Путеводитель по карьере в кибербезопасности

Алисса Миллер

MANNING

Cybersecurity Career Guide

Alyssa Miller

Серия «Библиотека программиста»

Алисса Миллер

Путеводитель по карьере в кибербезопасности

Перевод с английского М. Райтмана

Электронное издание

Ростов-на-Дону
ФЕНИКС
2025

УДК 004.05
ББК 32.973-018.2
КТК 216
М60

© LICENSEE 2025. Authorized translation of the English edition 2022 Manning Publications.
This translation is published and sold by permission of Manning Publications,
the owner of all rights to publish and sell the same.

Миллер, Алисса.
М60 Путеводитель по карьере в кибербезопасности [Электронный ресурс]/ Алисса Миллер ; пер. с англ. М. Райтмана. — Электрон. текстовые дан. (1 файл pdf : 230 с.). —Ростов н/Д : Феникс, 2025. — (Библиотека программиста).

ISBN 978-5-222-43781-0

Книга предоставляет читателю широкий выбор профессий в кибербезопасности и помогает найти подходящую для себя. Автор, эксперт Алисса Миллер, делится 15-летним опытом работы в этой сфере и помогает читателям начать карьеру уверенно и успешно. Книга содержит практические советы, упражнения и методики для развития навыков.

УДК 004.05
ББК 32.973-018.2

Cybersecurity Career Guide
Text by Alyssa Miller
© М. Райтман, перевод, 2024
© ООО «Феникс», оформление, 2024

Содержание

Посвящение

Многочисленными навыками и опытом, приобретенными мной за прошедшие годы и сделавшими возможным написание этого руководства, я в немалой степени обязана трем замечательным руководителям, с которыми работала на протяжении своей карьеры. Итак, я посвящаю эту книгу следующим людям.

Тиму Патноду, который пошел на риск, приняв молодого голодного программиста без образования в свою команду разработчиков банковских продуктов. Тим, ты преподал мне первые уроки того, как быть вдохновляющим лидером, что оказало огромное влияние на развитие моей карьеры.

Донне Бомейстер, которая девять лет спустя рискнула нанять программиста, не имевшего опыта работы в области безопасности, и поставила меня во главе своей команды тестировщиков. Ваш чуткий, открытый, но уверенный стиль руководства научил меня быть лидером, пользующимся доверием команды и позволяющим ей стать истинной и мощной движущей силой прогресса.

И наконец, Патрику Флемингу, показавшему мне, каким должен быть лидер, который умеет вдохновлять и быть гибким так, чтобы команда достигала новых высот.

Благодарю вас троих за то, что вы помогли мне вырасти в профессиональном и личностном плане и стать тем, кто я есть сегодня. Я никогда не забуду то, что получила от каждого из вас.

Предисловие

Я выросла хакером. Я работаю с компьютерами всю жизнь и на протяжении почти двух десятилетий считаюсь профессионалом в области кибербезопасности. Эта сфера успела занять в моем сердце особое место, пока я находилась в хакерских сообществах 1990-х годов и создавала успешную карьеру.

Я наблюдала, как кибербезопасность постепенно превращалась из области, о которой практически никто не знал, из-за чего мне часто приходилось объяснять, чем я занимаюсь, в сферу, затрагивающую жизнь практически каждого жителя планеты. В результате она стала одним из самых обсуждаемых карьерных направлений не только в технологической индустрии, но и в обществе в целом.

Развитие технологий и их проникновение в нашу повседневность сопровождается резким ростом спроса на специалистов по кибербезопасности. В отраслевых и мейнстримных СМИ я часто читаю, что в этой сфере у людей наблюдается пробел в навыках. Согласно оценкам, от нескольких сотен тысяч до миллионов вакансий в этой сфере остаются незакрытыми. Тем не менее в разговорах с людьми, стремящимися выйти на этот рынок труда, я нередко узнаю о сложностях, с которыми они сталкиваются. Между тем, что говорят представители отрасли, и опытом соискателей существует некоторый диссонанс. Этот диссонанс я и постаралась устранить.

Я искала ответы с помощью опросов, интервью и других методов исследования. Моя цель заключалась в том, чтобы соискатели и компании, которые в них нуждаются, нашли друг друга. Написание этого руководства было одним из основных направлений моей деятельности, нацеленной на развитие нашего профессионального сообщества.

Оно призвано помочь людям, желающим построить карьеру в сфере кибербезопасности, определить, понять и преодолеть множество препятствий, стоящих у них на пути. Я надеюсь, что эта книга облегчит путь новым профессионалам, стремящимся обезопасить наш цифровой мир.

Благодарности

Книга, подобная этой, не могла появиться стараниями лишь одного человека. Поэтому я воспользуюсь моментом, чтобы сказать спасибо всем замечательным людям, благодаря которым она увидела свет.

Начну с Кейси Шуньяк, чья любовь, поддержка и идеи позволили сделать книгу значительно лучше. Именно усилиями Кейси, которая помогла мне справиться с потерей мотивации во время пандемии COVID-19, мой труд увидят те, кому он может принести пользу. Благодаря ее комментариям о содержании книги у меня появилось представление, как охватить более широкую аудиторию читателей. За это я выражаю ей глубокую признательность.

Также хочу поблагодарить многих представителей индустрии кибербезопасности, которые помогали мне в ходе интервью и исследований. Алет Денис, Каролина Террасас, Кирстен Реннер, Квадво Берджи, Кэтлин Смит, Габриэль Хемпель, Кинан Скелли, Митч Паркер и Лесли Кархарт — спасибо вам за ваши знания и мнения, нашедшие отражение на страницах этого руководства. Кроме того, я выражаю особую благодарность двум замечательным людям — Карлу Герцу и Рэю — за то, что они стали главными защитниками моей работы, делились своими соображениями, когда это было необходимо, и просто оказывали мне огромную поддержку.

Большое спасибо сотрудникам издательства Manning, которые помогли мне пройти через весь процесс написания книги: Карен Миллер, редактору — консультанту по аудитории; редактору-рецензенту Александру Драгосавлевичу; руководителю моего проекта Дейрдре Хайам; моему редактору Шерон Уилки и корректору Джейсону Эверетту.

Кроме того, хочу поблагодарить тысячи людей, которые участвовали в исследованиях, положивших начало написанию этой книги, и поделились неожиданными данными и умозаключениями. Ваша готовность делиться опытом позволила совершить целый ряд открытий, и я безмерно благодарна вам за то, что вы помогли мне помочь многим другим найти свой карьерный путь в сфере кибербезопасности. И наконец, спасибо десяткам тысяч членов нежно любимого мной профессионального сообщества, с которыми я имею возможность ежедневно взаимодействовать благодаря социальным сетям, мероприятиям и отраслевым СМИ. Именно оно вдохновляло меня при написании этого руководства, и я искренне ценю каждого из его участников.

В завершение выражаю признательность всем рецензентам. Алекс Саез, Аманда Деблер, Амит Ламба, Бьорн Нойхаус, Бобби Лин, Даниэль Варга, Дхивья Сивасубраманян, Дипен Н. Кумар, Элаварасу А. К., Эмануэль Ориджи, Джорджроберт Фриман, Харш Раваль, Хьюго Соуза, Ян Винтерберг, Джейсон Хейлз, Йорг Дишер, Марк Рулло, Мишель Ди Педе, Натан Дельбу, Пол Амманн, Рафик Наккаш, Роб Гольц, Стив Атчу и Зарак Махмуд, ваши предложения помогли значительно улучшить эту книгу.

Об этой книге

Эта книга поможет вам найти свой путь к тому, чтобы стать выдающимся специалистом по кибербезопасности. Вы получите четкие практические советы, созданные на основе независимых исследований и интервью с сотнями менеджеров по найму, — следуя этим советам, вы сможете войти в новую для себя сферу и быстро подняться по карьерной лестнице.

Для кого предназначена эта книга

Эта книга представляет собой исчерпывающее руководство, способное помочь любому человеку, желающему начать карьеру в области кибербезопасности. Она будет полезна людям из всех слоев общества, обладающим техническими навыками и знаниями любого уровня. Не имеет значения, хотите вы получить первую профессию или сменить ее: это руководство снабдит вас всеми необходимыми инструментами, чтобы вы начали свой карьерный путь и определились с долгосрочными планами, связанными с профессиональным развитием.

Структура книги

Руководство разделено на три части, каждая из которых состоит из трех глав. Первая часть дает общее представление о кибербезопасности. Вы узнаете, насколько эта сфера обширна и какие она предлагает карьерные пути. Здесь также обсуждаются многие проблемы и препятствия, с которыми вы можете столкнуться во время карьерного роста. Некоторые

из таких препятствий будут проиллюстрированы результатами исследований.

Вторая часть книги посвящена поиску работы. Здесь вы найдете практические упражнения, которые помогут вам выявить свои увлечения и интересы и понять, в каких направлениях кибербезопасности они могут пригодиться. Наша цель — найти правильную точку приложения усилий и повысить шансы на то, чтобы вы выбрали направление, лучше всего соответствующее вашим способностям. В этой части вы также узнаете, как структурировать процесс поиска работы, как составить резюме, подготовиться к собеседованию и успешно его пройти.

В последних трех главах, составляющих третью часть книги, пойдет речь о том, как настроиться на достижение долгосрочных карьерных целей в сфере кибербезопасности. Здесь представлены инструменты, которые позволят освоить и использовать сети профессиональных контактов и системы наставничества для продвижения по своему пути. Также вы получите мощные инструменты для преодоления синдрома самозванца — одного из наиболее разрушительных для карьеры факторов. В последней главе руководства вы научитесь ставить реалистичные цели и не сбиваться с пути, ведущего к новым достижениям, и таким образом из всех кусочков у вас сложится единая карьерная картина.

Дополнительные онлайн-ресурсы

Существует несколько онлайн-ресурсов для тех, кого интересует карьера в сфере кибербезопасности. Ниже перечислены три инструмента, которые помогут вам начать ее строить.

- *Cyber Career Pathways Tool* — инструмент, созданный в рамках Национальной инициативы по карьере и исследованиям в области кибербезопасности (NICCS) и размещенный на сайте Агентства по кибербезопасности и защите инфраструктуры США (CISA); он поможет изучить карту карьерных путей и выбрать свой маршрут (**https://niccs.cisa.gov/workforce-development/cyber-career-pathways**).
- *TryHackMe* — бесплатный образовательный сайт, предназначенный для того, чтобы специалисты в области кибербезопасности осваивали различные навыки через изучение небольших уроков и решение задач (**https://tryhackme.com**).
- *CompTIA Resource Center* — коллекция бесплатных образовательных ресурсов от Ассоциации производителей вычислительной техники (CompTIA), позволяющих узнать больше о сфере кибербезопасности и связанных с ней технологиях и областях (**www.comptia.org/resources**).

Об авторе

Хакер с детства, Алисса Миллер всегда питала страсть к технологиям и сфере безопасности. Она купила свой первый компьютер в 12 лет и быстро освоила методы взлома модемных коммуникаций и программного обеспечения. Карьеру начала с должности разработчика ПО, что позволило ей переключиться на сферу кибербезопасности, где она проработала около двух десятилетий. За эти годы она прошла путь от пентестера до главы службы безопасности, получив опыт работы в различных организациях.

К 30 годам Алисса уже занимала управленческие позиции. Будучи руководителем программы тестирования безопасности и управления уязвимостями в финансовой компании из списка Fortune 200, она узнала обо всех позитивных и негативных сторонах найма и развития специалистов по кибербезопасности. За годы работы в сфере консалтинга ей довелось подготовить целую группу консультантов по безопасности приложений. Сейчас, в должности исполнительного директора другой крупной компании, предоставляющей финансовые услуги, она снова применяет свой опыт в подготовке команд, внедряя практики обеспечения кибербезопасности в своем подразделении с оборотом в несколько миллиардов долларов.

Алисса — признанный и уважаемый специалист в сфере кибербезопасности. Она регулярно говорит о том, что сообщество должно не только развивать профессиональные дисциплины, но и повышать уровень подготовки специалистов. Алиссу часто приглашают выступать на международных мероприятиях и в СМИ, чтобы поделиться

результатами своих исследований с представителями деловых кругов и отраслевыми сообществами. Благодаря сочетанию технических знаний и лидерских навыков ей удается преодолеть разрыв между специалистами по безопасности и руководителями компаний.

Алисса стремится изменить подход к обеспечению безопасности современного образа жизни и сосредоточить внимание на защите конфиденциальности и укреплении доверия. Она убежденная активистка, и поддержка профессионального сообщества с ее стороны, среди прочего, проявляется в работе с различными отраслевыми некоммерческими организациями, участии в ряде конференций и членстве в нескольких сообществах руководителей.

Об иллюстрации на обложке

Обложку этой книги украшает изображение якута из коллекции Жака Грассе де Сен-Совёра, опубликованное в 1797 году. Каждая из его иллюстраций тщательно нарисована и раскрашена вручную.

В те дни место жительства, профессию и статус человека можно было легко определить по его одежде. Издательство Manning превозносит изобретательность и инициативность компьютерной индустрии, помещая на обложки тематических книг иллюстрации из подобных коллекций, демонстрирующие богатое разнообразие региональных культур прошлого.

Часть I

Карьерные направления в сфере кибербезопасности

Строить карьеру — задача непростая вне зависимости от того, ищете вы первую работу или хотите сменить вид деятельности. Популярность сферы кибербезопасности значительно возросла, и не только из-за того, что она важна для современного мира, но и из-за сформированного ею «горячего» рынка труда. Но что конкретно подразумевается под кибербезопасностью? Какие пути открыты для людей, желающих построить карьеру в этой области? Какие навыки им необходимы и как правильно подойти к выбору работы?

На все такие вопросы мы ответим в первых трех главах этой книги. В главе 1 вы найдете определение понятия «кибербезопасность» и познакомитесь с историей ее развития. Мы поговорим о роли, которую кибербезопасность играет в нашем мире, а также о некоторых доминирующих в ней идеологиях. В главе 2 вы получите более полное представление о разнообразии специальностей в этой сфере. Здесь мы также обсудим важнейшие отличительные качества профессионала. В главе 3 мы рассмотрим основные проблемы и препятствия, способные помешать человеку ступить на этот карьерный путь. Мы наметим типичные направления для карьерного роста и поговорим о навыках, которые вам могут потребоваться.

Итак, приготовьтесь: вам предстоит открыть для себя захватывающий, сложный и динамичный мир кибербезопасности. Прочитав первую часть, вы получите самое полное представление о пути, который вам предстоит пройти.

Глава 1
Что такое кибербезопасность

В этой главе

- Определение термина «кибербезопасность» и погружение в историю
- Роль кибербезопасности, ее ценности и идеология
- Важность разнообразия в развитии сферы кибербезопасности

Итак, вы хотите помочь защитить наш новый цифровой мир, построив карьеру в области кибербезопасности? Если вы уже изучали этот вопрос, то наверняка не раз слышали о так называемом разрыве в навыках. Вероятно, вы даже натыкались на результаты исследований, согласно которым количество незакрытых вакансий в области кибербезопасности может достигать четырех миллионов. А если вы ищете свою первую работу, то, скорее всего, потратите на ее поиск более шести месяцев.

Если вы заканчиваете обучение или хотите сменить профессию, то, вероятно, задавались вопросом вроде: «Как начать карьеру в кибербезопасности?» Поискав ответ, вы, скорее всего, с сожалением обнаружили, что его — единого и общепринятого — не существует.

За 15 лет работы в сфере кибербезопасности я наняла нескольких невероятно талантливых людей на их первые должности в этой области.

Я наблюдала, как созданные мной команды превращаются в мощные и эффективные группы специалистов. Тем не менее, несмотря на свои успехи в найме и развитии талантов, я не могу игнорировать неспособность профессионального сообщества указать четкий карьерный путь от начинающего специалиста до руководителя. Я не раз видела, как давно зарекомендовавшие себя профессионалы применяют неэффективные практики найма, дают плохие советы новичкам и чрезмерно их контролируют.

Но у меня есть для вас хорошая новость: вы приобрели эту книгу. На ее страницах я помогу вам понять уникальную природу того, что обычно называют *отраслью кибербезопасности*. Мы вместе совершим путешествие, начав с того, что дадим определение той сфере, частью которой вы хотите стать. Опираясь на интервью с представителями профессионального сообщества, я продемонстрирую, как не связанные на первый взгляд навыки и опыт могут оказаться полезными для карьеры в этой области. Вооружившись результатами опросов среди 1500 профессионалов и начинающих специалистов, я расскажу, как можно ускорить переход в эту сферу.

На протяжении всей книги я буду говорить о важности образования, сертификации и наставничества для получения работы. Я поделюсь мыслями о том, как интерпретировать объявления о вакансиях в сфере кибербезопасности, как анализировать и подчеркивать свой уникальный опыт, чтобы максимально эффективно позиционировать себя и повысить шансы на получение первой должности. Я дам вам представление о типах собеседований, которые обычно проводят в процессе найма, и поделюсь советами о том, как их проходить. Я также расскажу, как после устройства на работу успешно двигаться по выбранному карьерному пути.

Чтобы сделать первый шаг к должности в сфере кибербезопасности, необходимо понять, что такое кибербезопасность, какие здесь есть роли и как они проявляются в различных областях повседневной жизни.

1.1. Что такое кибербезопасность

Термин «кибербезопасность» встречается в современном обществе повсеместно. Эта тема ежедневно обсуждается в СМИ, политических и деловых кругах и так или иначе затрагивает жизнь большинства людей. Однако, несмотря на все это, мало кто может однозначно ответить на простой вопрос: а что же такое кибербезопасность?

Единого общепринятого определения не существует. Однако большинство людей согласятся, что кибербезопасность — это продолжение

того, что до сих пор часто называют *информационной безопасностью* (ИБ). В 1961 году исследователи из Массачусетского технологического института (МТИ) создали первую защищенную паролем С*истему разделения машинного времени* (CTSS, Compatible Time-Sharing System). Многие считают это событие моментом рождения информационной безопасности — практики защищать информацию и электронные системы от несанкционированного доступа.

Примерно десять лет спустя исследователи начали подключать компьютеры к сети ARPANET, созданной Агентством перспективных исследовательских проектов Министерства обороны США. Эта сеть была призвана обеспечить быстрый и надежный обмен данными между компьютерными сетями, раскинувшимися на обширных территориях. Именно сеть ARPANET легла в основу того, что сегодня называется интернетом.

Однако в 1988 году, за три года до того, как интернет стал общедоступным, исследователь Роберт Моррис решил подчеркнуть риски безопасности, которым подвергались исследовательские компьютеры в этой сети. Он разработал программу, способную распространяться по системам, подключенным к интернету. Используя бреши в безопасности ОС UNIX, она устанавливалась на компьютеры и создавала собственные копии. Таким образом Моррис создал первого интернет-червя. К несчастью, этот червь вышел из-под контроля и сделал зараженные системы непригодными для использования. В результате Моррис стал первым человеком, осужденным за уголовное преступление в соответствии с Законом о мошенничестве и злоупотреблениях с использованием компьютеров, принятым в 1986 году, а также была создана *Группа реагирования на инциденты информационной безопасности* (CERT, Computer Emergency Response Team) в Университете Карнеги — Меллона при финансовой поддержке федерального правительства США.

Создание CERT можно считать моментом рождения того, что сегодня называется кибербезопасностью. Таким образом, *кибербезопасность* — это совокупность исследований, технологий и практик, используемых для защиты взаимосвязанных технологических систем, данных и пользователей от атак, несанкционированного доступа и/или повреждения.

1.2. Роль кибербезопасности

Цели кибербезопасности зависят от контекста, в котором применяются соответствующие практики. В СМИ под кибербезопасностью часто понимают защиту бизнеса от атак со стороны киберпреступников. Однако в медиа нередко обсуждается и ее роль в функционировании общества

в целом. Сфера кибербезопасности охватывает все аспекты жизни людей, начиная с защиты системы выборов и обеспечения национальной/международной безопасности и заканчивая охраной частной жизни пользователей интернета.

