчета, при котором риски отображаются на «матрице». Так работают и с проблемами так-

тического уровня, и со стратегическими, суммарными рисками. Например, если у приложения множество уязвимостей, все они объединяются в одну оценку. Затем аналогичными методами группы приложений объединяются в портфель, и строится матрица для него и других портфелей. Процесс агрегирования при этом, как правило, представляет собой некую форму выдуманной математики, неведомой ни актуариям, ни статистикам, ни математикам.

В одном широко применяемом подходе «вероятность» и «воздействие» оценивают субъективно, скажем по шкале от 1 до 5, и эти два значения используются для указания конкретного риска на матрице (называют ее по-разному: матрицей рисков, тепловой картой, картой рисков и т. д.). После матрицу часто дополнительно делят на секции низкого, среднего и высокого риска, подобно тому как показано на рис. 1.1. События, характеризующиеся высокой вероятностью и высокой степенью воздействия, окажутся в правом верхнем углу «высокого риска», в то время как события с низкой вероятностью и слабым воздействием будут в противоположном углу «низкого риска». Идея в том, что чем больше число, тем важнее событие и тем раньше нужно обратить на него внимание. Возможно, интуитивно такой подход кажется вам разумным, если так, то вы не одиноки.

			Воздействие				
			Ничтожное	Незначительное	Умеренное	Критическое	Катастрофическое
			1	2	3	4	5
Вероятность	Часто	5	Средний	Средний	Высокий	Высокий	Высокий
	Как правило	4	Средний	Средний	Средний	Высокий	Высокий
	Время от времени	3	Низкий	Средний	Средний	Средний	Высокий
	Редко	2	Низкий	Низкий	Средний	Средний	Средний
	Практически никогда	1	Низкий	Низкий	Низкий	Средний	Средний

Рис. 1.1. Знакомая матрица риска (она же тепловая карта или карта риска)

Различные варианты подсчета и карт риска одобрены и продвигаются в стандартах и руководящих документах несколькими крупными организациями, среди которых Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST), Международная организация по стандартизации (International Standards Organization, ISO), MITRE.org и сообщество «Открытый проект по обеспечению безопасности веб-приложений» (Open Web Application Security Project, OWASP). Большинство организаций, занимающихся кибербезопасностью, утверждают, что по меньшей мере один из продвигаемых вариантов является частью их основной концепции оценки риска. На самом деле большинство крупных компаний, занимающихся разработкой программного обеспечения, включая Oracle, Microsoft и Adobe, оценивают собственные уязвимости с помощью поддерживаемого NIST стандарта оценок под названием «Общая система оценки уязвимостей» (Common Vulnerability Scoring System, CVSS). Кроме того, множество существующих решений по безопасности также используют показатели CVSS как для оценки уязвимостей, так и в связи с атаками. Несмотря на то что во многих подобных руководящих документах содержатся хорошие рекомендации

по управлению, то, как они используются для расстановки приоритетов в управлении рисками в масштабах предприятия, лишь усиливает риски.

Буквально сотням производителей систем безопасности и даже органам по стандартизации пришлось принять ту или иную форму системы оценки. Фактически концепции балльных оценок и матрицы рисков лежат в основе подходов к управлению рисками в индустрии безопасности.

Во всех случаях подходы строятся на идее, что такие методы приносят значительную пользу, то есть предполагается, что с ними лучше, чем без них. По мнению представителей одной из организаций по стандартизации, подобное ранжирование рисков вполне приемлемо:

> Как только тестировщик определяет потенциальный риск и хочет выяснить, насколько тот серьезен, первым шагом становится оценка *вероятности*. В общем смысле – это приблизительная мера того, насколько велика вероятность, что злоумышленник найдет и использует данную уязвимость. Не обязательно быть очень точным в оценке. В целом достаточно определить, является ли вероятность низкой, средней или высокой.
>
> *OWASP*[19] *(курсив наш. – Д. Х., Р. С.)*

Стоит ли верить последней фразе? Учитывая, в основе каких критически важных решений могут лежать подобные методы, мы утверждаем, что не стоит. Это проверяемое утверждение, и оно реально *проверялось* множеством различных способов. Рост атак в области кибербезопасности сам по себе уже намекает на то, что, возможно, настало время попробовать иной подход.

