УДК 004.056
ББК 32.973-018.2
Х12

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

Хаббард, Дуглас У.

Х12 Как оценить риски в кибербезопасности. Лучшие инструменты и практики / Дуглас У. Хаббард, Ричард Сирсен ; [перевод с английского М. А. Райтмана]. — Москва : Эксмо, 2023. — 464 с. — (КиберБез. Лучшие книги о безопасности в сети).

ISBN 978-5-04-166353-7

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.

УДК 004.056
ББК 32.973-018.2

ISBN 978-5-04-166353-7

Содержание

ЧАСТЬ III
УПРАВЛЕНИЕ РИСКАМИ КИБЕРБЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

ПРИЛОЖЕНИЯ

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.

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.

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»* (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,

---

* М.: Олимп-Бизнес, 2009.

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.

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