Чтобы осознать ее масштаб, надо сперва понять, как кибербезопасность встроена в различные грани нашей жизни. Из-за того, что она столь глубоко укоренена во всем, что мы делаем, многие воспринимают ее как должное или вовсе игнорируют. Прежде чем обсуждать направления и специализации, существующие в этой сфере, давайте подробно рассмотрим, какие роли она играет в различных контекстах.

1.2.1. Кибербезопасность в деловом мире

Под кибербезопасностью коммерческих организаций обычно понимается защита финансовых интересов компаний. Организации функционируют в рамках модели *активов* (элементов бизнеса — носителей или источников финансовой стоимости) и *обязательств* (элементов, которые уменьшают финансовую стоимость активов или создают такой риск).

Чтобы расширить свои возможности, в середине двадцатого века предприятия начали применять так называемые *информационные технологии* (ИТ), предполагающие использование цифровых систем — компьютеров — для управления информационными активами бизнеса. По мере развития ИТ-систем, которое на протяжении последнего десятилетия было особенно бурным, все больше и больше бизнес-активов становится частью цифровой сферы.

Явление, связанное с оцифровкой предприятиями своих критически важных активов и возрастающей ролью ИТ-систем, стали описывать новым термином — «цифровая трансформация». Например, медицинские записи, которые раньше хранились на бумажных носителях или на пленке, теперь все чаще переносят в системы *электронных медицинских карт* (EMR-системы). Хранение всей этой информации в цифровом виде делает ее более доступной для ознакомления и совместного использования. Фактически вокруг этой цифровой трансформации сформировался целый рынок ИТ-продуктов и услуг, помогающих организациям осуществлять ее практически в любой отрасли, начиная со здравоохранения и заканчивая образованием и транспортом.

Со временем предприятия переносят в цифровую сферу все больше активов, и с этим возрастает риск атак со стороны киберпреступников: попыток украсть данные или сделать системы недоступными для использования. Информационные активы, некогда защищенные от подобных атак, с перемещением в цифровую сферу подвергаются риску,

причем его источник может находиться в любой точке мира. Возможность подключаться к системе и оперативно получать доступ к данным, а также взаимодействовать с ними через интернет спровоцировала не только взрывной рост количества цифровых активов, но и появление новых угроз, которым они подвергаются.

Технологии, практики и ресурсы кибербезопасности, в свою очередь, позволяют минимизировать риски, связанные с этими угрозами. Таким образом, основная задача кибербезопасности в области бизнеса — защищать постоянно растущую сферу цифровых активов.

В основе деятельности предприятий лежат модели управления рисками. Руководители больших и малых компаний всегда взвешивают риски, ассоциируемые с тем или иным событием или изменением условий, а затем пытаются свести их к минимуму. Например, такая организация, как Facebook[1], может сопоставить потенциальный доход от продажи пользовательских данных с потенциальной ответственностью за нарушение законов о конфиденциальности. Кроме того, бизнес и его руководители должны сопоставлять потенциальные затраты, связанные с реализацией угроз, с затратами на снижение соответствующего риска. Эти сложные компромиссы определяют финансовые решения и другие организационные стратегии. Поскольку сфера цифровых активов постоянно расширяется, неудивительно, что кибербезопасность играет все большую роль в анализе рисков.

Таким образом, кибербезопасность становится все более важным элементом управления рисками в организации. К специалистам по кибербезопасности часто обращаются за оценкой уровня риска, которому подвергается конкретный бизнес-актив. Поэтому обязанности соответствующих групп уже не ограничиваются технологическими рамками. Сотрудники службы безопасности должны понимать ландшафт угроз, куда входят государства, хактивисты, внутренние источники опасности и так далее, и доносить их характеристики до сотрудников других подразделений, не обладающих такими же широкими техническими знаниями. Требуется также, чтобы специалисты по кибербезопасности понимали важность того или иного актива для бизнеса в целом и могли максимально точно описывать риски, которым он подвергается.

Поскольку ИТ-системы стали неотъемлемой частью бизнес-модели, их важность для делового мира существенно возросла. Сбой в работе системы, из-за чего она оказалась недоступной для использования, может сильно повлиять на бизнес. Подумайте о крупнейших розничных сетях и о том, какие убытки они понесут, если их кассовые системы

[1] Принадлежит компании Meta Platforms, Inc., признана экстремистской, ее деятельность на территории России запрещена. — *Прим. ред.*

перестанут работать хотя бы на полчаса. От надежности ИТ-систем сегодня зависит работа медицинских и финансовых учреждений, логистических компаний и представителей практически всех остальных отраслей.

Учитывая, что многие из этих критически важных систем взаимосвязанные, кибербезопасность играет важную роль в обеспечении их доступности и стабильности работы. Злоумышленники, стремящиеся нанести организации ущерб, могут осуществить атаку типа *отказ в обслуживании* (DoS-атаку) в попытке сделать корпоративные системы недоступными на определенный период. Предотвращать успешное выполнение подобного рода атак — лишь одна из многочисленных обязанностей специалистов по кибербезопасности.

Как правило, такие защитные практики применяются в рамках работы команд, отвечающих за стабильное функционирование систем. В сфере ИТ такие группы обычно называют *оперативными*. Команды, которые отвечают за повседневное функционирование средств защиты, называются *оперативными группами по обеспечению кибербезопасности*.

Примеры повседневных задач специалиста по кибербезопасности

- Мониторинг атак на различные системы.
- Реагирование на успешные атаки, нарушающие целостность системы или систем.
- Проверка систем и людей на предмет наличия *уязвимостей* (слабых мест с точки зрения безопасности).
- Отслеживание, проверка и создание отчетов об устранении этих уязвимостей.
- Взаимодействие с разработчиками по вопросам создания безопасного программного обеспечения.
- Разработка и развертывание средств обеспечения безопасности (также известных как *средства контроля*).
- Взаимодействие с руководителями по вопросам выделения бюджетных средств на обеспечение безопасности.
- Предоставление аудиторам свидетельств применения средств контроля безопасности.
- Поддержание работы различных систем безопасности (учетных записей пользователей, брандмауэров и так далее).

По мере усиления зависимости бизнес-моделей от цифровых активов и ИТ-систем все ярче проявляется еще одна тенденция. С головокружительной скоростью растет уровень жесткости государственного

регулирования и отраслевых требований в отношении использования ИТ-систем. Многие из правил и требований касаются того, как организации защищают свои системы, реагируют на утечки или раскрытие данных и защищают конфиденциальность потребителей.

Так что на сотрудниках службы безопасности лежит львиная доля ответственности за то, чтобы компания в работе достигла соответствия всем требованиям и стандартам, поддерживала его и могла это соответствие подтвердить. Начнем с того, что им часто приходится интерпретировать смысл этих требований. Притом они могут сотрудничать с другими подразделениями, например с юридическим отделом, командой по управлению рисками или аудиторской группой, однако знания и опыт, которыми обладают специалисты по кибербезопасности, играют в процессе решающую роль.

Затем с помощью этого опыта и знаний разрабатываются и внедряются необходимые средства контроля, которые в итоге должны обеспечить соответствие организации предъявляемым требованиям. Эти средства принимают форму процессов, практик, политик и технологий, призванных в необходимой степени защитить данные и системы организации.

По тому, какое значение имеет кибербезопасность в деловой среде, можно сделать вывод, что сотрудники соответствующих служб вовлечены практически во все аспекты бизнеса. Если традиционные группы специалистов по информационной безопасности могли сосредоточиться исключительно на технических средствах контроля доступа и мерах противодействия, современный цифровой мир сделал специалистов по кибербезопасности частью всех деловых взаимодействий.

1.2.2. Кибербезопасность на страже общественного порядка

С переходом от делового мира к обществу в целом фокус специалистов по кибербезопасности смещается. Кибербезопасность стала неотъемлемой частью не только бизнес-среды, но и повседневной жизни. Функционирование правительства, системы национальной безопасности, правоохранительных органов и даже межличностные взаимодействия — все это в двадцать первом веке неразрывно связано с цифровой сферой.

Сегодня правительство на всех уровнях очень сильно зависит от компьютерных и мобильных приложений, цифровых данных и других технологических возможностей, ставших частью цифрового мира. Чтобы сомнения в важности ИТ-систем для повседневной работы властей развеялись, достаточно вспомнить о *программах-вымогателях* — вредоносном

программном обеспечении, которое, будучи установленным на компьютер жертвы, делает данные на нем недоступными до тех пор, пока злоумышленникам не выплатят выкуп.

Одна из наиболее громких атак на местное правительство произошла в мае 2019 года в Балтиморе, штат Мэриленд. Работа части городских органов власти оказалась парализована более чем на месяц из-за того, что электронная почта, платежные и некоторые другие системы внезапно стали недоступны. Общая сумма неполученных доходов и затрат на восстановление была оценена в 18 миллионов долларов. Аналогичным атакам подвергались многие другие федеральные, региональные и местные органы власти по всему миру.

Разумеется, ИТ-системы отвечают не только за повседневное функционирование правительств. Сейчас все шире распространяются электронные системы для проведения голосования. Поскольку общественность требует подсчитывать результаты выборов еще быстрее и точнее, власти США и других стран активно внедряют цифровые терминалы для голосования. Однако эти терминалы также подвергаются атакам. Проблемы с безопасностью и попытки взлома были выявлены во время прошлых выборов, в частности при выборах президента США в 2016 и 2020 годах. Впрочем, Агентство по кибербезопасности и защите инфраструктуры США и независимые фирмы пришли к выводу, что благодаря усилиям специалистов ни одна из таких попыток не увенчалась успехом.

Государственные учреждения регулярно обращаются к специалистам и исследователям в области кибербезопасности за помощью в защите от атак, поскольку ставки слишком высоки. Ни один аспект деятельности правительства нельзя назвать низкорисковым с точки зрения подверженности кибератакам. Даже атаки на парки, музеи и другие учреждения в государственном ведении могут спровоцировать быструю и мощную негативную реакцию со стороны общественности. Ни один политик не хочет, чтобы его имя было связано с кибератакой, имевшей место в сфере его ответственности. Таким образом, укрепление безопасности государственных учреждений требует согласованных усилий, которые многие специалисты назвали бы запоздалыми.

Однако эта проблема касается не только гражданского правительства. Военные во всем мире тоже становятся все более зависимыми от технологических систем в том, что касается защиты стран своих и союзных. Сетевые технологии теперь присутствуют везде, от боевой техники до средств связи и мониторинга. В военной сфере кибербезопасность играет буквально жизненно важную роль. По мере внедрения новых технологий правительства и их подрядчики все чаще обращаются к исследователям и специалистам по кибербезопасности за помощью

в обеспечении защиты этих систем от атак, начиная с этапа проектирования и заканчивая их применением в полевых условиях.

Работа правоохранительной системы внутри страны — естественное продолжение военной деятельности государства. Сегодня многие ее аспекты, от патрулирования улиц и проведения расследований до функционирования уголовного правосудия, зависят от применения компьютеров и других подключенных к интернету электронных устройств. Атаки на них рискуют пагубно отразиться на соответствующих учреждениях и сделать невозможным соблюдение законов и судебное преследование нарушителей. Наше общество становится все более взаимосвязанным, и все чаще преступления совершаются с использованием электронных устройств. Квалифицированные специалисты по кибербезопасности, способные не только защитить системы того или иного учреждения, но и помочь в расследовании преступлений, чрезвычайно нужны.

Наконец, нельзя не отметить, что сетевые технологии пронизывают повседневную жизнь большинства жителей планеты, которые уже не представляют своего существования без социальных сетей, электронных коммуникаций, мобильных приложений и так называемых умных устройств. Все это — потенциальные цели для киберпреступников. Многие пользователи не знают, как безопасно использовать такие технологии и как их защитить от атак. Исследователи и специалисты в сфере кибербезопасности могут помочь решить и эту проблему, например, повышая осведомленность людей, разрабатывая и внедряя контрмеры или выявляя уязвимости в бытовой электронике и программном обеспечении.

1.3. Культура кибербезопасности

На протяжении нескольких десятилетий росло и развивалось сообщество людей, разделяющих идеи деконструкции, исследования и защиты технологий. Здесь сложилась своя культура и множество субкультур — они вместе сильно повлияли на то, как сейчас выглядит сфера кибербезопасности, и сформировали уникальный набор норм и ценностей, которых придерживаются представители сообщества: начиная с хакеров и исследователей и заканчивая специалистами по корпоративной безопасности.

Перечислить все ценности и идеологии сообщества нереально. И не только потому, что их слишком много или они в некотором роде бесплотны, но и потому, что общепринятых среди них нет. Впрочем, существует несколько доминирующих ценностей, которые следует усвоить любому человеку, желающему стать частью этого сообщества.

1.3.1. Неприкосновенность частной жизни и свобода

Личная свобода и неприкосновенность частной жизни — важнейшие элементы идеологии тех, кто занимается информационной безопасностью. В период зарождения хакерской культуры люди со всего мира общались через коммутируемые телефонные сети и так называемые *электронные доски объявлений* (bulletin board systems, или BBS). Чтобы получить доступ к такой системе, участникам приходилось доказывать, что они что-то «взломали».

Это часто предполагало демонстрацию данных компании, чью систему они взломали, или своей способности управлять чужими технологиями и заставлять их работать не так, как изначально задумывалось. Поскольку эти действия считались незаконными, очень высоко ценилось умение хакера сохранять анонимность и не привлекать внимания правительств и официальных лиц.

Большинство членов таких ранних сообществ в повседневной жизни были изгоями, а здесь обретали единомышленников. В сообществе не имели значения пол, этническая принадлежность, социальный статус и другие признаки, по которым людей часто дискриминировали в обществе. Вместо этого каждого участника оценивали исключительно по его знаниям и навыкам. Они могли вести содержательные дискуссии на интересующие их темы с людьми со схожими увлечениями, не опасаясь, что этому помешают какие-либо стереотипы или предубеждения.

По мере развития интернет-технологий к анонимности прибавилась возможность удобнее подключаться к обширным сообществам единомышленников. Однако скрытная и часто подпольная природа ранних хакерских групп начала постепенно меняться. Они становились все более заметными широкой публике, которую все сильнее интересовала их деятельность.

В то же время, как уже говорилось, в корпорациях и государственных учреждениях развивались идеи и практики, связанные с обеспечением информационной безопасности. Промышленность, правоохранительные и правительственные органы, занимавшиеся ИБ, начали формировать собственные профессиональные сообщества.

Постепенно между этими двумя очень разными группами установились хрупкие и слегка натянутые отношения. В ходе встреч и конференций по безопасности их члены обменивались информацией ради общей цели: сделать технологии лучше и безопаснее для всех. Но представления о том, что именно делает технологию «лучше», зачастую все еще разделяют эти группы.

Из-за этого они до сих пор не доверяют друг другу, а иногда и откровенно враждуют. В результате защита конфиденциальности и свободы стала главной ценностью, особенно среди наиболее идеалистически

настроенных хакеров и исследователей. До сих пор многие участники этого сообщества используют *псевдонимы*, чтобы защитить тайну своей личности и сохранить анонимность.

1.3.2. Открытый обмен информацией

Одним из ключевых факторов, благодаря которому сплотились первые хакеры, стала возможность *свободно обмениваться информацией*. Это не те киберпреступники, о которых мы слышим сегодня; это люди, стремившиеся лучше разобраться в технологии, чтобы потом ее можно было усовершенствовать. Однако обмен информацией иногда сопровождался выражением изрядной доли высокомерия. Тот, кто хвастался успешными взломами, пользовался наибольшим доверием в сообществе. И все же возможность делиться информацией и использовать чужие открытия была и остается важной ценностью сообщества.

Это характерно не только для хакерской культуры. Ученые уже давно признали важность открытого обмена информацией, что отразилось в исследованиях, посвященных кибербезопасности.

Культура обмена информацией с целью улучшить технологию ради всеобщего блага, в частности, проявляется в количестве ежегодных независимых конференций по информационной безопасности. Сегодня по всему миру организуются тысячи конференций, где обсуждают уязвимости, средства защиты и другие темы. Каждый год в августе в Лас-Вегасе проходит недельная серия конференций, которая неофициально называется «*Летним лагерем для хакеров*» и привлекает от 30 000 до 40 000 человек со всего мира.

Важность этой идеологии для сообщества выражается в том, как его члены реагируют на коммерциализацию интернета. На начальных этапах казалось, что интернет позволит свободно обмениваться знаниями в невиданном прежде масштабе. Какое-то время так и было. Тем не менее, компании быстро осознали, что с его помощью могут создать дополнительные источники прибыли и взаимодействовать с клиентами принципиально новым способом.

Чтобы защитить свои конкурентные преимущества и создать новые рынки, предприятия делали свои достижения в интернет-сфере корпоративной тайной. Новые технологии, обеспечивавшие большую секретность и защиту прав на интеллектуальную собственность, не соответствовали идеологии открытого обмена информацией. Сообщество безопасности, в свою очередь, постоянно боролось за то, чтобы разрушить эти барьеры и добиться от компаний большей прозрачности в том, что касалось их деятельности в интернете.

1.3.3. Не навреди

Первые хакеры быстро поняли, что способны помочь в улучшении технологии ради всеобщего блага. Обнаружив уязвимости в системах, они пытались сообщить об этом их владельцам. К сожалению, владельцы и правоохранительные органы рассматривали деятельность хакеров скорее как преступную, нежели как полезную.

Однако постепенно предприятия и даже правоохранительные органы начали осознавать, что знания и навыки дружественных хакеров позволят им защититься от настоящих злоумышленников. Так появился термин «этичный хакер» — человек, который использует методы взлома, чтобы находить уязвимости, и сообщает о них с целью их устранения. Несмотря на то, что термин утратил популярность, сама концепция все еще жива.

Чтобы такая деятельность оставалась в рамках закона, необходимо было тщательно продумать и соблюдать принципы этичного взлома. В результате «хорошие» хакеры разработали правила, методы и стандарты, которые отличали их от злоумышленников. В основе их этического кодекса лежит принцип «не навреди». Эти правила участия в тестировании систем гарантируют, что обнаруженные уязвимости не будут использованы для причинения ущерба системе или человеку.

Сейчас в сфере кибербезопасности этот принцип остается актуальным и применяется ко многим видам деятельности, которыми ежедневно занимаются исследователи, хакеры и специалисты-практики. А вот вредоносная деятельность во имя защиты, основанная на идеях наступательной кибербезопасности и кибервойн, провоцирует бурные дебаты.

1.4. «Отрасль» кибербезопасности

В деловом мире, в средствах массовой информации и в политическом дискурсе термином «отрасль кибербезопасности» часто описывается совокупность людей, технологий и практик, связанных с защитой цифрового мира. С момента, когда появились ИБ-специалисты, она рассматривалась как отдельная дисциплина.

У нас есть концепция *карьеры в сфере кибербезопасности* — вероятно, потому вы и читаете эту книгу. Правительства, корпорации и другие организации создают *группы по кибербезопасности*. Производители программного и аппаратного обеспечения выпускают *продукты для обеспечения кибербезопасности*, призванные защитить нас от всех мыслимых типов атак. Однако далеко не все уверены, что кибербезопасность следует рассматривать как отдельную отрасль.

1.4.1. Кибербезопасность — отдельная отрасль?

Сфера кибербезопасности представляет собой огромный коммерческий рынок. Согласно ряду исследований, в 2019 году во всем мире на решения, направленные на обеспечение кибербезопасности, было потрачено от 170 до 250 миллиардов долларов США. Кроме того, этой тематике посвящены курсы в колледжах, университетах и других учебных заведениях. На протяжении многих лет, пока группы ИБ-специалистов стояли особняком в корпоративных организационных структурах, рассматривать кибербезопасность в качестве отрасли было удобно и имело смысл.

Однако эта сфера давно вышла за рамки простой защиты ИТ-систем от несанкционированного доступа и повреждения. Внедрение соответствующих практик больше не ограничивается одним лишь применением технических контрмер. Сейчас на безопасность обращают внимание все сферы бизнеса, международных отношений и жизни общества. Называя кибербезопасность *отраслью*, мы подразумеваем, что она автономна, существует сама по себе и просто взаимодействует с другими аспектами нашей реальности. Это не отражает того факта, что безопасность — фундаментальная концепция, имеющая отношение к каждой части цифрового мира.