Поэтому давайте проясним нашу позицию в отношении существующих методов. *Они неудачные. Они не работают.* Тщательное изучение исследований, посвященных как этим методам, так и методам принятия решений в целом, указывает на следующее (обо всем этом подробнее говорится в главах 4 и 5).

• Нет доказательств, что типы балльных оценок и методы построения матриц рисков, широко используемые в кибербезопасности, повышают эффективность суждений.

• Напротив, есть доказательства, что эти методы вносят искажения и ошибки в процесс оценивания. Один из исследователей – Тони Кокс – даже утверждает, что они «хуже, чем действия наугад» (исследование Кокса и многие другие будут подробно описаны в главе 5).

• Вся мнимая «работа» методов, вероятно, является разновидностью эффекта плацебо. То есть метод может заставить вас почувствовать себя лучше, даже если его применение не способствует ощутимому улучшению в оценке рисков (или вовсе увеличивает число ошибок).

• В опубликованных исследованиях имеется огромное количество доказательств эффективности количественных, вероятностных методов.

• К счастью, большинство экспертов по кибербезопасности, похоже, готовы и способны использовать более эффективные количественные решения. Однако распространенные заблуждения (в том числе неправильные представления о базовой статистике), которых придерживаются часть людей, создают ряд препятствий для внедрения более эффективных методов.

Способ, с помощью которого служба кибербезопасности оценивает риск и выявляет степень его снижения, лежит в основе определения того, где следует использовать ресурсы в первую очередь. И если выбранный способ не работает или как минимум требует значительных улучшений, то именно это тогда и является главной проблемой, которой следует заняться службе кибербезопасности! Очевидно, что создание прочного фундамента для методов принятия решений и оценки рисков кибербезопасности повлияет на все остальные действия в сфере

кибербезопасности. Если оценка рисков сама по себе слабое место, то ее исправление – самая важная «заплатка» для специалиста по кибербезопасности.

Предложение по управлению рисками кибербезопасности

В этой книге нами предлагается другое направление развития кибербезопасности, а каждое решение, рассматриваемое в его рамках, в итоге будет полностью соответствовать названию книги. То есть мы будем разбирать вопросы, описывая, как измерить риски кибербезопасности – *все что угодно* в области рисков кибербезопасности. Измерения станут инструментами для предложенных решений и, кроме того, продемонстрируют, каким образом эти решения выбирались. Итак, давайте считать, что мы все принимаем наш новый количественный подход, который строится на следующих принципах.

• *Можно значительно улучшить существующие методы*. Многие аспекты существующих методов были оценены и признаны непродуктивными. Подобное неприемлемо в масштабах проблем, с которыми сталкивается сфера кибербезопасности.

• *В кибербезопасности можно применять тот же количественный язык анализа рисков, что и в других сферах.* Как будет показано далее, существует множество областей, в которых риск огромен, данные минимальны, а участники хаотичны, и для этих областей регулярно строятся модели с помощью традиционных математических методов. Не нужно заново изобретать терминологию или методы, когда они уже есть в других сферах, где также сталкиваются со сложными проблемами анализа рисков.

• *Существуют методы, которые уже показали себя более результативными по сравнению с профессиональным чутьем.* И это верно даже для случаев, когда указанные методы, как и обычные, широко используемые, основываются только на субъективных суждениях экспертов по кибербезопасности.

• *Усовершенствованные методы вполне применимы.* Нам об этом известно, поскольку их уже применяли. Каждый из описанных в книге методов применялся хотя бы одним из авторов в реальных условиях в корпоративной среде. В настоящее время этими методами пользуются специалисты по кибербезопасности из самых разных отраслей.

• *Описываемые модели можно усовершенствовать с помощью эмпирических данных.* У вас больше данных, чем кажется. Они доступны из различных, как существующих, так и новых, только появляющихся источников. Но даже при ограниченных данных математические методы все равно могут быть эффективнее субъективных суждений. Кроме того, сами методы анализа рисков также можно измерять и отслеживать, чтобы постоянно их совершенствовать.

Книга разделена на три части, каждая из которых по-своему подтверждает все перечисленные принципы. В первой части представлен простой количественный метод, требующий чуть больше усилий, чем существующие методы балльной оценки, но в нем применяются техники, продемонстрировавшие заметно более эффективные результаты. Затем мы обсудим, как измерить сами методы измерения. Другими словами, попытаемся ответить на вопрос «Как узнать, что они работают?» относительно различных методов оценки кибербезопасности. Последняя глава первой части будет посвящена разбору распространенных возражений против количественных методов, подробному рассмотрению исследований, показывающих несостоятельность методов балльной оценки, а также обсуждению заблуждений и ложных представлений, удерживающих от перехода на более эффективные методы.

Во второй части мы отойдем от вопроса «почему используются определенные методы» и сосредоточимся на том, как еще улучшить простую модель, описанную в первой части. Мы поговорим о том, как добавить полезные детали к простой модели, как помочь специалистам по кибербезопасности отточить свои навыки оценки неопределенности и как улучшить модель с помощью эмпирических данных (даже если кажется, что данных мало).

В третьей части будет показана более общая картина: как эти методы можно реализовать в компании, как возникают новые угрозы и как развивающиеся инструменты и методы способствуют повышению эффективности измерений рисков кибербезопасности. И еще мы попытаемся сформулировать призыв к сфере кибербезопасности в целом.

А для начала в следующей главе будет заложена основа для понимания термина «измерение». Термин может казаться простым и очевидным, но неверное понимание измерений и методов их осуществления частично является причиной нежелания применять измерения в области кибербезопасности.

Примечания

1. Greg Miller, “FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered,” *Washington Post,* November 14, 2013, www.washingtonpost.com/world/national-security/fbi-directorwarns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-hasaltered/2013/11/14/ 24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html.

2. Dan Waddell, Director of Government Affairs, National Capital Regions of $(ISC)^2$ in an announcement of the Global Information Security Workforce Study (GISWS), www.isc2.org, May 14, 2015.

3. Stephen Gandel, “Lloyd’s CEO: Cyber Attacks Cost Companies $400 Billion Every Year,” Fortune.com, January 23, 2015, http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/.

4. Sue Poremba, “2014 Cyber Security News Was Dominated by the Sony Hack Scandal and Retail Data Breaches,” *Forbes Magazine*, December 31, 2014, www.forbes.com/sites/sungardas/2014/12/31/2014-cybersecurity-news-was-dominated-by-the-sony-hack-scandal-and-retaildata-breaches/#1c79203e4910.

5. Kevin Haley, “The 2014 Internet Security Threat Report: Year Of The Mega Data Breach,” *Forbes Magazine*, July 24, 2014, www.forbes.com/sites/symantec/2014/07/24/the-2014-internet-security-threat-reportyear-of-the-mega-data-breach/#724e90a01a98.

6. Matthew Heller, “Lloyd’s Insurer Says Cyber Risks Too Big to Cover,” CFO.com, February 6, 2015, ww2.cfo.com/risk-management/2015/02/lloyds-insurer-says-cyber-risks-big-cover/.

7. Jim Bird and Jim Manico, “Attack Surface Analysis Cheat Sheet.” OWASP.org. July 18, 2015, www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet.

8. Stephen Northcutt, “The Attack Surface Problem.” SANS.edu. January 7, 2011, www.sans.edu/research/security-laboratory/article/did-attacksurface.

9. Pratyusa K. Manadhata and Jeannette M. Wing, “An Attack Surface Metric,” *IEEE Transactions on Software Engineering* 37, no. 3 (2010): 371–386

10. Gartner, “Gartner Says 4.9 Billion Connected ‘Things’ Will Be in Use in 2015” (press release), November 11, 2014, www.gartner.com/newsroom/id/2905717.

11. The President’s National Security Telecommunications Advisory Committee, “NSTAC Report to the President on the Internet of Things,” November 19, 2014, www.dhs.gov/sites/default/fi les/publications/IoT%20Final%20Draft%20Report%2011–2014.pdf.

12. Alissa Ponchione, “CISOs: The CFOs of IT,” *CFO*, November 7, 2013, ww2.cfo.com/technology/2013/11/cisos-cfos/.

13. Matthew J. Schwartz, “Target Ignored Data Breach Alarms,” *Dark Reading* (blog), *InformationWeek,* March 14, 2014, www.darkreading.com/attacks-and-breaches/target-ignored-data-breach-alarms/d/d-id/1127712.