> **Определение.** Кибербезопасность — это больше, чем отрасль. Важно понимать, что она тесно связана со всеми аспектами цифрового мира. Таким образом, говорить о ней как об *отрасли* — значит поддерживать устаревшее представление о кибербезопасности как об обособленной функции организации и общества в целом.

1.4.2. Последствия цифровой трансформации

Как говорилось в разделе 1.2, в результате цифровой трансформации многие элементы повседневности перешли в электронную и цифровую сферу. Технологии больше нельзя назвать всего лишь частью нашей жизни; как сказала моя коллега и хорошая подруга Керен Элазари, это *и есть* наша жизнь. Теперь мы не просто защищаем системы, технологии и данные, мы защищаем фундаментальные аспекты современного мира.

Цифровая трансформация продолжается: все больше и больше некогда материальных объектов вокруг нас оцифровывается, — и кибербезопасность становится неотъемлемой частью нового мира. Количество и степень серьезности угроз растут в геометрической прогрессии. Ни одна группа, ни одна дисциплина и ни одна область знаний

не в состоянии предоставить нам защиту от всего: слишком разнообразны и обширны векторы атак.

1.4.3. Человеческий фактор

Цифровой мир растет за счет преобразования всего, что мы знаем, в данные и системы, так что на первый план вышла еще одна ключевая концепция: необходимость учета *человеческого фактора*. В ИБ-сообществе распространена идея о том, что чаще всего человек — самое слабое звено в защите. Как бы она ни была надежна, как бы ни были хороши технологии, человеку достаточно допустить единственную ошибку, чтобы злоумышленник успешно реализовал атаку.

В результате развития этой концепции появились эксперты по социальной инженерии. Организации нанимают таких специалистов, чтобы оценить готовность персонала к отражению атак. Ключевыми элементами соответствующих стратегий стали эксперты по человеческому поведению и информационной подготовке. Они помогают людям изменить привычный способ реагирования на такие методы социальной инженерии, как фишинг, телефонное мошенничество и манипуляции в ходе личного общения. В 2020 году конференция RSA (одна из крупнейших и старейших конференций по кибербезопасности) выбрала «Человеческий фактор» в качестве главной темы для своего ежегодного недельного мероприятия в Сан-Франциско.

Понимание важности человеческого фактора еще больше расширяет представление о том, что такое кибербезопасность. На практике специалисты начинают учитывать не только технологии, но и вшитые в нас поведенческие модели, методы манипулирования, а также разрабатывают меры противодействия дезинформации.

1.4.4. Интернет всего

То, насколько цифровая трансформация изменила нашу картину мира, нам еще только предстоит осознать. Возьмем, к примеру, *интернет вещей* (IoT, Internet of Things) — в современном понимании сеть *умных устройств*. Оба термина описывают продукты и технологии, которые до этого работали автономно, а теперь благодаря связи друг с другом обретают новые формы функциональности.

Современные холодильники способны определить, какие продукты заканчиваются, и заказать необходимое в интернет-магазине. Автомобили подключаются к сети с самыми разными целями, начиная

с использования навигаторов и заканчивая вызовом помощи. В феврале 2020 года на платформе Kickstarter была запущена кампания по сбору средств для создания свечи, которую можно зажигать удаленно через приложения на смартфоне. Кажется, что к интернету подключено уже все на свете.

В то же время взрывной рост числа подключенных к интернету устройств, как и следовало ожидать, сопровождался взрывным же ростом числа угроз и векторов атак. Кибербезопасности теперь уделяют внимание даже в тех технологиях, для которых раньше не существовало цифровых угроз. Вот и еще одно свидетельство того, что эта сфера проникает во все аспекты нашей жизни.

Итак, можем ли мы по-прежнему называть кибербезопасность отраслью? Не стоит ли вместо этого рассматривать ее как часть каждого аспекта нашего мира — так же как просто безопасность была частью жизни наших предков на протяжении всей истории? Да, есть люди, которые специализируются на разработке безопасной среды. Существуют лучшие практики, создаются стандарты и соблюдаются правила. Но, в конце концов, безопасность — неотъемлемая характеристика всего, от рабочих мест до зданий и дорог. Возможно, рассуждая о карьерных путях и специализациях в этой сфере, нам стоит думать о кибербезопасности в таком же ключе.

1.4.5. Так что, кибербезопасность — это отрасль?

Как видите, область кибербезопасности обширна и охватывает не только постоянно расширяющийся мир технологий, но и общие вопросы безопасности людей. Практически все аспекты нашей деятельности теперь прочно связаны с цифровой средой.

Таким образом, применительно к кибербезопасности понятие «отрасль» оказывается слишком ограничивающим. Теперь это важнейший элемент нашего образа жизни, а не то, что можно легко от него отделить. В отличие от информационной безопасности, которую в прошлом иногда рассматривали как ИТ-дисциплину, кибербезопасность — не просто набор конкретных навыков и практик, а нечто более концептуальное.

1.5. Важность человеческого разнообразия в сфере кибербезопасности

В разделе 1.4.3 мы говорили о человеческом факторе и о том, что человеческие ошибки могут свести на нет все усилия, которые мы

прикладываем, чтобы сохранить наш образ жизни с помощью технических средств. Поэтому при решении проблем, связанных с кибербезопасностью, мы должны принимать в расчет тех, кого стремимся защитить. Но как же нам защитить всех жителей мира — с разной культурой, разными идеалами, уровнем образования и способностями?

Оказывается, в этом направлении важно сделать один большой шаг: создать разнообразие среди людей, которые создают средства защиты. Обеспечить безопасность нашему цифровому образу жизни поможет разнообразие мыслей, точек зрения и идей, помогающих в решении проблем. Кроме того, необходимо выявить особенности групп, которые мы пытаемся защитить.

Ничего из этого не получится достичь, если у всех членов команд будет одинаковый опыт, образование, схожая культура и карьерный путь. Чтобы кибербезопасность работала, надо приветствовать привлечение специалистов, имеющих столь же разнообразный жизненный опыт, что и другие члены нашего общества, и даже специально их искать. Это означает, что в сфере кибербезопасности есть место для каждого. Более того, мы в этом нуждаемся — чтобы у нас работало как можно больше представителей различных групп.

1.5.1. Недостаток разнообразия в сфере кибербезопасности

В своем «Отчете о разнообразии и инклюзивности»[2] за 2020 год (Diversity and Inclusion Report) компания Synack представила результаты опроса сотен специалистов об их опыте работы в сфере кибербезопасности. Респондентов спрашивали, считают ли они, что им были предоставлены такие же возможности для карьерного роста, как и представителям других полов или этнических групп. 34% участников женского пола ответили на такой вопрос отрицательно. Еще более тревожен (53%) показатель представителей этнических меньшинств. Эти результаты свидетельствуют о проблеме недостаточного разнообразия, которая годами существует в технологической отрасли, особенно в сфере кибербезопасности.

В 2017 году Международный консорциум по сертификации в области безопасности информационных систем, или (ISC)², совместно с компанией Frost & Sullivan опубликовал результаты «Глобального исследования рабочей силы в области информационной безопасности»[3] (Global Information Security Workforce Study). Этот опрос показал, что

---

[2] http://mng.bz/PW92. — *Прим. авт.*

[3] http://mng.bz/J1Op. — *Прим. авт.*

в Северной Америке доля женщин-респондентов составляет всего 14%. В остальных регионах планеты показатель был еще меньше. Недостаточной представленности женщин в сфере кибербезопасности уделяется большое внимание в СМИ и различных исследованиях, но проблема до сих пор не решена. Согласно результатам того же опроса, лишь 23% респондентов из США идентифицировали себя как представители этнических меньшинств, что также не соответствует их общей доле в населении страны. Например, темнокожими или афроамериканцами считают себя 13,4% населения, а в опросе таких всего 9%.

Этот разрыв часто объясняют противоречивыми причинами. В своей книге я не стану обсуждать достоинства этих теорий. Важно лишь понимать, что недостаток разнообразия, в частности гендерного, действительно существует, и от его устранения во многом зависит успех наших начинаний. К счастью, проблема была признана, и наше сообщество уже работает над ее решением.

1.5.2. Почему это важно

Обеспечение разнообразия — это не просто дань политкорректности. Мир технологий и кибербезопасности постепенно осознает ценность разнообразия, которая лежит в плоскости не только морали и справедливости. Как я уже говорила в начале раздела, нам нужны специалисты, понимающие особенности мышления тех, кого мы пытаемся защитить, учитывая к тому же важность человеческого фактора. Такая способность позволяет находить более правильные решения.

Например, в 2014 году Счетная палата США опубликовала отчет[4], где говорилось, что участились случаи ложных срабатываний сканеров тела, установленных в аэропортах по требованию Администрации транспортной безопасности. Часто ложные срабатывания ассоциировались с головными уборами, тюрбанами и париками. В 2017 году организация ProPublica сообщила[5], что уровень ложных срабатываний у сканеров, особенно часто связанных с прическами, распространенными среди афроамериканок и темнокожих женщин, по-прежнему высок. Такие выводы были основаны на результатах независимого исследования, проведенного этой организацией.

Это заставляет задуматься: почему подобные сложности не выявляли раньше? Неужели «цветные» женщины не участвовали в разработке и тестировании устройств? Если бы состав проектной группы оказался

[4] https://www.gao.gov/assets/gao-14-357.pdf. — *Прим. авт.*

[5] http://mng.bz/wnd7. — *Прим. авт.*

более разнообразным, удалось бы предотвратить появление таких проблем, обойти их еще на начальном этапе? Ведь именно в этом заключается важность разнообразия. Процессы мозгового штурма и решения проблем более эффективны, когда их участники обладают разнообразными взглядами и опытом, на которые можно опереться. Поэтому для успешного решения проблем в сфере кибербезопасности нам следует обеспечить максимальное разнообразие внутри нашего сообщества.

1.5.3. Какое отношение это имеет к вашей карьере

Хотя это кажется проблемой сообщества и отрасли в целом, вам, как человеку, желающему построить карьеру в сфере кибербезопасности, важно понимать, что она в принципе существует. В главах 8 и 9 мы поговорим о том, что может сдерживать ваш карьерный рост. Об этой же конкретной трудности необходимо узнать на раннем этапе, когда у вас только начинает складываться представление о составе сообщества кибербезопасности, истории его развития и перспективах.

В самом начале карьерного пути, побудившего взять в руки эту книгу, вам может оказаться трудно найти свое место в сообществе, если вы не увидите среди его участников тех, с кем будете себя ассоциировать. В этот момент вспомните, о чем шла речь в этом разделе, и поймите: вам здесь не просто рады — в вас здесь нуждаются. В следующей главе мы подробно рассмотрим направления в сфере кибербезопасности, в которых вы можете найти себя.

ПОДВЕДЕНИЕ ИТОГОВ

- Кибербезопасность — это совокупность исследований, технологий и практик, используемых для защиты взаимосвязанных технологических систем, данных и пользователей от атак, несанкционированного доступа и/или повреждения.
- Цели кибербезопасности зависят от контекста, однако в цифровом мире взаимосвязанных систем все они сводятся к защите нашего образа жизни.
- Сфера кибербезопасности может существенно выиграть от разнообразия опыта и культур, и сообщество уже работает над тем, чтобы устранить недостаток в этом разнообразии.

Глава 2
Карьерные возможности в сфере кибербезопасности

В этой главе

- Разнообразные направления в сфере кибербезопасности
- Особенности специалистов по кибербезопасности, работающих в разных направлениях
- Отличительные качества хорошего специалиста по кибербезопасности

В главе 1 мы говорили о том, что такое кибербезопасность и для чего она нужна. Теперь пришло время копнуть чуть глубже и рассмотреть различные карьерные направления, существующие в этой сфере сегодня.

В первой главе вы узнали, что разнообразие играет огромную роль в защите цифровых ценностей — одного из столпов нашего общества на протяжении уже долгого времени. Здесь вы увидите, что направления в сфере кибербезопасности также отличаются большим разнообразием.

2.1. Множество направлений в сфере кибербезопасности

Если вы хотите построить карьеру в кибербезопасности, вам следует начать с анализа ее направлений. В каждом из тех, что перечислены на рис. 2.1, можно выделить ряд специальностей, которые непрерывно эволюционируют и меняются. Понимание того, какие направления больше всего соответствуют вашим способностям, опыту и интересам, поможет вам лучше фокусировать усилия при построении карьеры. Учитывая динамичный характер специальностей в этой сфере, составить их исчерпывающий список и поддерживать его в актуальном состоянии невозможно.

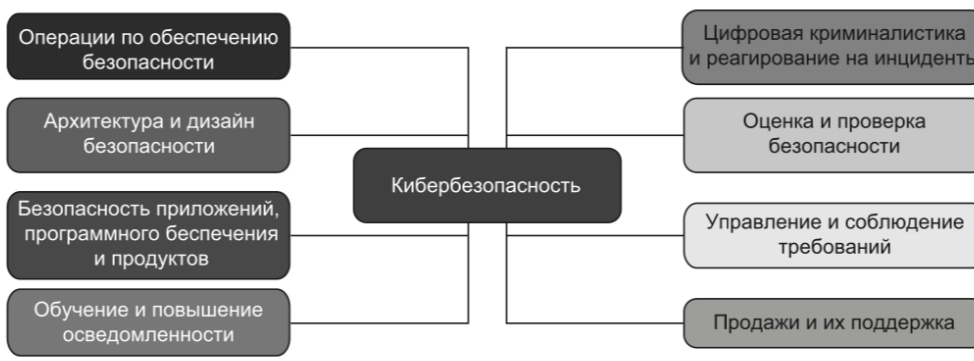

Рис. 2.1. Основные направления в сфере кибербезопасности

Кроме того, не существует общепринятой системы должностей и категорий, хотя многие представители сообщества не раз пытались ее создать. И технология, и подходы продолжают меняться, а с ними меняются должности и методы их категоризации. Тем не менее мы попробуем выделить хотя бы основные направления, чтобы вы получили общее представление о широте и разнообразии современных специализаций. Также мы обсудим множество руководящих позиций, существующих внутри них.

2.1.1. Операции по обеспечению безопасности

Говоря об операциях по обеспечению безопасности, мы имеем в виду людей на переднем крае этой сферы, которые отвечают за повседневное управление системами, мониторинг, приоритизацию и первоначальное

реагирование на атаки. Эти специалисты, как правило, обладают большим набором навыков, поскольку несут ответственность за поддержание определенного уровня безопасности всех технологий организации.

Получается, что спектр обязанностей у этих специалистов широк. За операции по обеспечению безопасности обычно отвечает *центр оперативного управления информационной безопасностью* (SOC, security operations center). Во многих организациях такой отдел постоянно проверяет систему на наличие признаков, связанных с безопасностью событий. Обнаружив потенциальный инцидент, сотрудники центра должны определить, атака ли это, а затем при необходимости надлежащим образом на него отреагировать.

Однако операции по обеспечению безопасности не ограничиваются рамками деятельности SOC. Зачастую к ним также относится администрирование основных средств защиты организации: этим могут заниматься сотрудники службы технической поддержки или отдельные лица в единой структуре. В конечном счете они несут ответственность за повседневное техническое обслуживание, в том числе за администрирование учетных записей пользователей и управление программным обеспечением, защищающим настольные компьютеры. В более крупных организациях над этим иногда работают целые группы специалистов. Например, те, кто обслуживает конкретные средства защиты, могут взаимодействовать с группой из SOC и службой технической поддержки, отвечая при этом за фактическое обслуживание и настройку самих средств.

Специалисты этого направления также взаимодействуют с представителями многих других направлений, о которых речь пойдет далее. Например, при выявлении атаки они могут привлечь группу реагирования на инциденты, чтобы дать более комплексный ответ (подробнее об этом мы поговорим чуть позже). Они также должны иметь представление о текущем ландшафте угроз, а потому им очень важно регулярно получать информацию от сотрудников службы киберразведки.

Многие люди, желающие построить карьеру в сфере кибербезопасности, начинают именно с этого направления. Такие специалисты часто работают с автоматизированными системами и решают однотипные задачи, оттого обучение на рабочем месте получается эффективным. Кроме того, они могут легко использовать опыт в ИТ-сфере в повседневной деятельности. Наконец, благодаря самой сути таких должностей и широкому кругу обязанностей работа в этом направлении будет отличным способом познакомиться со множеством технологий и концепций, которые специалисты по кибербезопасности призваны защищать.

2.1.2. Цифровая криминалистика и реагирование на инциденты

Один из ключевых аспектов кибербезопасности — реагирование на атаки и выявление их источников и последствий. Область, охватывающая такие задачи, известна как *цифровая криминалистика и реагирование на инциденты* (DFIR, digital forensics and incident response). Оценивает потенциальные атаки и принимает первичные меры защиты от них SOC, но если атаке подвергся широкий спектр систем и требуется более скоординированный и специализированный ответ, то к делу может быть привлечена группа реагирования на инциденты (IR-группа).

Задача IR-группы — обеспечить скоординированный и методичный ответ на инциденты, связанные с безопасностью. Критерии подобных инцидентов могут существенно различаться в разных организациях. В их определении часто играют роль такие факторы, как терпимость к риску, степень важности бизнеса и ресурсы SOC. Процессы реагирования также могут сильно различаться в зависимости от организации. Размер, возможности, нормативно-правовая база, бизнес-модель и многие другие факторы влияют на то, как организация реагирует на инциденты, угрожающие безопасности.

Критерии определения инцидента и порядок реагирования на него часто документируются в *плане реагирования на инциденты*. Каждой организации необходимо подготовить такой план и в нем подробно описать процесс оповещения о потенциальных инцидентах, изложить последовательность действий IR-группы, а также перечислить все отделы, которые должны быть задействованы в случае необходимости.

За разработку и обновление такого плана, как правило, отвечает IR-группа. Однако, учитывая, что он так или иначе затрагивает все части организации, IR-группа часто сотрудничает с юридическим отделом, отделом по маркетингу и связям с общественностью, SOC, другими группами специалистов по безопасности и даже с командами, отвечающими за развитие бизнеса и разработку продуктов.

Поскольку IR-группа должна быть в состоянии реагировать на инциденты, затрагивающие любую из технологий организации, требуется, чтобы ее сотрудники имели множество навыков, в том числе работы с сетями и беспроводной связью, а также обладали опытом разработки ПО и были подкованы в теме межличностного взаимодействия. Организации с более зрелыми IR-функциями понимают ценность разнообразия среди сотрудников в группе реагирования на инциденты. В некоторых организациях такая группа также отвечает за цифровую криминалистику, а в других эти роли отделены друг от друга.

Под *цифровой криминалистикой* понимается расследование инцидентов, связанных с безопасностью (или даже не связанных с безопасностью

событий), которое часто происходит уже после разрешения ситуации. Специалисты здесь изучают обнаруженные в системах улики, чтобы выяснить, как именно была осуществлена атака и какие данные и системы она затронула. Также они выявляют, документируют, сохраняют улики, собранные в атакованных системах, и представляют экспертное заключение по ним. В организациях, работающих в строго регулируемых отраслях, эта роль может быть особенно важна.

Все вышесказанное означает, что сотрудникам, занимающимся цифровой криминалистикой, необходимо обладать обширным набором навыков. Понимать не только низкоуровневое поведение систем, но и цепочки ответственного хранения и других концепций, имеющих отношение к работе с уликами. Люди этой профессии должны быть особенно внимательны к деталям и уметь эффективно вести документацию.

Несмотря на то что DFIR-специальности обычно относят к продвинутому уровню, опытные профессионалы из других сфер вполне могут обладать достаточной квалификацией, чтобы занимать такие должности. Бывшие сотрудники правоохранительных органов с опытом проведения расследований и работы с уликами часто находят себе здесь место. То же касается сетевых и системных администраторов, а также специалистов по обслуживанию инфраструктуры, которые хорошо разбираются в данных о событиях и низкоуровневом поведении различных систем. Кроме того, огромное значение здесь имеют навыки устной и письменной коммуникации, поскольку иногда за решение технических задач и документирование результатов отвечают разные люди.

2.1.3. Архитектура и дизайн безопасности

Деятельность специалистов по архитектуре и дизайну безопасности скорее превентивна, но от этого их роль не становится менее важной. Специалисты из этой области отвечают за то, чтобы придумать, спроектировать и внедрить средства и технологии обеспечения безопасности. Эту работу часто выполняют люди, знакомые с широким спектром технологий, от брандмауэров и средств защиты конечных точек до систем *управления инцидентами и событиями информационной безопасности* (SIEM, security incident and event management).

Они могут взаимодействовать с сотрудниками многих других подразделений организации. Необходимо, чтобы предлагаемые ими технологии были пригодны для широкомасштабного применения. В случае крупных компаний или государственных учреждений это иногда представляет особую проблему. Архитектор безопасности должен уметь взаимодействовать со специалистами, которые не имеют отношения

к вопросам безопасности и часто не обладают техническими знаниями; это нужно, чтобы дизайн и архитектура разрабатываемых систем соответствовали потребностям бизнеса.

Также для такого специалиста важно иметь представление о потенциальных угрозах и знать — по крайней мере неформально, — как разрабатывать их модели. Они должны понимать, с какими угрозами сталкивается организация, приоритизировать их в соответствии с общим ландшафтом рисков для бизнеса, а затем разрабатывать решения, которые устраняют или в достаточной степени снижают риски этих угроз.

Как и во многих других направлениях кибербезопасности, здесь коммуникативные навыки играют очень важную роль. Архитектор безопасности отвечает не только за определение требований и разработку решения, но и за представление этого решения на различных уровнях организации, чтобы получить финансирование и поддержку. Вероятно, это наиболее сложный аспект этой специальности, поскольку предполагает преодоление разрыва между техническими и деловыми соображениями. Архитектор должен не только обладать техническими знаниями для разработки эффективных средств защиты, но и понимать мотивы и методы бизнес-профессионалов, чтобы добиться поддержки своих инициатив со стороны высшего руководства.

Архитектору безопасности необходимо иметь богатый и разнообразный опыт, поэтому такая должность может быть одной из самых высокооплачиваемых в организации. Чтобы достичь успеха, он должен уметь опираться на свой опыт работы с различными технологиями, подходами и платформами, а также следить за появлением новых угроз и тенденций. Организациям подчас сложно найти таких специалистов, однако если им это удастся, уровень безопасности бизнеса существенно вырастет.

2.1.4. Оценка и проверка безопасности

Одно из наиболее популярных и широко известных направлений кибербезопасности — ее оценка и проверка. Именно пентестер (или *этичный хакер*) первым приходит на ум, когда задумываешься о работе в кибербезопасности. Однако это направление не ограничивается тестированием на проникновение.

Оценка и проверка безопасности предусматривает совокупность практик, направленных на защиту организации через выявление и устранение недостатков в системе безопасности. Такие специалисты не только ищут уязвимости, но и отслеживают известные слабые места, чтобы присвоить им должный приоритет и устранить. Эта деятельность

может распространяться на сети, компоненты инфраструктуры и программное обеспечение, а также выходить за рамки ИТ-систем и включать физическую охрану, проверку персонала и даже обзор общедоступной информации об организации, также известный как *разведка с использованием открытых источников* (OSINT, open source intelligence).

Некоторые виды деятельности, относящиеся к оценке и проверке безопасности в организации, перечислены в табл. 2.1.

Табл. 2.1. Основные виды деятельности, связанные с оценкой и проверкой безопасности

Вид деятельности	Описание	Цели
Сканирование на предмет наличия уязвимостей	Периодическое автоматизированное сканирование среды организации, чтобы проверить, нет ли в системе безопасности слабых мест	Регулярно проверять безопасность разнообразных компонентов ИТ-инфраструктуры
Тестирование на проникновение	Оценка определенного спектра ИТ-систем с использованием методов злоумышленников: как правило, сочетания автоматических инструментов с ручным взломом	Получить более полное и глубокое (по сравнению с обычным сканированием) представление об уязвимостях в целевых системах
Атака «красной команды»	Атака определенного спектра ИТ-систем, чтобы достичь некой конкретной цели, с использованием методов злоумышленника и способов избегания обнаружения	Смоделировать реальную атаку, чтобы оценить степень риска, связанного с существующими в среде уязвимостями
Атака «фиолетовой команды»	Атака «красной команды» при взаимодействии с «синей командой», ответственной за обнаружение атак и защиту от них	Смоделировать реальную атаку, чтобы оценить и улучшить способность средств защиты отражать атаку или восстанавливаться после нее
Социальная инженерия	Использование обмана и особенностей человеческой психологии, чтобы убедить персонал раскрыть конфиденциальные данные или предоставить доступ к конфиденциальным ресурсам. Обычно путем имитации фишинговых и/или вишинговых атак	Выяснить, как сотрудники организации реагируют на попытки манипулирования, и повысить их осведомленность о корректных действиях
Обеспечение физической безопасности	Попытка обойти физические средства защиты без обнаружения, чтобы получить доступ к конфиденциальным ресурсам. Обычно методами социальной инженерии (и часто личного взаимодействия)	Сымитировать попытку получить несанкционированный доступ к ресурсам, чтобы убедиться, что физические средства защиты и реакция персонала позволят ее отразить

Табл. 2.1. Основные виды деятельности, связанные с оценкой и проверкой безопасности. *Окончание*

Вид деятельности	Описание	Цели
OSINT-аудиты	Изучение общедоступных источников информации, поиск конфиденциальных данных об организации или ее сотрудниках	Установить факты раскрытия конфиденциальных данных, связанных с особенностями бизнес-практик или действиями персонала

Специалисты по оценке и проверке безопасности должны обладать широким спектром навыков. Совершенно очевидно, что тестирование на проникновение и осуществление атак «красной» и «фиолетовой команд» требует применения множества технических знаний. Профессионалу следует уметь выявлять признаки уязвимостей и понимать методы их эксплуатации. Поскольку зачастую атакуют сетевые устройства, операционные системы, а также системное или прикладное ПО, наличие опыта в соответствующих областях может быть особенно полезным. Например, многие бывшие разработчики ПО нередко специализируются на проведении тестов на проникновение в области приложений, поскольку благодаря опыту лучше распознают ситуации, когда не соблюдаются принципы безопасного программирования.

А вот социальная инженерия обычно требует не глубоких технических навыков, а понимания основ межличностного взаимодействия, психологии и особенностей человеческого поведения, которые позволяют влиять на людей и заставлять их выполнять нужные действия. Психологическое образование или соответствующий опыт работы, например в сфере продаж, часто оказываются полезными специалистам в этой области. Многие навыки социального инженера не поддаются количественной оценке. Здесь требуется человек особого типа: проницательный, способный быстро соображать и обладающий развитыми навыками межличностного взаимодействия. Однако техническая смекалка ему тоже не повредит. Социальные инженеры должны уметь собирать информацию о своих целях, и в этом им может пригодиться определенный технический опыт.

Сочетание технических и нетехнических навыков еще важнее, когда речь идет об оценке физической безопасности. Здесь тоже, безусловно, требуются навыки социальной инженерии, поскольку при проведении подобной оценки специалистам обычно приходится взаимодействовать с охранниками, сотрудниками и другими людьми и влиять на них. Однако им также необходимы особые технические навыки, в том числе умение взламывать замки, глубокие познания в области электроники и даже опыт работы с радиосвязью.

Однако, как говорилось ранее, это направление не ограничивается выявлением слабых мест в системе безопасности. Важнейший компонент деятельности любой организации — *управление уязвимостями*; это процессы и системы, которые позволяют каталогизировать, приоритизировать и устранять выявляемые уязвимости. Кто-то возразит, что такая работа относится к операциям по обеспечению безопасности. Однако с практической точки зрения управление уязвимостями чаще всего тесно связано с ее оценкой и проверкой. В некоторых случаях за управление уязвимостями может отвечать команда специалистов по управлению рисками. Она изучает все виды рисков, которым подвергается организация, и помогает руководителям решить, какие из них необходимо устранить в первую очередь. В этом смысле управление уязвимостями хорошо вписывается в ее сферу ответственности. В конечном счете именно группа, отвечающая за оценку и проверку безопасности, должна обнаруживать слабые места, чтобы их можно было устранить до того, как ими воспользуются злоумышленники.

Чтобы еще раз продемонстрировать степень разнообразия карьерных возможностей в этом направлении, я приведу пример Квадво Берджи, старшего аналитика по работе с уязвимостями из Агентства по кибербезопасности и защите инфраструктуры США (CISA), подведомственного Министерству внутренней безопасности (DHS). Берджи выступает посредником между исследователями, выявляющими уязвимости в распространенных программах и продуктах, и организациями, отвечающими за поддержку этих продуктов. В частности, он помогает управлять базой данных общеизвестных уязвимостей информационной безопасности Common Vulnerabilities and Exposures (CVE), принадлежащей некоммерческой организации MITRE. Несмотря на то что его работа не связана с оценкой сетей и программного обеспечения, ему и его команде необходимо понимать соответствующие концепции, поскольку они помогают создавать отчеты о выявленных уязвимостях. Помимо всего прочего, его команда отвечает за то, чтобы поставщики, которым сообщается о выявленных недостатках, адекватно реагировали на эти отчеты.

2.1.5. Безопасность приложений, программного обеспечения и продуктов

Это направление сосредоточено на обеспечении безопасности элементов, которые организации создают, чтобы продавать их, оказывать с их помощью услуги или поддерживать работу внутренних процессов. Под обеспечением *безопасности приложений* обычно понимается то, как организации защищают разрабатываемые ими программы.

Понятие *безопасности программного обеспечения* несколько двусмысленное, но в основном оно касается защиты любого ПО, используемого в организации, — разработанного ли внутри нее или приобретенного у стороннего производителя. *Безопасность продукта* в общем смысле относится к защите любых программных или аппаратных продуктов, продаваемых компанией. Все эти три области объединяет одно: к ним применяется концепция жизненного цикла, на всех этапах которого должны использоваться методы обеспечения безопасности.

Под безопасностью приложений понимается использование методов защиты в рамках *жизненного цикла разработки программного обеспечения* (SDLC, software development life cycle). Результаты множества исследований, проведенных за несколько десятилетий, показали, что обнаруживать и устранять уязвимости на ранних этапах разработки приложений гораздо дешевле и эффективнее, чем после их запуска в производство.

Со своего появления в 2008 году DevOps подкидывает проблем тем, кто стремится сделать безопасность эффективной частью непрерывной поставки ПО. В *культуре DevOps* разработчики ПО и персонал, занимающийся поддержкой операций, сотрудничают в рамках модели общей ответственности. Благодаря стремлению специалистов по безопасности внедрить методы ее обеспечения в ранние этапы разработки ПО родилась концепция *DevSecOps*. Ее практики безопасности также обычно относятся к сфере защиты приложений.

Защита программного обеспечения расширяет сферу защиты приложений, ведь организация может использовать и сторонние программы. Это направление опирается на общность жизненного цикла приобретения и развертывания стороннего ПО и цикла разработки собственного.

Под обеспечением безопасности продукта обычно подразумевается защита продуктов, продаваемых организацией. Иногда это понятие позволяет подчеркнуть тот факт, что продукт — не всегда программы или приложения. Это могут быть также устройства или другие материальные товары, в безопасности которых компания должна убедиться. Опять же, поскольку в их разработке и обновлении используется концепция жизненного цикла, обеспечение безопасности должно быть интегрировано в его этапы.

Специалисты этого направления должны обладать техническими навыками, а также глубоко понимать процесс разработки ПО и продуктов вплоть до уровня кода или компонентов. Во многих случаях такое понимание оказывается обязательным. Специалисту будет трудно внедрять принципы безопасного программирования совместно с разработчиками, если он не написал за свою жизнь ни строчки кода. Кроме того, эмпатия, обусловленная наличием опыта работы в похожей сфере, может оказаться полезной при попытке повлиять на поведение создателей продукта или ПО.

2.1.6. Управление и соблюдение требований

Мы уже познакомились с идеей *управления и соблюдения требований* ранее в этой главе. К организациям как государственного, так и частного сектора предъявляется все больше отраслевых и правовых требований. Кроме того, в большинстве компаний есть внутренние политики и стандарты, регламентирующие применение необходимых средств защиты, процессов и технологий. Задача специалистов по управлению и соблюдению требований — обеспечить соответствие деятельности всех подразделений организации внешним нормативам и внутренним политикам.

Как правило, такие специалисты занимаются не только кибербезопасностью. Корпоративные политики, а также отраслевые и правительственные требования обычно распространяются на многие области, представляющие интерес для бизнеса. Однако по мере роста числа правил, связанных с конфиденциальностью и безопасностью, растет потребность в квалифицированных кадрах, обладающих знаниями в этой области.

Специалисты этого направления отвечают за административную сторону деятельности организации. Взаимодействие с юридическими и аудиторскими службами для них обычное дело. Им часто приходится интерпретировать законы и другие правила в плане их влияния на бизнес. Кроме того, они оценивают текущий уровень соответствия организации требованиям, анализируют пробелы и разрабатывают рекомендации по их устранению, а также сотрудничают с внутренними и внешними аудиторами, чтобы продемонстрировать соответствие требованиям в ходе регулярных проверок.

Учитывая эти ключевые обязанности, таким специалистам может пригодиться опыт юридической или аудиторской деятельности. Им также необходимы развитые навыки межличностного общения, поскольку их работа требует взаимодействия с техническими специалистами и с высшим руководством. При взаимодействии с командами им может пригодиться технический опыт, однако глубокие знания конкретных технологий им обычно не требуются.

2.1.7. Обучение и повышение осведомленности

В последнее время человеческий фактор играет все более значимую роль в обеспечении кибербезопасности. Многие из наиболее известных атак были успешно осуществлены из-за человеческой ошибки и методов социальной инженерии. Поэтому во всех отраслях и секторах обычным

явлением становится обучение сотрудников, клиентов, пользователей и даже представителей широкой общественности. Направление, связанное с *обучением и повышением осведомленности*, охватывает все способы непосредственного обучения людей современным правилам безопасности.

Большинство средних и крупных организаций уже внедрили подобные программы в той или иной форме. Ценность такого обучения хорошо изучена и общеизвестна, и по многим отраслевым и правительственным постановлениям проводить его обязательно. Содержание учебных программ может варьироваться в зависимости от организации. Где-то обучают под руководством инструктора, где-то используют компьютерные обучающие модули, иногда проводятся соревнования и внутренние маркетинговые кампании. Внедрить и отслеживать эффективность программ обычно поручают команде специалистов, обладающих навыками в области образования.

Однако повышение осведомленности — не единственная форма обучения. Из-за того что кибербезопасности стали уделять огромное внимание, появилось множество учебных программ и университетских курсов, помогающих людям освоить навыки для работы в этой области. На подобных курсах часто преподают профессионалы с большим опытом в сфере кибербезопасности, причем многие из них все еще активно работают в разных ее направлениях.

При подготовке к написанию этой книги мне довелось пообщаться с Габриэль Хемпель, которая имеет обширный опыт в проведении оценки и обеспечении безопасности приложений (в частности, облачных) и выпускает учебные материалы для нескольких организаций. Ее история впечатляет тем, что она попала в сферу кибербезопасности совершенно нетрадиционным путем: перешла туда из биомедицины. Однако она хорошо понимала связь между этой областью здравоохранения и науки и кибербезопасностью.

Она использует свой разнообразный опыт в различных направлениях кибербезопасности не только для создания качественных образовательных материалов. Несмотря на отсутствие долгой карьеры в этих областях, она смогла превратить полученные знания в контент, позволяющий эффективно обучать других людей. Эта уникальная способность синтезировать информацию и обмениваться ею очень важна для специалиста по кибербезопасности.

Таким образом, человек с опытом работы в сфере образования и с техническими знаниями, позволяющими ему понимать концепции кибербезопасности, может с успехом играть любую из этих ролей. Помимо непосредственно навыков инструктирования этим людям не помешает умение разрабатывать программы обучения и учебные планы.

2.1.8. Продажи и их поддержка

Я уверена, что заголовок этого раздела вызовет недоумение у многих читателей. Зачем включать продажи в список направлений кибербезопасности? Я долго думала, стоит ли это делать. Однако без продаж, без инженеров по продажам и других лиц, поддерживающих этот процесс, не появилось бы ни одного из тех замечательных инструментов кибербезопасности и средств защиты, которыми мы сегодня пользуемся. И это неоспоримый факт.

Отношения между ИТ-специалистами и продавцами продуктов действительно довольно напряженные. Однако, как бы ни жаловались представители отрасли на некоторые сомнительные тактики продавцов, эти люди должны быть частью нашего сообщества.

Продажа продуктов происходит не сама собой. В этом процессе участвуют продавцы, инженеры по продажам, архитекторы решений и другие отнюдь не случайные люди. Специалисты по продажам должны понимать концепции кибербезопасности, на которых основан их продукт. Инженерам по продажам и архитекторам решений необходимы глубокие технические знания, чтобы они могли помогать клиентам выбирать правильные продукты и настраивать их так, чтобы он подходил для целей их организации.

Итак, я выделила *продажи и их поддержку* в отдельное направление, потому что те, кто в нем работает, вносят свой вклад в защиту цифрового мира. Этим специалистам необходимо понимать принципы обеспечения безопасности и иметь специальную подготовку, связанную с применением различных инструментов и методов защиты. Мы не можем отделить людей, участвующих в распространении и развертывании средств защиты, от остальных представителей сообщества, ежедневно использующих эти инструменты.

Я поговорила с одним таким человеком, Каролиной (Линой) Террасас — специалистом по кибербезопасности в Cisco, ведущей компании в области сетевых технологий и кибербезопасности. Она сказала, что суть ее деятельности заключается в консультировании клиентов. Она встречается с ними, выясняет особенности их рабочей среды и дает рекомендации по тому, как улучшить практики использования существующих инструментов или в какие новые инструменты инвестировать. Таким образом, несмотря на то что она занимается продажами, ее работа непосредственно влияет на общий уровень безопасности этих организаций.

Вполне очевидно, что человек, обладающий опытом продаж и готовый расширить свою базу знаний в области кибербезопасности, может с легкостью найти себе место в этой сфере. Инженеры по продажам и архитекторы решений часто полагаются на обширный прошлый опыт, дополняя его специализированным обучением по продукту или

продуктам, которые они продвигают. Однако такой опыт не обязателен для технически подкованного человека, способного быстро освоить продукт наряду с общими навыками обеспечения безопасности. Многие люди, ныне занимающие технические должности в области кибербезопасности, начинали с продаж или их поддержки.

Образование Террасас было связано с компьютерами и технологиями. Однако вместо того, чтобы пойти по пути инженера, она выбрала карьеру в сфере продаж. Ее путь служит примером того, как технический практический опыт можно сочетать с принципами продаж, чтобы создать нечто весомое с точки зрения обеспечения кибербезопасности.

2.1.9. Лидеры и руководители

Составляя список направлений в сфере кибербезопасности, я сомневалась, следует ли давать отдельное место в этом ряду руководящим должностям. В значительной степени они представляют собой кульминацию карьеры в направлениях, обсуждавшихся в этой главе. Вы, вероятно, заметили, что они отсутствуют в диаграмме на рис. 2.1.

Однако, когда я разговариваю со специалистами по кибербезопасности об их карьерных целях, многие выражают желание перейти на более высокую должность. Все они хотят когда-нибудь стать директором по информационной безопасности (CISO). Чтобы возглавить целое подразделение, человек должен обладать дополнительными навыками и способностями, которые обычно не свойственны специалистам более низкого уровня. Потому я и считаю важным здесь упомянуть об этом.

Как я уже говорила, человек на руководящей должности обычно имеет обширный опыт в одном, а часто и в нескольких направлениях кибербезопасности. Поднимаясь по карьерной лестнице, лидер должен получить хотя бы общее представление о различных процессах, за которые ему предстоит нести ответственность. Кроме того, необходимо научиться оказывать влияние на другие подразделения и эффективно общаться с высшим руководством.