14. Elizabeth Weise, “Chief Information Security Officers Hard to Find – and Harder to Keep,” *USA Today*, December 3, 2014, www.usatoday.com/story/tech/2014/12/02/sony-hack-attack-chiefinformation-security-offi cer-philip-reitinger/19776929/.

15. Kelly Kavanagh, “North America Security Market Forecast: 2001–2006,” Gartner, October 9, 2002, www.bus.umich.edu/KresgePublic/Journals/ Gartner/ research/110400/110432/110432.html.

16. Sean Brodrick, “Why 2016 Will Be the Year of Cybersecurity,” *Energy & Resources Digest,* December 30, 2015, http://energyandresourcesdigest.com/ invest-cybersecurity-2016-hack-cibr/.

17. Deborah Gage, “VCs Pour Money into Cybersecurity Startups,” *Wall Street Journal*, April 19, 2015, www.wsj.com/articles/vcs-pour-moneyinto-cybersecurity-startups-1429499474.

18. PWC, *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015,* September 30, 2014, www.pwc.be/en/news-publications/ publications/2014/gsiss2015.html.

19. OWASP, “OWASP Risk Rating Methodology,” last modified September 3, 2015, www.owasp.org/index.php/ OWASP_Risk_Rating_Methodology.

Глава 2. Руководство по измерениям для сферы кибербезопасности

Успех складывается из настойчивости, упорства и готовности на протяжении двадцати двух минут разбираться с задачей, которую большинство людей бросили бы после тридцати секунд.
Малкольм Гладуэлл. Гении и аутсайдеры. Почему одним все, а другим ничего?[1]

Прежде чем обсуждать, каким образом в сфере кибербезопасности можно измерить буквально все, нужно поговорить об измерениях как таковых и сразу отмести возражение, что некоторые вещи в кибербезопасности просто не поддаются измерению. Дело в том, что ряд недоразумений, связанных с методами измерений, измеряемыми явлениями или даже с самим понятием измерений, препятствует многим попыткам проводить измерения. Данная глава не принесет ничего нового тем, кто уже читал книгу «Как измерить все, что угодно. Оценка стоимости нематериального в бизнесе». Это отредактированный вариант главы из первой книги с примерами, измененными под сферу кибербезопасности. Так что если вы уже читали первую книгу, то, возможно, предпочтете пропустить главу. В ином случае с главой лучше ознакомиться, чтобы понять важнейшие основы.

По нашему мнению, существует лишь три причины, почему можно посчитать что-либо, в том числе кибербезопасность, не поддающимся измерениям. И все три коренятся в тех или иных заблуждениях, которые мы делим на категории: концепция, объект и метод. Различные возражения против измерений будут подробнее разбираться далее (особенно в главе 5), а пока давайте рассмотрим самое основное.

1. *Концепция измерений*. Термин «измерения» часто понимается неправильно. Как только вы осознаете его реальное значение, гораздо больше объектов и явлений окажутся измеримыми.

2. *Объект измерения*. Не дается точное определение для того, что подвергается измерениям. Небрежные и двусмысленные формулировки мешают измерениям.

3. *Методы измерения*. Многие процедуры эмпирического наблюдения малоизвестны. Если бы люди были знакомы с некоторыми из этих базовых методов, стало бы очевидно, что многие вещи, считающиеся неизмеримыми, не только можно измерить, но, вероятно, они уже давно измерены.

Хороший способ запомнить эти три распространенных заблуждения – воспользоваться памяткой, например «howtomeasureanything.com», где буквы «c», «o» и «m» в «.com» означают «концепцию», «объект» и «метод». Как только выясняется, что эти возражения возникают от недопонимания, становится очевидно, что измерить можно все что угодно.

Концепция измерений

Пока законы математики остаются определенными, они не имеют ничего общего с реальностью; как только у них появляется нечто общее с реальностью, они перестают быть определенными.
Альберт Эйнштейн (1879–1955), немецкий физик

Хоть это может показаться парадоксальным, но вся точная наука подчинена идее аппроксимации. Если человек говорит, что он что-

то точно знает, можно с уверенностью сказать, что вы разговариваете с невнимательным человеком.
Бертран Рассел (1872–1970), британский математик и философ

Для людей, считающих, что какие-то вещи невозможно измерить, сама концепция измерения, или, точнее, ее неверная интерпретация, становится, вероятно, главным препятствием, которое необходимо преодолеть. Если ошибочно полагать, что измерение означает соответствие какому-то почти недостижимому стандарту определенности, то тогда даже в физических науках лишь немногое будет поддаваться измерению.