Директор по информационной безопасности, как правило, вершина карьеры в этой сфере; эта роль охватывает все, что связано с кибербезопасностью целого подразделения или даже всей организации. Руководитель должен уметь применять знания в области кибербезопасности и навыки управления бизнесом в повседневных ситуациях, а также четко понимать, как работа всех восьми описанных направлений складывается в картину единой стратегии.

Еще более важно для него понимать, в чем заключается деятельность остальных руководителей и как в нее вписывается кибербезопасность.

Именно ему предстоит информировать других руководителей и совет директоров о текущем уровне защиты компании. Чем лучше высшее руководство будет осознавать важность кибербезопасности, тем чаще директоров по информационной безопасности будут привлекать к совещаниям на самом высоком уровне.

С верхами руководства люди, отвечающие за информационную безопасность, должны говорить о ней особым образом. Руководители далеки от этой темы, и обсуждение с ними технических деталей угроз, уязвимостей и тому подобного может быть неуместным. Пытаясь получить финансирование для дополнительных ресурсов, инструментов, технологий и проектов, отвечающие за безопасность лидеры должны быть в состоянии продемонстрировать, как их инициативы связаны с общим успехом организации.

Вот почему руководящая должность, хоть и может казаться впечатляющей, даже, вероятно, естественной целью, подходит далеко не всем. В этой роли лучше всего раскрываются те, кто хочет разбираться и работать в области не только безопасности, но и управления бизнесом. Здесь требуется уникальное сочетание технических знаний и навыков делового администрирования. Однако, несмотря на такое количество требований, работа в этой должности может оказаться делом стоящим. Нести полную ответственность за стратегию безопасности организации — шанс сформировать свое наследие.

Разумеется, есть риск, что это наследие может не оправдать ожиданий. Поэтому планируя свое будущее, подумайте: действительно ли эта кажущаяся идеальной роль — желанная вершина вашей карьеры?

2.2. Характеристики специалиста по кибербезопасности

Чтобы занять конкретную должность в каждом из направлений кибербезопасности, надо получить конкретные же навыки и опыт. Однако у специалистов в этой области есть некоторые общие черты. Именно на них обращают внимание многие менеджеры по найму при поиске талантов.

2.2.1. Изобретательность и креативность

По сравнению со многими другими область кибербезопасности относительно молода. Кроме того, она постоянно развивается. Каждая уникальная ситуация, с которой сталкивается практик, требует такого же уникального и заточенного под нее решения. Поэтому люди, от природы

склонные изобретать и создавать что-то новое или совершенствовать существующее, хорошо подходят для работы в сфере кибербезопасности.

Первые хакеры часто стремились разобраться в технологии, чтобы в дальнейшем манипулировать ею и создавать на ее основе что-то новое. Те же принципы работают в сфере кибербезопасности и сегодня. Существующие решения и методы зачастую просто не могут удовлетворить текущие потребности в защите. В этих случаях специалисты по безопасности должны применять новаторский подход и находить творческие способы решения проблем.

2.2.2. Неуемная любознательность

Неуемная любознательность имеет решающее значение для специалистов по кибербезопасности. При возникновении проблемы они должны быть готовы разобраться в ней, проведя собственное расследование. Неважно, идет ли речь о реагировании на предупреждение о потенциальном инциденте, о проверке приложения на конкретную уязвимость или об оценке компании на соответствие новым требованиям, профессионалы должны проявлять беспредельную любознательность.

Ответы, интересующие специалистов по безопасности, не всегда легко найти. Поэтому их любопытство должно граничить с одержимостью. Готовность прыгнуть в «кроличью нору» и досконально изучить проблему — неотъемлемое качество самых уважаемых профессионалов в этой области. Настойчивость в преодолении неудач в итоге позволяет им достичь успеха. Такая любознательность свойственна тем, кто готов, хочет и умеет учиться. С учетом постоянно растущей скорости развития технологий, непрерывное обучение становится обязательным условием.

2.2.3. Жажда знаний

Помимо любознательности, специалистам по безопасности также необходимо демонстрировать желание и способность постоянно учиться. Самые эффективные сотрудники службы безопасности — те, у кого есть потребность досконально разбираться в интересующем их объекте, не довольствуясь простым пониманием его функций.

Понимание принципа работы технологий позволяет им внедрять инновации и создавать новые решения. Потребность в таком понимании побуждает человека выявлять аспекты технологии, нуждающиеся в улучшении, и добывать знания для их совершенствования. В сфере безопасности это относится не только к технологическим системам

(и людям), которые мы пытаемся защитить, но и к тем технологиям и практикам, которые мы используем для их защиты. Непрерывное совершенствование показало свою эффективность в обеспечении высокоуровневой кибербезопасности. Обучение и рост специалистов в этой области гарантирует то, что они будут постоянно работать над повышением качества, безопасности и надежности своих систем.

2.2.4. Идеализм

Вера в идеалы, которые разделяют участники сообщества кибербезопасности, и следование им имеет особую важность для всех, кто хочет построить карьеру в этой сфере. Тот, кто способен видеть общую картину и стремиться к общему благу, став профессионалом в кибербезопасности, будет придерживаться этического кодекса в своей работе.

Навыки, технологии и знания этих профессионалов могут быть использованы не только во благо, но и во зло. Приверженность идеалам сообщества кибербезопасности (подробно описанным в главе 1) означает, что у них есть тот этический компас, что позволяет принимать решения, соответствующие принципам сообщества и организаций, которые построены на них.

2.2.5. Забудьте о «рок-звездах информационной безопасности»

Понятие «рок-звезда информационной безопасности» было порождено хакерской культурой и тематическими конференциями и приобрело широкую известность благодаря обсуждению вопросов кибербезопасности в СМИ и социальных сетях. Большинство людей знает, что в этой сфере работает ряд выдающихся личностей. Хакеры, которые обнаруживают и раскрывают особенно примечательные эксплойты, специалисты по безопасности, ведущие популярные блоги и подкасты, люди, которые часто выступают с программными докладами на тематических конференциях, — всех их называют *рок-звездами информационной безопасности*.

Эти личности обрели известность, поскольку кибербезопасность стала доминирующей темой в СМИ. Брюс Шнайер, Лесли Кархарт, Эд Скудис и Кэти Муссурис — вот лишь несколько влиятельных экспертов, к которым представители средств массовой информации обращаются за комментариями. Кроме того, хакерская культура на протяжении нескольких десятилетий была окутана ореолом таинственности и активно воспевалась в кино и на телевидении. В результате некоторые из тех,

кто желает построить карьеру в сфере кибербезопасности, ищут славы или имеют нереалистичное представление о том, в чем заключается суть работы в этой области.

Желание получить признание коллег или общества за ваши навыки и способности вполне здоровое. Но если вы сделаете это своей главной целью, оно скорее нанесет ущерб вашей карьере. Анализ мотивов, побуждающих вас заняться кибербезопасностью, критически важен для планирования дальнейшего пути. Чего вы хотите добиться и почему? В мире кибербезопасности царит неопределенность, он постоянно меняется. Подумайте, действительно ли вы к этому готовы.

2.3. Соображения анонимности

Многие участники сообщества кибербезопасности предпочитают сохранять анонимность и действовать максимально скрытно. На это есть много причин. Работа в сфере безопасности, предполагающая защиту систем от злоумышленников или борьбу с потенциально преступными элементами, может сделать человека мишенью. Кроме того, многие ценности хакерской культуры, обсуждавшиеся в главе 1, способны побудить человека оставаться анонимным. Почему мы коснулись этой темы именно сейчас?

Дело в том, что это личное решение должно быть принято в самом начале карьеры. Если вы решили сохранять анонимность, об этом необходимо позаботиться сразу. Вы можете начать строить карьеру, соблюдая конфиденциальность, а затем решить стать более публичным, но не наоборот. Практически все понимают, что, когда личная информация уходит в общий доступ, этого уже не отменить.

Несмотря на то что на первый взгляд такое решение может показаться тактическим и даже незначительным, все может измениться через несколько лет после начала карьеры. Вы должны решить, каким объемом информации готовы поделиться с миром. Необходимо определить для себя границы, которые будете защищать. Вы хотите делиться информацией о своих детях? Скорее всего, нет. Вы готовы мириться с тем, что случайные пользователи интернета смогут узнать ваш адрес? Вы вообще хотите сообщать людям свое настоящее имя, пол и другие идентифицирующие вас характеристики? На все эти вопросы следует ответить заранее.

Однако не стоит думать, что единственный вариант — это сохранять анонимность. Вы можете решить сразу же открыто заявить о себе, и на то есть несколько причин. Во-первых, сохранение анонимности — это еще один источник напряжения, который вам придется постоянно

терпеть. Кроме того, на это придется тратить дополнительные усилия. Нужно будет следить, как вы взаимодействуете с другими людьми, что вы говорите, чем делитесь, какие сайты посещаете и так далее. Вам придется все время оставаться настороже.

Во-вторых, сохраняя анонимность, вы делаете себя потенциальной жертвой доксинга: кто-то может выяснить и раскрыть миру информацию о вас. Вы получите бóльшую свободу, лишив злоумышленников такой опции, если открыто заявите о себе с самого начала.

В-третьих, анонимность может ограничить вас в средствах при установлении деловых контактов, а они играют огромную роль при поиске новой работы. Есть вероятность, что вы захотите создать личный бренд, способный открыть перед вами множество дверей в профессиональном плане. Создать такой бренд, сохраняя конфиденциальность, тоже реально, но это будет гораздо сложнее.

Никто, кроме вас, не может принять это решение. Тем не менее подумать об этих вещах и учесть наиболее важные для себя аспекты следует *до* начала карьеры.

ПОДВЕДЕНИЕ ИТОГОВ

- В сфере кибербезопасности есть несколько основных направлений, каждое из которых включает в себя множество ролей и должностей.
- Достичь успеха и стать профессионалом можно в любом из них.
- Карьерный рост в сфере кибербезопасности не ограничивается выполнением высокотехнологичных функций.
- Наиболее успешными профессионалами в сфере кибербезопасности становятся изобретательные и креативные люди, которые отличаются неуемной любознательностью, постоянно учатся и верят в идеалы своего сообщества.

Глава 3
Навыки, пользующиеся спросом на горячем рынке

В этой главе

- Текущее состояние рынка труда в сфере кибербезопасности и основные проблемы, с которыми мы сталкиваемся
- Система карьерного роста в сфере кибербезопасности
- Основные технические навыки, необходимые специалисту по кибербезопасности
- Основные гибкие навыки, необходимые специалисту в этой сфере

В своем официальном отчете о состоянии рынка труда в сфере кибербезопасности за 2019 и 2020 годы (2019/2020 Official Annual Cybersecurity Jobs Report) компания Cybersecurity Ventures проанализировала вакансии в этой области и предсказала, что к началу 2021 года незакрытыми останутся более 3,5 миллиона. В другом отчете, опубликованном в 2018 году отраслевой ассоциацией (ISC)^2, прогнозировалось, что количество открытых вакансий к 2021 году составит 2,93 миллиона. Несмотря на разницу в цифрах, оба исследования говорят о том, что число незанятых рабочих мест в сфере кибербезопасности представляет собой серьезную проблему.

Для тех, кто хочет начать здесь карьеру, это может показаться хорошей новостью. Вы можете подумать, что отрицательный уровень безработицы должен значительно облегчить поиск работы, однако не спешите радоваться. В реальности многие новички с огромным трудом находят свою первую должность в сфере кибербезопасности. Чтобы помочь вам лучше подготовиться, далее мы обсудим текущее состояние рынка труда, некоторые из распространенных должностей и навыки, необходимые для того, чтобы эти должности занять.

3.1. Соискатели и вакансии

Анализ текущего состояния рынка труда в сфере кибербезопасности дает противоречивые результаты. С одной стороны, есть множество незакрытых вакансий, в чем можно убедиться, просто просмотрев соответствующие разделы сайтов вроде LinkedIn и Indeed[6]. С другой стороны, многим людям, желающим заняться кибербезопасностью, трудно найти здесь работу.

Еще более интересно, что с такой проблемой сталкиваются не только новички, но и соискатели с многолетним стажем.

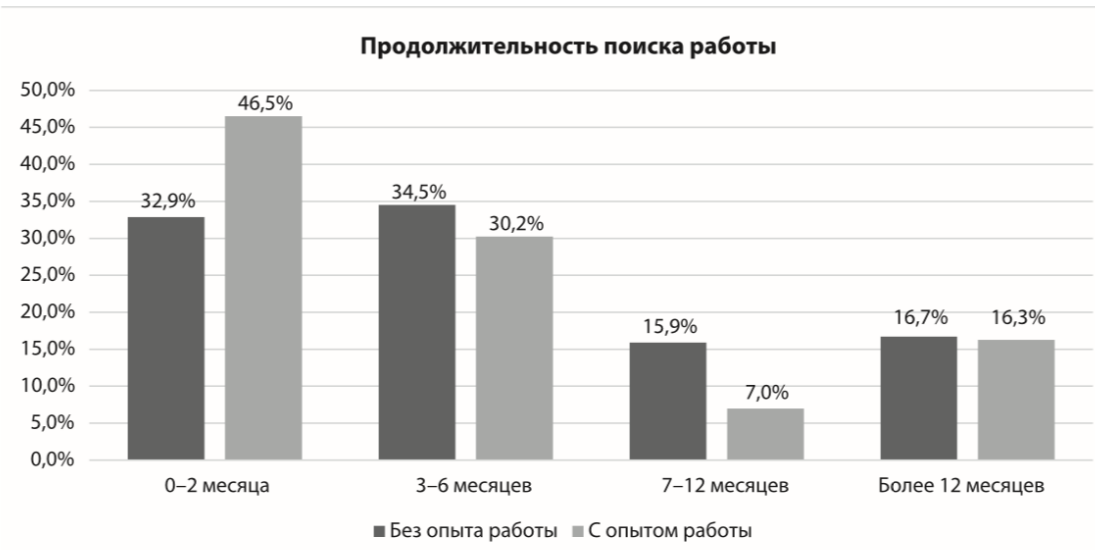

Рис. 3.1. Трудности с поиском работы в сфере кибербезопасности испытывают и новички, и опытные сотрудники. Согласно результатам проведенного мной опроса, более 32% кандидатов-новичков искали свою первую работу более семи месяцев

[6] Американские сайты для поиска работы. — *Прим. ред.*

В январе и феврале 2020 года я провела исследование о построении карьеры в сфере кибербезопасности; оно состояло из двух опросов с участием специалистов по кибербезопасности и представителей академического сообщества. Первый был создан для людей без опыта, которые никогда не работали в этой области, но хотели бы в нее перейти. Второй — для людей, занимавших должности, связанные с кибербезопасностью. Участников обеих групп, находящихся в поиске работы, спрашивали, как долго продолжается этот поиск. Результаты, приведенные на рис. 3.1, оказались неожиданными. Более 16% участников обеих групп сообщили, что ищут работу уже более 12 месяцев.

Cybersecurity Workforce Study («Исследование рынка труда в сфере кибербезопасности»), проведенное (ISC)² в 2019 году, показало, что в 11 ведущих экономиках мира в сфере кибербезопасности занято 2,8 миллиона специалистов. В моем опросе доля респондентов, находящихся в поиске работы, составляла около 4,2%. Это говорит о том, что в этих 11 странах более 27 000 опытных специалистов тратят на поиск новой работы более шести месяцев. У нас нет хорошего способа оценить количество жителей планеты, ищущих свою первую работу в сфере кибербезопасности, однако, учитывая растущую популярность соответствующих учебных специальностей во всем мире, можно с уверенностью сказать, что это число внушительное. Далее в главе мы обсудим, почему важно это понимать и что это значит для тех, кто хочет построить карьеру в сфере кибербезопасности.

Рис. 3.2. Удивительно, но данные опроса показывают, что наличие ученой степени, отраслевого сертификата или помощи наставника не коррелирует с более коротким сроком поиска работы

Учитывая приведенные цифры, совершенно очевидно, что нам необходимо глубже изучить факторы, способные влиять на поиск работы в этой области. Например, есть ли у соискателя ученая степень в области информатики или ИТ, специализированные сертификаты и даже обращался ли он за помощью к наставнику.

Все эти вопросы были заданы начинающим профессионалам в сфере кибербезопасности, участвовавшим в моем опросе в 2020 году. Результаты получились неожиданными и даже тревожащими, если рассматривать их вне контекста. Как видно на рис. 3.2, срок поиска работы во всех этих группах различался совсем незначительно. В среднем короткие сроки были характерны для участников без ученой степени. Однако выводы, сделанные на основе этого набора данных, могут быть неточными: среди прочих учитывались будущие выпускники, которые начинают искать работу еще до получения диплома. Тем не менее в целом цифры весьма похожи: по-видимому, вышеперечисленные факторы практически не влияют на сложность поиска первой работы.

Человеку, потратившему с трудом заработанные деньги на получение ученой степени или отраслевого сертификата, это может показаться обескураживающим. Не переживайте: все это было не зря. Чтобы объяснить, почему периоды поиска работы схожи, необходимо учитывать множество факторов. Кроме того, ученые степени, сертификаты и помощь наставников по-прежнему представляют ценность — о ней мы подробно поговорим в следующих главах. Пока эти данные просто демонстрируют многогранность проблемы и разные типы сложностей, преследующих соискателя-новичка в сфере кибербезопасности, а также служат основой для стратегий, которые мы обсудим позже.

3.2. Система карьерного роста в сфере кибербезопасности

Как было сказано в главе 2, в сфере кибербезопасности множество направлений, и в каждом из них множество постоянно эволюционирующих должностей. Однако при составлении своего карьерного плана вам также важно понимать, как происходит *продвижение по карьерной лестнице*.

Под продвижением мы понимаем постепенный переход с низкого уровня на более высокие. Чтобы разобраться в нем, надо уметь распознавать и определять ключевые навыки, которые играют решающую роль при назначении соискателей на те или иные должности в сфере кибербезопасности.

Люди, желающие построить новую карьеру, обычно начинают с постановки глобальной цели. Они пытаются представить, какую должность будут занимать через 5, 10 или даже 15 лет работы в выбранной области. Это хорошее упражнение; любому человеку, отправляющемуся в новое карьерное путешествие, важно уметь смотреть будущее в долгосрочной перспективе. Это позволяет наметить курс и установить краткосрочные цели для отслеживания прогресса, а также мотивирует продолжать профессионально развиваться.

Чтобы обдумать свой карьерный рост в сфере кибербезопасности, необходимо иметь представление о наиболее распространенных уровнях, которые вам предстоит пройти. Речь идет не о конкретных должностях, специфичных для направления, а о спектре ответственности в должности соответствующего уровня. Если новый специалист поймет, как проходит этот процесс, ему будет легче определиться с карьерными целями.

Это очень важно. Кто-то считает, что цель каждого человека — занять руководящую должность. Однако многие люди, в частности технические специалисты, к этому вовсе не стремятся, поскольку такая работа требует совсем другого образа мышления и набора навыков. И далеко не все хотят ее выполнять. Итак, давайте вначале рассмотрим различные уровни должностей и соответствующие им обязанности и ожидания.

3.2.1. Должности начального уровня

Должности начального уровня — отправная точка практически в любой карьерной системе. Их занимают новички, только пришедшие в ту или иную сферу. От них не ожидают соответствующего опыта, их задача — развить в себе базовые навыки, которые легко адаптировать к любому виду деятельности. Как говорилось ранее, в сфере кибербезопасности людям трудно найти должность начального уровня.

На такие вакансии организации обычно стремятся найти высококвалифицированных специалистов. Когда далее в этой главе мы будем говорить о должностных инструкциях, вы увидите, какие проблемы способен породить такой подход. Время от времени в сфере кибербезопасности появляются вакансии и на *должность младшего сотрудника*, которые обычно предусматривают период обучения на рабочем месте. Это замечательно, потому что такие должности не только помогают специалисту развивать навыки, но и показывают, что компания готова инвестировать в своих сотрудников.

3.2.2. Старшая группа должностей

По мере наработки опыта специалисты по безопасности переходят на так называемые *старшие должности*. В зависимости от роли для этого может потребоваться от пяти до восьми лет опыта. Переход на более высокую должность означает бóльшую ответственность. Обычно ожидается, что эти люди будут руководить конкретными проектами или станут наставниками для других сотрудников организации.

Анализ рынка труда в сфере безопасности показывает, что вакансий на такие руководящие должности больше всего. Организации ищут опытных людей, способных поделиться знаниями, полученными на предыдущих местах работы и требующих минимального предварительного обучения. В сфере безопасности такие люди часто отвечают за решение большинства тактических повседневных задач.

3.2.3. Должность архитектора

Архитектор безопасности — это узкоспециализированный профессионал с обширными знаниями в области кибербезопасности, которые охватывают множество технологий и организационных парадигм. А потому соискатель, чтобы занять эту должность, как правило, должен иметь не менее десяти лет опыта. Она одна из самых высокооплачиваемых, если не считать руководящих, однако вакансии на них встречаются реже всего.

Архитекторы отвечают за информационную безопасность на самом высшем уровне. Они должны уметь учитывать особенности различных технологий и разрабатывать решения, применяя множество защитных техник. Поэтому архитекторы тратят много времени на проектирование систем и анализ данных, собранных с помощью специальных инструментов. Ожидается также, что они будут руководить группами и обучать менее опытных сотрудников, когда в том возникнет необходимость.

3.2.4. Лидерство в сфере кибербезопасности

Переход с уровня самостоятельного сотрудника на должность, предполагающую курирование других профессионалов, — желанная карьерная цель для многих людей. Этот переход может принимать различные формы и варьироваться в зависимости от организации.

В большинстве случаев первый шаг на этом пути — заполучить роль *руководителя команды*, или *тимлида*, которая обычно не имеет официального названия. Связанные с ней задачи могут поручить старшему сотруднику или специалисту, хотя его фактическая должность при этом зачастую остается прежней. В таких случаях лидерские функции менее формальны. Хотя от таких специалистов ожидают исполнения обязанностей руководителя по отношению к членам команды, они обычно не имеют подотчетных сотрудников и не отвечают за регулирование заработной платы. Иногда их привлекают к управлению эффективностью, но обычно даже тогда за результаты этой деятельности несет ответственность менеджер.

В сфере безопасности, как и в большинстве других областей, первой официальной руководящей должностью считается *менеджер*. Она предполагает наличие подотчетных сотрудников. В сфере безопасности менеджер часто отвечает за деятельность команды специалистов определенного профиля. Например, в крупном SOC он может возглавлять группу, которая занимается исключительно мониторингом брандмауэров или приоритизацией предупреждений от SIEM-системы. Однако в компаниях с небольшими ИТ-отделами менеджеры могут руководить многопрофильной командой, действующей в рамках различных направлений безопасности. Это важно понимать, потому что разница в ожиданиях порождает разницу в требованиях, предъявляемых компаниями к соискателям.

На следующих двух уровнях обычно располагаются *старшие менеджеры* и/или *директора*. Предполагается, что они контролируют деятельность менеджеров. Разница между управлением отдельными сотрудниками и менеджерами значительна, ее не следует недооценивать. Именно поэтому компании довольно методически и консервативно подходят к закрытию таких вакансий. Многие профессионалы, которые добираются до должности менеджера, никогда не продвигаются дальше этого уровня, потому что оказываются неспособны сменить стиль руководства. На эти вакансии чаще привлекают извне людей с соответствующим опытом, а не продвигают сотрудников компании.

Обязанности менеджеров, как правило, сосредоточены на повседневных тактических и оперативных аспектах бизнеса. Другими словами, они координируют деятельность команд, направленную на достижение конкретных целей. Они должны уметь читать, отслеживать и сообщать статистику по системам и проектам, которые контролируют. Часто на менеджеров также возлагается определенная ответственность за управление заработной платой. Кроме того, они отвечают за наем сотрудников в свои команды.

Деятельность старшего менеджера и директора скорее стратегическая. Их основная обязанность не отслеживать выполнение отдельных задач, а управлять работой, связанной с долгосрочными целями команды. Обычно такие руководители планируют, чем будет заниматься команда, на несколько лет вперед, измеряют высокоуровневые показатели ее эффективности и формируют четкое представление о работе для ее участников.

3.2.5. Высшее руководство

К *высшему руководству* обычно относятся вице-президенты (включая помощника вице-президента, старшего вице-президента и исполнительного вице-президента) и такие высшие должностные лица, как директор по информационной безопасности (CISO). Многие люди, начинающие карьеру в сфере безопасности, видят своей конечной целью именно роль CISO. Часто считается, что она принадлежит высшему эшелону должностей в этой сфере.

Однако для перехода на этот уровень необходимо значительно сместить акценты. Несмотря на то что вице-президенты и директора по информационной безопасности обладают обширным опытом в этой сфере, уровень их технических знаний значит меньше, чем навыки делового администрирования. От них ожидают понимания бизнес-концепций и того, как обеспечение безопасности способствует достижению бизнес-целей. Их деятельности акцентируется на высокоуровневых функциях: количественной оценке и анализе рисков, разработке стратегии, связанной с безопасностью, планировании бюджета. Технические знания здесь нужны для общения со специалистами, а не для выполнения конкретных задач. Это важно понимать, поскольку такая роль подходит далеко не всем профессионалам в этой области.

По сравнению с другими руководящими должностями роль директора по информационной безопасности все еще относительно нова. Нередко ее поручают техническим специалистам, доросшим до этого уровня. К сожалению, иногда это оказывается ошибкой, поскольку организации все еще не вполне понимают, как эта роль вписывается в их структуру управления. Поэтому важно не идеализировать должность CISO. Чтобы достичь карьерного успеха, необходимо объективно и критически проанализировать собственные стремления и выяснить, действительно ли занятие должности такого уровня входит в их число. Убедитесь, что вы понимаете суть этой работы, и решите, насколько она вам подходит, не зацикливаясь на ее впечатляющем названии.

3.3. Основные навыки, необходимые специалистам по кибербезопасности

При подборе специалистов по кибербезопасности работодатели обычно ищут тех, кто обладает множеством технических и нетехнических навыков. Важно знать, что это за навыки и какое значение они имеют в той или иной роли: это поможет не только спланировать свой карьерный путь, но и лучше соотнести собственные умения с требованиями компании. А также понять, почему в описание должности включили тот или иной пункт.

В этом разделе описываются основные навыки, которые работодатели перечисляют в объявлениях о вакансиях. Этот список не исчерпывающий, но вы хотя бы получите представление о том, какие навыки вам следует развить, чтобы быть готовыми работать в интересующей вас должности.

3.3.1. Основные технические навыки

В некоторых случаях сложно понять, что подразумевается под «техническими навыками». Здесь имеются в виду знания и умения, связанные с конкретной технологией, будь то аппаратное обеспечение, программное обеспечение или что-то другое. Уровень таких навыков легко измерить, что потенциальные работодатели иногда и делают. Подробнее об этом мы поговорим в главе 5.

Учитывая, что в сфере кибербезопасности востребован широкий спектр навыков, ожидать от соискателя совершенного владения всеми было бы нереалистично. Кроме того, набора навыков, универсального для каждого специалиста в этой области, нет. Важно понять, какие из них наиболее важны для интересующей вас должности, а затем разработать план их развития.

Разработка программного обеспечения / программирование

Многие должности в области кибербезопасности требуют определенного опыта в разработке программного обеспечения или знания конкретного языка программирования. Некоторые участники сообщества считают, что владеть такими навыками обязательно. На мой взгляд, это чересчур (в разговоре о необходимых навыках таких обобщений следует избегать), однако нельзя не согласиться с тем, что знание языка программирования — или, что еще лучше, опыт в разработке программного обеспечения — будут очень полезны специалисту по кибербезопасности.

Владение одним или несколькими языками программирования — актуальный навык, поскольку специалистам по безопасности часто приходится писать сценарии или небольшие программы для автоматизации выполнения задач. Чрезвычайно полезным будет хорошо овладеть такими языками сценариев, как Perl, PowerShell, Bash или Python. К последним трем специалисты по безопасности прибегают особенно часто.

Операции по обеспечению безопасности обычно предполагают использование сценариев для автоматизации задач, поиска в журналах или интеграции нескольких систем мониторинга. Сценарии пригодятся специалистам по цифровой криминалистике и реагированию на инциденты, отвечающим за выявление брешей в системе безопасности организации, а также за поиск и хранение улик, которые позже могут быть использованы для судебного преследования нарушителей. Сценарии позволяют проводить поиск по большим объемам данных, давать скоординированный ответ на инциденты и анализировать собранные улики. Сценарии могут пригодиться даже при тестировании на проникновение для выполнения повторяющихся задач и быстрого сканирования больших наборов данных.

Еще один важный навык — понимание других экосистем разработки. Группы по безопасности часто привлекают к поиску и устранению уязвимостей в программном обеспечении. Понимание того, как работает код, лежащий в основе программы, может помочь при моделировании атак на ПО, призванном обнаружить его слабые места. Такая практика называется *наступательной безопасностью*, или *атакой «красной команды»* (red teaming). Также этот навык оказывается полезен в статическом анализе кода и анализе состава программного обеспечения. А еще он помогает понимать уязвимости, опирающиеся на особенности использования экосистем разработки. Например, многие экосистемы используют сторонние зависимости с открытым исходным кодом. Способность понимать, когда и как применяются эти зависимости, и выявлять связанные с ними уязвимости может оказаться чрезвычайно полезной.

Наконец, опыт программирования пригодится специалистам, отвечающим за безопасность приложений. Понимая жизненный цикл разработки ПО и функционирование конвейера поставки, эти специалисты могут действовать превентивно. Решение вопросов безопасности на более ранних этапах разработки обычно называется *сдвигом влево*. Понимание таких терминов, как *пользовательская история* (описание желаемых функций ПО), *бэклог* (список пользовательских историй, подлежащих реализации) и *спринты* (повторяющиеся циклы разработки программного обеспечения), а также контекста, в котором они используются, помогает более эффективно взаимодействовать с командами разработчиков. Таким образом, специалист по безопасности, обладая

знаниями в области программирования и разработки, может получить существенное преимущество.

Использование и администрирование сетей

Это может показаться очевидным, но понимать, как взаимодействуют системы, соединенные в сеть, чрезвычайно полезно для специалистов по безопасности. Многие аналитики SOC, цифровые криминалисты и сотрудники, отвечающие за реагирование на инциденты, начинают карьеру в качестве сетевых администраторов. Знакомство с такими концепциями, как модель TCP/IP, коммутация пакетов, маршрутизация и система доменных имен (DNS), оказывается весьма кстати, если вы отвечаете за мониторинг сети с целью выявления атак. Администрирование брандмауэров и других сетевых устройств безопасности тоже требует хорошо понимать принципы функционирования сетей. А если вы занимаетесь цифровой криминалистикой, отвечаете за реагирование на инциденты, изучаете данные SIEM-систем или расследуете недавний взлом, то эти знания вам просто необходимы.

Работа «красной команды» и тестирование на проникновение также немыслимы без понимания особенностей сетевых коммуникаций. В конце концов, эти практики предполагают манипулирование трафиком, обнаружение и обход средств защиты и не только. А потому необходимо уметь анализировать низкоуровневый сетевой трафик и управлять им, чтобы получать желаемые ответы или выявлять аномальное поведение системы.

Разумеется, специалист по безопасности может сосредоточиться на различных формах сетевых коммуникаций. Если вы знакомы с моделью взаимодействия открытых систем (OSI), то знаете о семи уровнях взаимодействия. В зависимости от должности, на которую вы претендуете, вам потребуются знания о том или ином уровне этой модели. Было бы трудно найти специалиста по безопасности, который разбирается в сетевых коммуникациях и говорит, что это не пригодилось ему в работе. Таким образом, знания в этой области могут открыть для вас множество дверей в мире безопасности.

Облачные технологии

Все больше организаций обращаются к облачным средам вроде Amazon Web Services (AWS), Microsoft Azure и Google Cloud: они избавляют от необходимости покупать собственные серверы и сети и позволяют пользоваться оборудованием поставщиков услуг. Эти среды предъявляют особые требования к безопасности и администрированию.

Такие новые облачные технологии, как контейнеры (виртуализированные и, как правило, компактные программно-определяемые

серверные модули), бессерверные среды и оркестрация, набирают популярность по мере того, как культура разработки DevOps привлекает к себе все больше внимания. По этой причине растет спрос на специалистов по безопасности, которые понимают связанные с ними уникальные угрозы и владеют инструментами для администрирования этих технологий и сред.

Иметь представление о том, что такое облачные среды и технологии, может быть полезно в работе на многих должностях. Умение ориентироваться в этих средах, понимание их конфигурации, а также знакомство с их средствами защиты и способами их обхода пригодится специалистам, занимающимся операциями по обеспечению безопасности, а также членам «красной команды».

Тем, кто отвечает за защиту, это знание поможет обеспечить более высокий уровень безопасности среды, а тем, кто отвечает за наступление, — более эффективно ее атаковать. Понимать, какую пользу способны принести данные, журналы и инструменты, важно даже специалистам по цифровой криминалистике и реагированию на инциденты. Они могут использовать облачные инновации, чтобы повысить эффективность мониторинга, ведения журналов и расследования инцидентов. По мере роста популярности облачных сред будет расти и спрос на профессионалов, обладающих этими навыками.

Криптография

Это еще один технический навык, важность которого кажется очевидной, но который все равно заслуживает отдельного разговора. *Криптография* — фундамент многих систем, которые обеспечивают безопасность в различных направлениях: от сетевых коммуникаций до информации в базах и репозиториях. Поэтому провести успешную атаку на криптографические алгоритмы, стоящие на страже наших данных, узнать о методах реализации этих алгоритмов и о том, какая структура лежит в их основе, — предел мечтаний злоумышленников и преступников.

Часть нашей работы как профессионалов в области безопасности — сделать так, чтобы криптографические технологии применялись должным образом, надежно защищались и не содержали уязвимостей, которые могут быть использованы для того, чтобы получить доступ к конфиденциальной информации. Специалистам по безопасности важно уметь оценивать целесообразность применения конкретных технологий шифрования, а также связанные с ними риски.

Учитывая, что криптография — неотъемлемая часть средств защиты, а потенциальные эксплойты обладают огромной ценностью, понимать хотя бы основные концепции здесь очень важно практически для каждого специалиста в сфере безопасности. Глубокие познания в области

алгоритмов и их математического обоснования, вероятно, для большинства излишни, однако полезно было бы видеть разницу между формами шифров (алгоритмов защиты данных) и иметь представление о характеристиках, благодаря которым они подходят для одного приложения и не годятся для другого.

Социальная инженерия

Социальная инженерия предполагает обман с целью манипулирования человеком и получения доступа к защищенному ресурсу. Вам может показаться, что навыки социальной инженерии не относятся к техническим, но вы ошибаетесь.

Да, здесь необходимо уметь общаться с людьми. Однако социальная инженерия также выработала конкретные тактики, методы и подходы. Недостаточно просто разговаривать с людьми — надо понимать, как работает человеческий мозг. У специалистов по социальной инженерии есть конкретная методология, помогающая определить цель, составить план действий и подготовиться к импровизации.

Навыки социальной инженерии также широко применяются в сфере кибербезопасности. Разумеется, есть профессионалы, чья обязанность — получить физический доступ к зданиям и данным через прямое взаимодействие с людьми. Однако такие интерактивные задачи, как *фишинг* (техника социальной инженерии, предполагающая использование электронной почты) или *вишинг* (голосовой фишинг), могут быть поручены сотрудникам, занимающимся оперативной деятельностью. В целом способность влиять на людей пригодится в любой работе, но особенно полезна в сфере безопасности, где специалисты часто являются источником негатива.

Обеспечение физической безопасности

Концепция *физической безопасности* размывает границу между информационной и кибербезопасностью. Такие физические средства контроля доступа, как дверные замки, системы электронной аутентификации, камеры наблюдения, системы обнаружения вторжений и физические барьеры, необходимы для защиты цифровых активов не меньше, чем криптография, средства сетевой защиты и тому подобное.

Во многих организациях за физическую и информационную безопасность отвечают разные группы. Однако в рамках кибербезопасности крайне важно, чтобы эти специалисты работали вместе. Многие современные средства контроля физического доступа полагаются на ряд ИТ-ресурсов, чья безопасность имеет огромное значение. Как правило, для этих систем характерен уникальный набор угроз и рисков, поэтому здесь могут быть уникальны и контрмеры.

Иногда мониторинг и защиту этих систем поручают оперативным группам, отвечающим за информационную безопасность, а потому понимать, как они функционируют и какие им свойственны уязвимости, может оказаться важным для специалиста SOC. Пентестеры также извлекут пользу из подобных знаний, столкнувшись с ними в сети, которую тестируют. Кроме того, существуют специалисты по *тестированию на физическое проникновение*: они отвечают за взлом средств физической защиты конкретного объекта.

Интерес к средствам физической защиты отчасти обусловлен тем, что их связь с реальным миром более осязаема, чем у бесплотных ИТ-систем. Однако не стоит переоценивать важность этих навыков в контексте кибербезопасности. Например, на многих конференциях по ИБ есть тематические зоны, называемые «деревнями», в том числе «деревня взлома замков», где участники могут узнать о различных типах замков и инструментах для их взлома. Однако, несмотря на высокий интерес к теме, шанс применить эти навыки на практике минимален. Джейсон Стрит, признанный специалист по тестированию на физическое проникновение, на одной из конференций заявил, что рабочие задачи почти никогда не требуют от него использовать его навыки взлома замков. Таким образом, хотя понимать устройство замков и их слабых мест иногда оказывается полезно, без умения их взламывать вполне можно обойтись.

Промышленные системы управления

Промышленные системы управления (ICS, industrial control system) — это ИТ-системы, устройства и сети для контроля и мониторинга физического оборудования и промышленных процессов. Под оборудованием и процессами могут пониматься производственные линии, системы управления складами и коммунальными услугами и тому подобное.

При обслуживании таких систем специалисты по безопасности сталкиваются с особым набором проблем, поскольку в них используются уникальные протоколы связи и устройства. В качестве примеров можно привести систему *диспетчерского управления и сбора данных* (SCADA), *программируемые логические контроллеры* (ПЛК), *диспетчерские пункты управления* (MTU) и *удаленные терминалы* (RTU).

Особая проблема безопасности ICS-систем заключается в том, что многие из них изначально не предназначались для подключения к крупным корпоративным сетям. Зачастую предполагается, что они будут изолированы от остального сетевого трафика и защищены. Эта проблема усугубляется тем, что во многих таких системах используются упрощенные версии ОС или даже специально разработанное встраиваемое ПО, и они не поддерживают многие из функций защиты, созданные для обычных ИТ-систем.

Таким образом, знакомство с системами управления этого типа может пригодиться специалистам по безопасности, работающим в сфере производства, коммунальных услуг, логистики и прочих подобных отраслях. С осознанием, что таким системам нужна защита, вырос спрос на специалистов, обладающих соответствующими навыками. Так что понимание уникальных характеристик этих систем, их уязвимостей и методов их защиты может открыть множество дверей в области кибербезопасности.

Радиосвязь

Рост популярности так называемых умных устройств и интернета вещей способствует распространению беспроводной связи, что создает совершенно новый ландшафт угроз. При защите беспроводных сетей необходимо учитывать особенные соображения безопасности, не характерные для традиционных сетей.

В контексте ИТ беспроводные коммуникации у людей чаще ассоциируются с технологиями вроде Wi-Fi и Bluetooth. Однако во всем, от умных устройств до глобальных сетей, используется целый ряд других специализированных средств радиосвязи. Даже если они поддерживают традиционные протоколы TCP/IP, они реализованы на основе уникальной технологии со своими уязвимостями. Поэтому каждой такой технологии свойствен уникальный набор рисков и угроз, которые необходимо понимать.