Если спросить руководителя или эксперта в сфере кибербезопасности, что означает измерение, они, как правило, ответят фразами наподобие «дать количественную оценку», «вычислить точное значение», «свести к одному числу», «выбрать репрезентативную выборку» и т. д. Во всех этих ответах говорится напрямую или подразумевается, что измерение – одно точное число, которое обязано быть верным. Если бы это было действительно так, то и правда лишь очень немногое можно было бы измерить.

Возможно, читателям доводилось слышать или самим говорить что-то вроде: «Нам не измерить реальный ущерб от утечки данных, потому что о некоторых последствиях нельзя знать наверняка». Или, быть может, такое: «Невозможно определить вероятность того, что мы окажемся объектом массированной атаки отказа в обслуживании, ведь неопределенность слишком велика». Подобные заявления указывают на описанные выше ошибочные интерпретации измерений, которые не только не связаны с реальным принятием решений, но и ненаучны. Когда ученые, актуарии или статистики проводят измерения, они используют другое фактическое определение.

Определение измерений

В процессе принятия практических решений следует рассматривать измерения как *наблюдения, количественно уменьшающие неопределенность*. Простого уменьшения, не обязательно устранения неопределенности для измерений будет достаточно. Даже если некоторые ученые формулируют определение немного иначе, применяемые ими методы доказывают, что для них измерения также являются исключительно вероятностной задачей и твердой уверенности в реальных величинах у них, как правило, нет. Тот факт, что ошибки неизбежны, но их все равно можно считать прогрессом по сравнению с предыдущими данными, является важнейшим в методах проведения экспериментов, опросов и других научных измерений.

Практические различия между этим определением и наиболее популярной трактовкой измерений огромны. Прежде всего, верным измерениям, чтобы считаться таковыми, не нужно быть абсолютно точными. К тому же отсутствие зарегистрированной ошибки (подразумевающее, что число точное) может быть признаком того, что не применялись эмпирические методы, такие как выборка и эксперименты (т. е. на самом деле это вообще не измерения). Измерения, соответствующие основным стандартам научной достоверности, будут сообщать о результатах с некоторой долей неопределенности, например: «Существует 90 %-ная вероятность того, что атака на систему приведет к сбою в ее работе на период от 1 до 8 часов».

Определение измерения

Измерение – количественно выраженное уменьшение неопределенности на основе одного или нескольких наблюдений.

Такая концепция измерения может оказаться новой для многих читателей, но есть веские математические основания и практические причины для подобной трактовки. В конечном счете измерение – это лишь информация, а для информации существуют строгие теоретиче-

ские рамки. Область знания, получившая название «теория информации», была разработана в 1940-х годах Клодом Шенноном, американским инженером-электриком и математиком. В 1948 году он опубликовал работу под названием A Mathematical Theory of Communication[2] («Математическая теория коммуникации»), заложив в ней основы теории информации и, по сути, большей части информационных технологий, с которыми работают специалисты по кибербезопасности.

Шеннон предложил математическое определение информации как степени уменьшения неопределенности в сигнале, которую он рассматривал с точки зрения энтропии, устраняемой сигналом. По Шеннону, адресат информации находится в некотором изначальном состоянии неопределенности, иными словами, ему уже что-то известно, а новая информация просто устраняет хотя бы часть неопределенности (т. е. необязательно полностью). Изначальное состояние знания или неопределенности адресата можно использовать для вычисления, скажем, пределов объема информации, передаваемой сигналом, минимальной интенсивности сигнала с поправкой на шум, а также максимально возможного сжатия данных.

Такая концепция «снижения неопределенности» крайне важна для бизнеса. Продуктивность значимых решений, принимаемых в состоянии неопределенности (например, связанных с утверждением крупных IT-проектов или новых средств контроля безопасности), можно повысить, пусть даже совсем немного, за счет снижения неопределенности. Иногда даже небольшое снижение неопределенности может сберечь миллионы долларов.