Степень защиты этих коммуникаций напрямую зависит от того, насколько хорошо специалист по безопасности разбирается в этих рисках и угрозах. Он должен уметь отвечать на следующие вопросы.

— Как и где в стеке происходит шифрование, если оно вообще имеет место?
— Можно ли заблокировать или внедрить трафик и какие возможности предусмотрены в стеке коммуникационных протоколов для решения таких проблем?
— Надежно ли защищена базовая прошивка устройств связи?

Разумеется, что интересует сотрудников по безопасности, интересует и потенциальных злоумышленников, а значит, и профессионалов, отвечающих за наступательную безопасность. Создается впечатление, что с распространением беспроводных коммуникаций организации и частные лица уделяют все меньше внимания их безопасности. Поэтому способность правильно оценивать степень защиты этих каналов связи имеет решающее значение для современных специалистов по тестированию на проникновение.

Вполне разумно ожидать, что радиосвязь будет все более активно применяться в сфере информационных технологий, что будет сопровождаться ростом спроса на специалистов по безопасности, обладающих знаниями о ней.

3.3.2. Гибкие навыки

Технические навыки играют важную роль в поиске работы в сфере кибербезопасности. Однако новички и профессионалы часто упускают из виду значимость так называемых *гибких навыков*. Эти умения не связаны с конкретной технологией или системой, но применимы в разной деятельности. В качестве примера можно привести навыки межличностного общения и управления рабочей нагрузкой.

Даже менеджеры по найму зачастую уделяют основное внимание техническим навыкам соискателя, считая гибкие навыки всего лишь полезным дополнением. Однако кандидат вполне может напомнить менеджеру о важности этих умений для работы в любой должности. Так что потенциальным соискателям стоит отточить не только технические, но и гибкие навыки.

Владение этими навыками обычно схоже с врожденными талантами. Одним людям эти умения даются сами собой, а другим нужно время, чтобы их освоить. Самоанализ для выявления своих сильных и слабых сторон в гибких навыках может потребовать усилий, но это чрезвычайно мощный инструмент для планирования саморазвития. О стратегиях оценки технических и гибких навыков мы подробно поговорим в главе 4. А пока давайте рассмотрим некоторые из них.

Исследовательские навыки

Если вы спросите менеджеров по найму, какие качества они ищут в специалисте по кибербезопасности, то двумя самыми распространенными будут *любознательность* и *страсть*. Способность досконально проанализировать интересующую ситуацию и найти нужные ответы чрезвычайно важна для реализации эффективных средств защиты. Некоторые из лучших специалистов по безопасности не склонны просто принимать ситуацию такой, какая она есть: они стремятся понять, *почему* она сложилась именно так. Любознательность подпитывает желание *исследовать* ситуацию, чтобы глубже в нее вникнуть. Как только человек разберется в ситуации, его креативность и новаторский дух могут подтолкнуть его к новым идеям.

Исследовательские навыки много значат в тех случаях, когда человек даже не знает, с чего начать. Эффективность исследования зависит

от способности находить нужную информацию, задавать правильные вопросы и в результате исчерпывающе на них отвечать.

В какой-то степени исследование предполагает готовность экспериментировать, то есть выдвигать гипотезы относительно вероятного ответа и проверять их. Например, если я вижу, что моя SIEM-система часто выдает оповещения определенного типа, я могу предположить, что это происходит из-за того, что уязвимое устройство в моей сети подвергается атаке. Я могу исследовать трафик, генерирующий эти оповещения, чтобы выяснить, выступает это устройство его источником или приемником. Если я пойму, что моя гипотеза неверна, то продолжу выдвигать новые гипотезы на основе полученной информации и проверять их, пока не найду ответ.

Совершенно очевидно, что эти навыки применимы во всех направлениях сферы кибербезопасности. Неважно, идет ли речь о защите или о наступательной безопасности, специалисты должны стремиться полностью разобраться в произошедшем инциденте и эффективно на него отреагировать. Только поняв, почему возникла та или иная проблема, вы сможете начать искать способ ее устранить.

Навыки решения проблем

Следующее умение, важное для профессионалов в области безопасности, навык *решения проблем*. Это здорово, что вы понимаете ситуацию и то, почему она возникла, но, чтобы ее изменить, вам потребуются навыки решения проблем. Может показаться, что решение проблемы и исследование — синонимы, но на самом деле это разные, хоть и связанные понятия, одно из которых ведет к другому. Многие люди умеют проводить исследования, но не знают, что делать с полученными фактами. Поэтому очень важно учитывать разницу между этими навыками и оценивать их отдельно.

Как говорилось ранее, решение проблемы предполагает сбор фактов о текущем состоянии, определение желаемого состояния и составление плана, как от текущего перейти к желаемому. Такой подход можно применять в бесчисленных аспектах кибербезопасности. Например, чтобы решить проблему недостаточной сложности пользовательских паролей.

Если я знаю, что пользователи моей системы используют слабые, уязвимые для взлома пароли, то мне известно текущее состояние. Но одного этого факта недостаточно для решения проблемы. Мне нужно понять, почему пользователи не используют более сложные пароли. Связано ли это с тем, что их не поддерживает система? Или с тем, что сложные пароли труднее запомнить? Мне нужно провести исследование, чтобы выяснить это. В ходе исследования я обнаруживаю, что система поддерживает более сложные пароли, так что проблема не в этом.

Затем я провожу опрос пользователей и выясняю, что люди используют слабые пароли, потому что им трудно управляться со сложными. Теперь я могу начать искать решение.

Чтобы исправить ситуацию, мне нужно придумать возможные варианты и определить, какой из них позволит из текущего состояния (пароли уязвимы для взлома) прийти к желаемому (пароли труднее скомпрометировать). Учитывая факты, я понимаю, что нужно упростить порядок использования надежных паролей. Для этого я могу развернуть менеджер паролей: он избавил бы пользователей от необходимости запоминать комбинации. Или внедрить схему биометрической аутентификации и вообще отказаться от паролей. Придумываем варианты, выбираем тот, который позволяет перейти к целевому состоянию, и составляем план действий — вот суть этого навыка.

Однако не все проблемы столь просты, особенно когда речь идет о кибербезопасности. Поиск решений, позволяющих прийти к желаемому состоянию, часто требует творческого подхода. Способность через анализ находить неочевидные решения отличает тех, кто хорош в решении проблем, от обычных людей. А еще, выбрав вариант решения и составив план, надо наладить сотрудничество с теми людьми, которых оно затрагивает, а также с теми, кто может помочь его выполнить.

Навыки сотрудничества

Способность работать совместно с другими сотрудниками организации — основополагающая для специалистов по кибербезопасности. От ее наличия может зависеть то, сможете вы повысить уровень безопасности своей организации или погрязнете в однотипных проблемах. *Сотрудничество* предполагает развитый навык выбирать людей, способных помочь в достижении цели, и эффективно взаимодействовать с ними.

Будь то попытка устранить уязвимость, обнаруженную в ходе недавнего теста на проникновение, выяснение, почему растет число предупреждений от SIEM-системы, или внедрение новой схемы аутентификации, инициативы в области безопасности редко реализуются одной группой. Для достижения цели сотрудники службы безопасности должны быть готовы взаимодействовать со специалистами из других подразделений. Если человек плохо ладит с другими, например ведет себя резко, не желает делиться информацией и принимать чужие идеи, то, скорее всего, ему не удастся эффективно исполнять роль в области безопасности.

Суть сотрудничества заключается в умении взаимодействовать и идти на компромисс с людьми, у которых могут быть другие цели и обязанности. Это способность влиять на других, а также принимать

и реализовывать их идеи, чтобы изменить текущую ситуацию. Этот важный навык пригодится сотрудникам множества подразделений. Однако еще более актуален он для специалистов по кибербезопасности — учитывая, что та затрагивает каждую из функций компании. Если вы собираетесь внедрить новую технологию биометрической аутентификации, то вам придется работать с сетевыми администраторами, группой технической поддержки и пользователями, чтобы гарантировать ее успешное развертывание и повсеместное применение. Чтобы привлечь всех этих людей к сотрудничеству, вы должны быть способны понимать их мотивы, опасения и приоритеты.

Эмпатия / эмоциональный интеллект

Эмпатия — это способность понимать эмоции и чувства других людей и сопереживать. Чтобы влиять на других, человеку необходимо сочетать эмпатию с эмоциональным интеллектом. *Эмоциональный интеллект* — это способность человека анализировать свои эмоции и эффективно их выражать. Если вы умеете понимать чужие и собственные эмоции и устранять разрыв между ними, выбирая подходящий способ общения, вы сможете заручаться поддержкой нужных людей.

Этот навык чрезвычайно важен как при горизонтальной, так и при вертикальной коммуникации. В первом случае специалист по безопасности стремится получить поддержку и помощь от людей того же уровня в организационной иерархии. А вертикальная коммуникация предполагает попытку повлиять на непосредственных руководителей. В обоих случаях необходимо учитывать заботы и приоритеты этих людей и мотивировать их к нужным действиям.

Многие недооценивают этот навык, но он необходим специалистам по кибербезопасности. Некоторые из них не продвигаются по карьерной лестнице, поскольку не имеют навыков межличностного общения. Развитие эмпатии и эмоционального интеллекта может здесь помочь.

Многозадачность и организаторские способности

Вероятно, не найдется такого специалиста по кибербезопасности, за чье внимание ежедневно не конкурировало бы множество задач. В этой сфере практически в любой работе есть конкурирующие цели, над которыми приходится работать параллельно и методично. Способность принимать разнообразные входные данные, структурировать и приоритизировать их, а затем планомерно обрабатывать называется *многозадачностью*.

Многозадачность часто упоминается в вакансиях на должности, связанные с безопасностью. К сожалению, не все специалисты обладают этим навыком. Некоторые люди привыкли выполнять одну задачу

за раз и полностью закрывать ее, прежде чем приступать к следующей. Однако в сфере кибербезопасности такой подход не работает.

Хорошая новость заключается в том, что этот навык, как и любой другой, вполне можно развить. Способность к многозадачности и организованности предполагают внимание к деталям и методичность в планировании. Тем, кто не умеет работать над несколькими задачами сразу, полезно придерживаться структурированного процесса. Если у вас с этим трудности, обратите внимание на источники, касающиеся тайм-менеджмента и развития организаторских способностей, чтобы разработать собственный метод управления нагрузкой.

Навыки письменной коммуникации

Еще один гибкий навык, который необходимо развивать, — это *навык письменной коммуникации*. Пентестер вы, специалист по реагированию на инциденты, архитектор безопасности или социальный инженер — неважно; вы должны уметь излагать свои идеи, предложения и выводы в письменной форме.

От этого навыка зависит многое в случае, когда необходимо получить поддержку от других людей, и нет разницы, идет ли речь о новой инициативе или об устранении уязвимости. Пентестер, не способный подробно описать обнаруженную им уязвимость так, чтобы его клиент его понял, не эффективен как сотрудник. Специалист по реагированию на инциденты, не способный представить детали ситуации достаточно ясно, чтобы руководство определилось с будущей стратегией, не справляется со своей ролью. То же самое можно сказать о любой должности в сфере безопасности.

При поиске работы важно помнить, что ваши навыки письменной коммуникации потенциальный работодатель будет оценивать в первую очередь. Ваши резюме и сопроводительное письмо первыми отразят то, насколько эффективно вы способны общаться в письменной форме.

К счастью, такие навыки тоже можно развить: этой теме посвящены множество учебных курсов, видеороликов и книг. Если ваш уровень в этой части оставляет желать лучшего, уделите первоочередное внимание развитию таких скиллов, особенно учитывая то, как они влияют на успешность в поиске работы.

Навыки публичных выступлений

И наконец, важно подумать над совершенствованием *навыков публичных выступлений*, или *презентационных навыков*. Как говорилось ранее, специалистам по безопасности часто приходится представлять идеи и концепции сотрудникам других подразделений. Вас могут попросить изложить группе людей результаты ваших исследований, предложение по внедрению новых технологий и так далее.

Не все должности в сфере безопасности требуют умения выступать перед большой аудиторией, но почти каждая требует умения эффективно делиться своими идеями и знаниями с людьми, далекими от этой сферы. Развитие презентационных навыков должно быть приоритетом для всех, кто работает или собирается работать в сфере безопасности.

ПОДВЕДЕНИЕ ИТОГОВ

- Несмотря на то что множество вакансий в области кибербезопасности не закрыты, начинающим и опытным специалистам трудно найти работу. Больше четверти опрошенных тратят на это более полугода.
- В сфере кибербезопасности есть разные уровни должностей, каждая со своими обязанностями. Хотя многие люди стремятся в карьере занять руководящую должность, эта работа подходит далеко не всем.
- Начинающим специалистам по безопасности следует развить некоторые технические навыки. Хотя нет универсального набора, многие технические навыки широко применяются в различных направлениях сферы кибербезопасности.
- Новички в сфере безопасности часто упускают из виду, а менеджеры по найму недооценивают гибкие навыки. Тем не менее соискателю следует оценить свой уровень владения ими и развить те, которые пригодятся в любой должности в сфере кибербезопасности.

Часть II

Подготовка к поиску работы

Тот факт, что вы дочитали до этого места, означает, что, получив более глубокое представление о кибербезопасности, вы все равно хотите построить карьеру в этой области. Это отличная новость — поздравляю!

Теперь, когда мы обсудили сферу, пришло время поговорить о *вас*. Любой карьерный путь начинается с самоанализа и планирования. Вы уже знаете, насколько обширны возможности в области кибербезопасности, но, вероятно, у вас есть множество вопросов, или вы не знаете, какое направление подходит именно вам. Кроме того, вы, должно быть, еще не готовы обсуждать практические карьерные стратегии.

Поэтому в главе 4 мы поговорим о вас и о том, как ваши интересы соотносятся с различными ролями в сфере кибербезопасности. Здесь вы найдете несколько упражнений, которые вам в этом помогут. Вы также узнаете, как применить свои базовые навыки в работе на различных должностях.

Глава 5 посвящена развитию навыков, необходимых для карьеры в сфере кибербезопасности. Мы поговорим о вариантах обучения и сертификации, а также о том, как они влияют на поиск вашей первой работы. Здесь упоминаются даже менее формальные виды обучения: так вы получите более полное представление о способах развития навыков.

Наконец, в главе 6 мы поговорим о стратегиях поиска первой работы. Мы рассмотрим тактики, касающиеся составления резюме, подготовки

к различным формам собеседований и даже ведения переговоров, чтобы вы получили наилучшее из возможных предложений.

Пришло время выяснить, какие практические шаги позволят вам ступить на этот новый карьерный путь. Вооружившись знаниями из второй части руководства, вы будете готовы приступить к поиску своей первой работы в сфере кибербезопасности.

Глава 4
Выбор наименее исхоженного пути

В этой главе

- Распространенные проблемы, с которыми сталкиваются соискатели-новички в сфере кибербезопасности
- Самоанализ и формулирование личной цели
- Соотнесение имеющихся навыков с личной целью и потенциальными ролями в сфере кибербезопасности
- Составление перечня способностей
- Выявление и фиксирование пробелов в навыках

Лучший способ подготовиться к поиску первой работы в сфере кибербезопасности — осознать, что наилучшего способа не существует. Мои подписчики в социальных сетях постоянно спрашивают: «Как начать работать в сфере кибербезопасности?» Многих интересует пошаговый алгоритм, которому они могли бы следовать. Некоторые хотят узнать, какое обучение или сертификация позволит им получить работу. Но дело в том, что универсального пути нет. Среди всех профессионалов специалисты по кибербезопасности, вероятно, имеют самый разнообразный опыт и самые необычные карьерные маршруты.

Чтобы выбрать правильный путь для развития навыков и подготовки к поиску первой работы, следует начать с самоанализа. Вы должны понять свои цели. Разумеется, со временем они могут измениться, но конкретные ориентиры необходимы. Вам надо проанализировать, что именно мотивирует вас заняться этим делом и что способно разжечь вашу страсть. Эти мотивация и страсть пригодятся вам в карьере.

Однако если бы мотивации и страсти было достаточно, то каждый третий начинающий специалист по кибербезопасности не искал бы свою первую работу по полгода. Вам также необходимо проанализировать свои способности. В главе 3 мы обсудили распространенные технические и гибкие навыки, важные для построения карьеры в этой области. Вы должны объективно оценить их уровень у себя. Вам также следует усвоить концепцию базовых навыков. Таланты, способности и опыт могут не иметь очевидной связи с навыками, необходимыми специалисту по кибербезопасности. Однако, если вы разобьете их на базовые навыки, вам будет легче применить их в своей новой роли.

Тем не менее оценка навыков и понимание того, как их применить в интересующих вас ролях, — это еще не все. Вам также необходимо проанализировать пробелы в своих навыках: подумать, какие из них вам понадобятся, чтобы работать в желаемой должности, а затем найти возможность их развить. Весь этот процесс описан далее.

4.1. Сложности, с которыми сталкиваются новички

Начать новую карьеру — необычайно трудная задача и для выпускника, и для того, кто хочет сменить профессию. Один из самых трудных этапов этого пути — найти первую работу. Это должна быть должность, позволяющая развивать свои навыки и вместе с тем вносить вклад в деятельность команды. Однако в сфере безопасности найти такую вакансию, которая не требует от соискателя уже развитых профессиональных навыков, чрезвычайно сложно.

4.1.1. Получение ученой степени в области кибербезопасности

Система образования попыталась решить проблему нехватки специалистов в сфере кибербезопасности. Сегодня университеты предлагают огромное количество программ, позволяющих получить ученую степень в этой области. Каждый год тысячи студентов записываются на них в надежде, что наличие степени ускорит поиск первой работы. К сожалению, данные моего опроса такой корреляции не отражают (см. рис. 4.1).

Однако пусть эти данные вас не расстраивают. Ученая степень по-прежнему имеет значение и может дать вам преимущество перед кандидатом, который в остальном от вас ничем не отличается, особенно если вы оба претендуете на должность начального уровня. Кроме того, многие организации по-прежнему настаивают на том, чтобы их сотрудники имели высшее образование. Учитывая, что получение образования, скорее всего, в любом случае входит в ваши планы, вы вполне можете выбрать для изучения именно направление кибербезопасности.

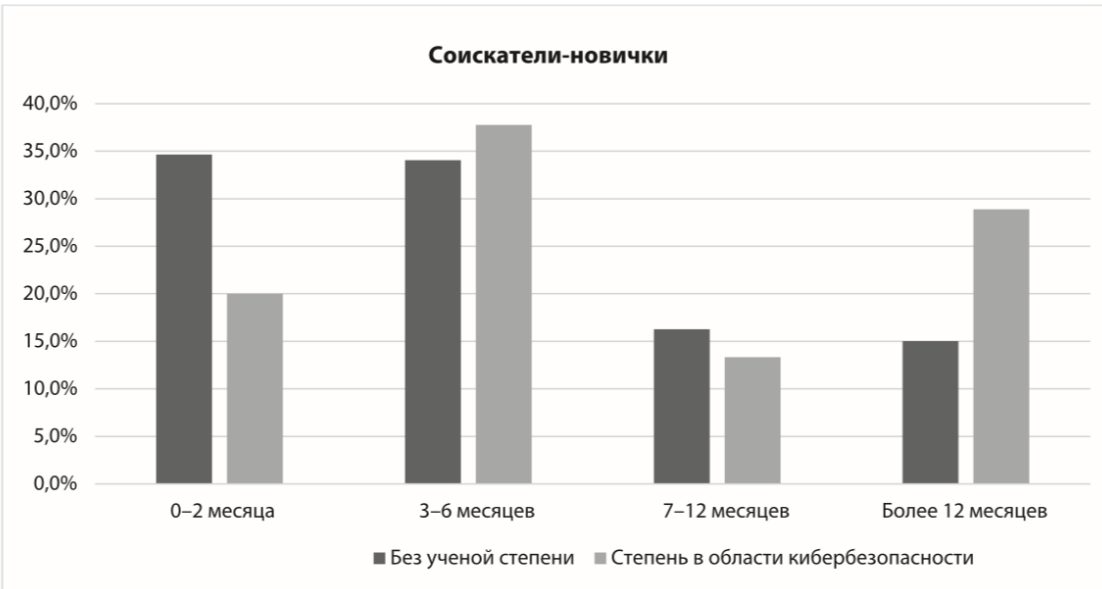

Рис. 4.1. Наличие ученой степени в области кибербезопасности не ускоряет поиск первой работы

Однако важно понимать, что ученую степень нельзя назвать стандартным этапом карьерного пути в этой сфере. Важная концепция, которая неоднократно подчеркивается в этой книге, заключается в том, что *единственного способа построить карьеру в сфере кибербезопасности не существует*.