Таксономия шкал измерения

Итак, измерения в области кибербезопасности похожи на любые другие в том смысле, что для них не нужна определенность. Различные типы измерительных шкал могут продвинуть наше понимание измерений еще дальше. Обычно мы думаем, что для измерений необходимы конкретные, строго определенные единицы, например доллары в год в бюджете кибербезопасности или минуты для определения продолжительности времени простоя системы.

А можно ли считать подходящей для измерений шкалу с градациями «высокий», «средний» и «низкий»? Специалистам по кибербезопасности часто встречаются подобные шкалы во многих стандартах и практиках во всех областях оценки риска. Такие величины, как «воздействие» или «вероятность», общепринято оценивать субъективно по шкале от 1 до 5, а затем комбинировать, чтобы определить степень риска как высокую, среднюю или низкую. Эти обманчиво простые методы поднимают целый ряд проблем, которые более подробно будут рассмотрены далее в этой книге. А пока давайте поговорим о том, в каких случаях имеет смысл использовать шкалы, отличные от общепринятых единиц измерения.

Обратите внимание, что в предлагаемом нами определении измерения говорится, что оно «выражено количественно». Неопределенность в любом случае следует выразить количественно, хотя объект наблюдения может быть вовсе не количественной величиной, а качественной, скажем, обозначать принадлежность к какому-либо множеству. Например, можно «измерить» что-то, ответив «да» или «нет» (допустим, произойдет ли в этом году утечка данных или будет ли предъявлен иск по киберстрахованию), и это все еще будет точно соответствовать нашему определению измерения. Однако степень неопределенности в отношении подобных наблюдений все равно должна быть выражена количественно, например: существует 15 %-ная вероятность утечки данных в этом году, существует вероятность 20 % предъявления иска по киберстрахованию и т. д.

Точка зрения, в соответствии с которой измерения применимы к вопросам с ответом «да/нет» и прочим качественным признакам, согласуется с другим признанным направлением научной мысли в области измерений. В 1946 году психолог Стэнли Смит Стивенс опубликовал

статью On the Theory of Scales and Measurement (Теория шкал и измерений)[3]. В ней описаны четыре различные шкалы измерения: номинальная, порядковая, интервальная и отношений. Если вы думаете о градусах Цельсия или долларах как единицах измерения, то вы используете интервальную шкалу и шкалу отношений соответственно. У обеих шкал есть четко определенная единица стандартной величины. В обоих случаях можно сказать, что 6 на 2 больше, чем 4 (6 градусов Цельсия или 6 долл.). Однако интервальная шкала не позволяет сказать, что 6 «на 50 % больше», чем 4, или «в два раза больше», чем 3. Например, 6 градусов Цельсия не «в два раза жарче», чем 3 градуса Цельсия (поскольку положение нуля на шкале Цельсия установлено произвольно в точке замерзания воды). А вот 6 млн долл. в два раза больше, чем 3 млн. То есть для интервальных шкал неактуальны некоторые математические вычисления, например умножение или деление.

Номинальные и порядковые шкалы еще более ограничены. У номинальной шкалы нет подразумеваемого порядка или величины, сюда можно отнести указание пола индивида, местоположения объекта или наличие у системы определенного признака. Номинальная шкала выражает состояние, не указывая, что одно состояние в два раза больше другого, или, если уж на то пошло, хотя бы просто больше или меньше оно относительно другого. Каждая шкала состояния – это просто *иное* состояние, не большее или меньшее. Порядковые шкалы, с другой стороны, ранжируют, но не сравнивают величины. Администратор обладает бóльшими правами, чем обычный пользователь, но при этом нельзя сказать, что его права в пять раз больше, чем у обычного пользователя, и в два раза больше, чем у другого пользователя. Поэтому большинство математических операций – кроме базовых логических или операций со множествами – неприменимы к номинальным или порядковым шкалам.

Тем не менее номинальные и порядковые шкалы могут быть информативными, даже несмотря на их отличия от более традиционных шкал измерения, таких как килограммы или секунды. Геологам полезно знать, что одна горная порода тверже другой, но не обязательно знать насколько. Метод, применяемый ими для сравнения твердости минералов, называется «шкала твердости Мооса», и используемая в нем шкала является порядковой.

Конец ознакомительного фрагмента.