4.1.2. Поиск своего пути в сфере кибербезопасности

Если вы спросите опытных специалистов по кибербезопасности, как они пришли в эту область, то обнаружите, что многие из них вообще не имеют типичного технического образования. Например, Алет Денис,

победившая в конкурсе Social Engineering Capture the Flag (CTF)[7] на DEF CON 27[8], получила черный значок DEF CON — одну из высших наград для участников хакерского сообщества. Можно было бы подумать, что человек, отмеченный такой наградой, пришел в область кибербезопасности еще в подростковом возрасте и прошел здесь долгий путь. Однако в случае с Денис это не так.

В ходе интервью для этого руководства Денис рассказала, что попала в сферу безопасности не так давно и совершенно неожиданным образом. На момент написания книги она по-прежнему работала специалистом по анализу рынка в крупной фирме по подбору персонала. Она занялась кибербезопасностью меньше чем за три года до своей крупной победы на DEF CON, когда открыла свой небольшой бизнес Dragonfly Security, который развивает в свободное от основной работы время. До этого у нее не было никакого опыта деятельности в этой сфере; все знания она получила в ходе самообразования и общения с другими профессионалами. И ее история — лишь одна из многих. Это уникальная особенность сообщества безопасности, из-за которой в то же время к нему не так легко присоединиться.

Я посвятила целый раздел описанию множества карьерных путей в сфере кибербезопасности, чтобы вы знали, что вне зависимости от своего опыта можете найти себе в ней место. Как говорилось ранее, разнообразие имеет критическое значение, вам просто нужно понять, как ваши навыки связаны с должностью, на которую вы претендуете, и научиться обосновывать значимость этой связи. Далее мы поговорим о том, как это сделать.

4.2. Познайте себя

Почему вы хотите начать карьеру в сфере кибербезопасности? Что вас интересует? Почему именно кибербезопасность, а не разработка программного обеспечения, управление проектами или маркетинг? Почему бы не стать врачом или юристом? Какие из аспектов кибербезопасности будоражат вас больше всего?

Я часто задаю эти вопросы людям, которые обращаются ко мне через социальные сети за помощью в построении карьеры. И меня тревожит,

---

[7] Дословно: захватить флаг. В сфере информационной безопасности — командные соревнования, в ходе которых участники решают различные задачи в условиях, схожих с реальными. Каждая верно решенная задача дает команде преимущество перед соперниками, «флаг». — *Прим. ред.*

[8] Один из крупнейших в мире ежегодных хакерских съездов. Проходит в Лас-Вегасе, США. — *Прим. ред.*

что многие не могут объяснить, почему их интересует именно эта область. Некоторые называют в качестве мотивирующих факторов высокие зарплаты и гарантии занятости. Возможно, это не самый благородный ответ, но, по крайней мере, он осознанный и честный, а это очень важно. Другие говорят, что не знают, что именно их интересует; они просто хотят больше узнать о кибербезопасности. Это тоже меня беспокоит, так как подразумевает, что люди принимают судьбоносное решение, не имея представления о том, чем собираются заниматься.

Здесь мне следует пояснить: я не считаю такой подход ошибочным или плохим. К сожалению, нельзя сказать, что профессиональное сообщество так уж хорошо потрудилось для того, чтобы у новичков сформировалось четкое представление о работе и карьерном пути в этой области. Из-за этого каждому специалисту приходится прокладывать собственный маршрут, а это начинается с понимания того, что побуждает его отчалить от берега. Нужно проанализировать, что именно вас интересует и как ваши навыки могут пригодиться потенциальному работодателю.

Этот самоанализ ляжет в основу вашей карьеры. Поэтому хорошенько подумайте, что важно для вас, чего вы хотите достичь, какие из имеющихся ресурсов могут вам в этом помочь и какие навыки вам нужно усовершенствовать, чтобы повысить шансы на успех. Первым делом следует понять, что вы за человек и что вами движет.

4.2.1. Поиск подлинного себя

Многим детям с раннего возраста говорят о том, что они могут быть кем угодно, и побуждают следовать за своими увлечениями. Однако по мере того, как на нас ложится все больше взрослых обязанностей, нас учат быть кем угодно, но только не самими собой. Пришло время вернуться к настоящему себе. При составлении заявки на вакансию крайне важно принимать в себе то, что делает вас уникальным. Кажется очевидным, что если вы хотите выделиться, то последнее, что вам нужно делать, — это составлять резюме и личную историю, прямо как все остальные. Однако большинство соискателей поступает именно так. Еще хуже то, что карьерные коучи и специалисты, рецензирующие резюме, зачастую поощряют такую стратегию.

Соискателям следует заложить основы личного бренда. Каким вы желаете предстать перед другими участниками профессионального сообщества? Чем хотите быть известны? Какую историю поведать миру? Все ваши действия в процессе поиска работы можно завязать на этот личный бренд. Если вы ищете первую работу в новой для себя сфере, то,

вероятно, не вполне уверены, как хотите позиционировать себя. Со временем вы, разумеется, можете изменить свой бренд, как это делают компании и продукты. Однако, направляя резюме рекрутерам, не забудьте отразить в нем то, что делает вас особенным.

Мой коллега Фил Гербишак рекомендует при создании личного бренда ответить на такой вопрос: «В чем ваша странность?» Он имеет в виду особенность, выделяющую вас на фоне остальных. Это должно быть что-то необычное, личное и искреннее. Особенность Фила — то, что он вырос на севере штата Висконсин, в маленьком городке, о котором почти никто не слышал. Он использует эту особенность своего происхождения, чтобы подчеркнуть масштаб своего успеха как тренера по продажам и личному брендингу. Он акцентирует внимание на этой части своей биографии, чтобы продемонстрировать влияние его уникальной точки зрения на то, как он управляет другими аспектами своей карьеры.

Это то, что следует сделать каждому соискателю, да и вообще каждому профессионалу в начале карьеры. Поэтому остановитесь на минутку и задумайтесь: что выделяет вас на фоне остальных? Что в вас такого странного или необычного? Вероятно, вы не сумеете ответить сразу; в этом случае следует потратить некоторое время на размышления.

Определившись с этим, вы сможете приступить к работе. Найдите и примите свою уникальность. Отталкиваясь от нее, создайте историю о себе, которая заставит работодателей запомнить ваше имя, а не воспринимать вас в качестве очередного ничем не примечательного соискателя. Будьте собой и используйте это, чтобы завладеть их вниманием.

Придется постараться, чтобы история затрагивала все аспекты вашего профессионализма. Излагайте ее последовательно в любой автобиографической информации, которой делитесь. Неважно где: на странице в социальной сети вроде LinkedIn или X (Twitter), в сопроводительном письме для резюме, направляемого работодателю, или в самом резюме, — убедитесь, что все источники рассказывают одну и ту же историю о вас.

Так ваши особенности будут глубже интегрированы в вашу профессиональную жизнь. Такое многократное представление собственной уникальности гарантирует, что рекрутеры и менеджеры по найму запомнят не только ваше имя, но и особенности вашей личности. Личные связи будут иметь ключевое значение на этапе поиска работы.

Упражнение: найдите свою уникальность

Следующее упражнение поможет вам найти свою уникальную черту и облечь ее в слова, которые будут направлять вас при создании личного бренда и карьеры. Важно выделить время на то, чтобы детально проработать это задание, и вы можете к нему многократно возвращаться.

В конце раздела вы используете то, что получилось, чтобы сформулировать заявление о личной цели. Итак, давайте приступим к поиску вашей особенности.

1. Представьте, что вы даете интервью газете и вас просят предоставить краткую, но исчерпывающую автобиографическую информацию.
2. Перечислите 10–15 вещей, которыми вы хотите запомниться людям.
3. Опираясь на этот список, опишите себя в единственном абзаце максимум из 200 слов. Если включить все пункты не получается, ранжируйте их и упомяните только самые важные.
4. Прочитайте абзац. Перечислите три вещи, о которых вы хотели бы рассказать подробнее.
5. Выберите аспект, выделяющийся на фоне всех остальных. Уникален ли он и хорошо ли описывает вас?

Теперь у вас есть кандидат на звание вашей особенности. Суть упражнения — найти что-то, что присуще лишь вам. Однако у этого чего-то есть предыстория, которую невозможно описать в двух словах. Узнав об этом, любой посторонний человек захочет подробностей. Это бесценный инструмент, позволяющий сделать вашу страницу в социальных сетях, профессиональную самопрезентацию и даже резюме запоминающимся и интересным. Это то, что способно выделить вас из толпы.

4.2.2. Поиск своей страсти

Страсть побуждает людей совершать великие поступки; она мотивирует нас работать ради достижения цели, несмотря на трудности. Если бы кто-нибудь прямо сейчас спросил вас, что больше всего привлекает вас в сфере кибербезопасности, смогли бы вы сразу дать ответ?

Многие люди считают кибербезопасность захватывающим направлением и мечтают в нем работать. Но, к сожалению, их рассуждения чаще всего остаются поверхностными. Если вы намерены построить карьеру в столь разноплановой области, важно решить, на чем вы хотите сосредоточить усилия. Никто не в силах овладеть всеми навыками и знаниями, имеющими отношение к кибербезопасности. Вам придется направить усилия на что-то одно. Понимание того, что именно подталкивает вас работать в этой области, поможет настроить этот фокус.

Итак, выделите время на то, чтобы разобраться в своем отношении к различным темам, связанным с безопасностью. Что вас больше всего воодушевляет? Решение головоломок? Знакомство с новыми технологиями? Постоянное обучение и развитие? Вы можете оттолкнуться

от результатов опроса начинающих специалистов по безопасности, представленных на рис. 4.2.

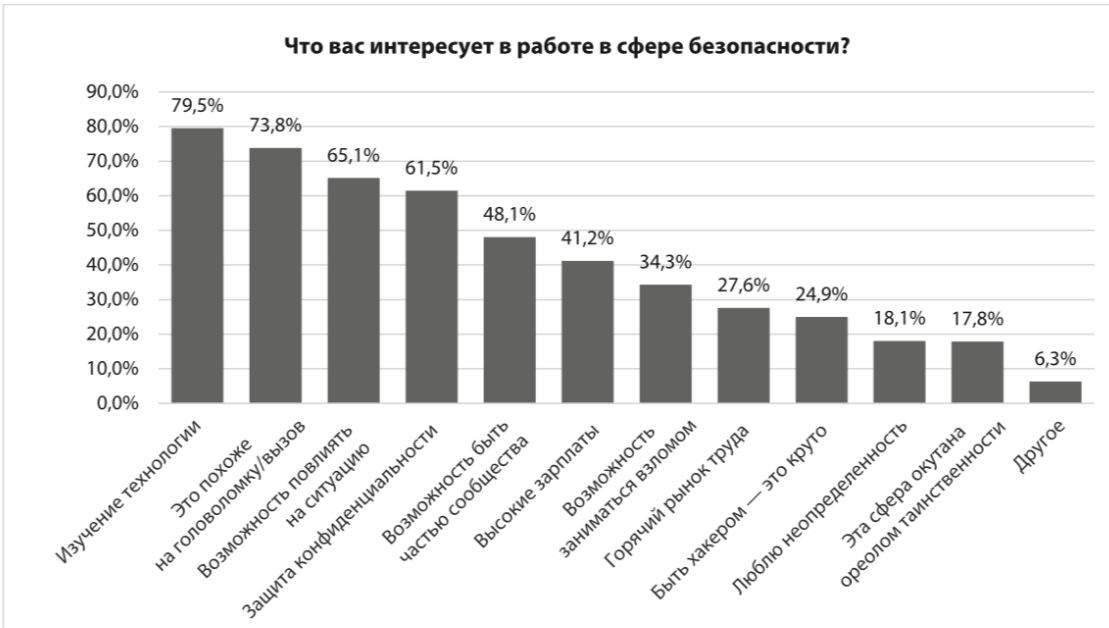

Рис. 4.2. Интересы начинающих специалистов по кибербезопасности

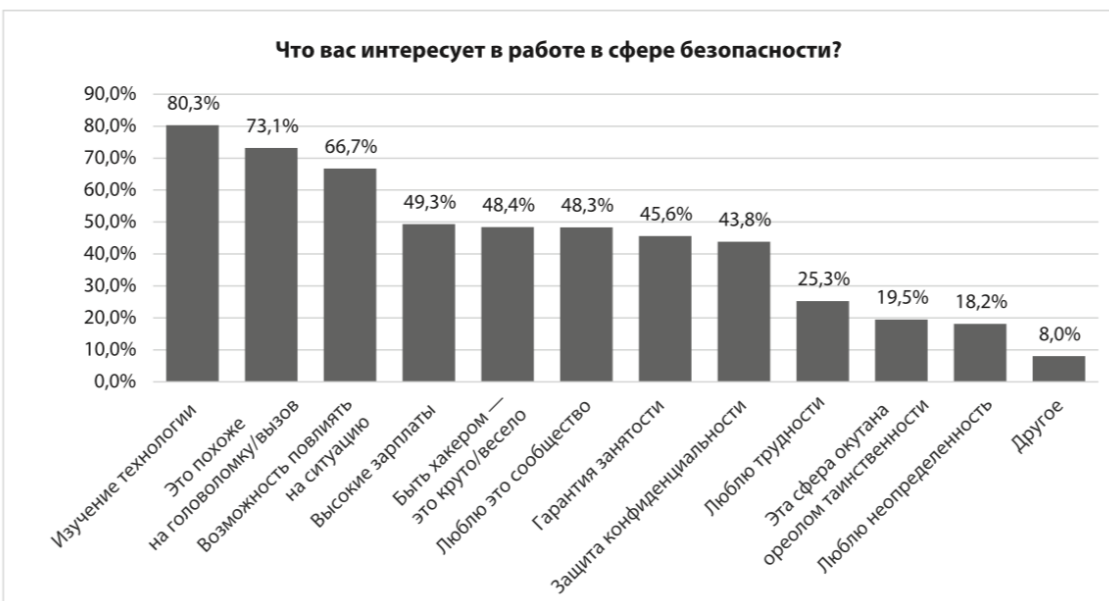

Рис. 4.3. Интересы опытных специалистов по кибербезопасности

На рис. 4.3 показаны результаты того же опроса, проведенного среди людей, которые уже некоторое время проработали в сфере кибербезопасности.

Сходство в ответах новичков и опытных профессионалов довольно показательно. Оно говорит о том, что страсть, которая приводит человека в эту область, продолжает мотивировать его на протяжении всей карьеры. Вот почему так важно разобраться с собственными мотивами. Сформулированные вами ответы могут не быть окончательными, однако если у вас появится более-менее четкое представление о том, чем вас привлекает сфера кибербезопасности, это поможет вам сосредоточить усилия на развитии ключевых навыков, соответствующих вашим интересам, и не тратить время на глубокое изучение тех областей, которые вас не особенно интересуют.

Разумеется, ваши ответы могут отличаться от ответов участников опроса. То, что интересует вас, может относиться к категории «Другое», и это здорово. Какими бы ни были ваши ответы, они помогут вам отыскать свой карьерный путь в сфере кибербезопасности.

Упражнение: найдите свою страсть

Подобный самоанализ не всегда дается легко. Людям бывает трудно выделить время, чтобы подумать о том, что их мотивирует. В этом упражнении описан простой алгоритм, помогающий преодолеть этот ментальный блок.

1. Найдите 3–5 блогов и/или новостных сайтов, посвященных кибербезопасности.
2. Скопируйте заголовки пяти первых попавшихся статей с каждого сайта и вставьте их в документ (или запишите на бумаге).
3. Опираясь исключительно на заголовки, ранжируйте статьи в соответствии с тем, насколько они вам интересны.
4. Просмотрите список и рядом с каждым заголовком напишите, почему вас интересует эта статья.
5. Проанализируйте список причин и сведите их к 3–5 категориям интересов. Названия категорий должны быть всеобъемлющими: тщательно продумайте их. Больше 5 категорий делать не стоит.

Теперь взгляните на получившиеся категории. Хорошо ли они описывают ваше отношение к сфере безопасности? Возможно, вы захотите сделать это упражнение несколько раз, поскольку новые статьи появляются ежедневно. Так или иначе, через некоторое время вы начнете замечать определенные тенденции. Это отличный способ развить самосознание.

Окончательный список из 3–5 интересов станет еще одной опорой, на которой будет строиться ваша долгосрочная карьера. Теперь пришло время объединить результаты проделанной работы.

4.2.3. Формулирование личной цели

Итак, вы потратили некоторое время на то, чтобы узнать, кто вы, каким хотите предстать перед людьми и что побуждает вас вступить в сообщество безопасности. Вы зафиксировали основные элементы своего личного бренда и причины, по которым стремитесь построить карьеру в сфере кибербезопасности. Пришло время объединить все это в заявление о личной цели.

Карьерные коучи часто рекомендуют формулировать такое заявление, какое будет служить вам ориентиром в вашем путешествии. Это то, на что вы сможете опираться не только при поиске работы, но и в ходе карьерного роста. На этом пути вам, вероятно, придется принимать трудные решения или переживать сомнения о выборе направления. Зафиксированная письменно, личная цель напомнит вам о том, как вы пришли туда, где вы находитесь, и поможет принять решение, соответствующее вашим интересам.

Ваше заявление о цели — личное. Вы можете хранить его в тайне или использовать в качестве элемента личного бренда. Как минимум важно сделать так, чтобы ваш личный бренд был основан на этом заявлении. Соответствие между личным брендом и собственной сущностью — ключевая особенность заслуживающего доверия и вдохновляющего профессионала. Я всегда рекомендую соискателям указывать свое заявление о цели или его производную в самом начале резюме. Эта привлекающая внимание фраза позволит вам заявить о своих намерениях и выделиться из толпы.

Давайте подробно разберем понятие «заявление о личной цели». Со словом «заявление» все ясно. Это некоторое утверждение, сообщающее кому-то о чем-то. Под понятием «цель» подразумевается то, чего автор заявления надеется достичь. Наконец, слово «личная» говорит о том, что сформулированная вами цель должна иметь непосредственное отношение к тому, кто вы, то есть выделять вас на фоне остальных профессионалов, ищущих работу в сфере безопасности. Я занималась наймом людей на различные должности более десяти лет и видела бесчисленное количество заявлений о целях, сосредоточенных на конкретных рабочих навыках или концепциях, но ничего не говоривших о самом человеке. Подобные резюме были самыми безликими и незапоминающимися.

Чтобы сформулировать впечатляющее заявление о цели, необходимо опереться на свою подлинную уникальность и на список увлечений: это позволит рассказать о себе и о том, чем вы хотите заниматься на протяжении карьеры. Поэтому, если вы еще не выполнили упражнения из предыдущих разделов, я настоятельно рекомендую вам сделать это, прежде чем формулировать заявление о цели. Итак, приступим.

Упражнение: сформулируйте заявление о личной цели

В заявлении о личной цели необходимо объединить ваши увлечения и особенности в утверждение из одного, максимум двух предложений. Это краткое описание того, кто вы и почему хотите построить карьеру в сфере кибербезопасности. Формат этого заявления должен быть примерно таким: «Я — (личный бренд), и моя страсть — (одно или два главных увлечения)».

Например, став хакером еще в детстве, я накопила на свой первый компьютер в 12 лет. Моя главная страсть — деконструировать технологию, чтобы ее понять и усовершенствовать. Таким образом мое заявление о цели можно сформулировать так: «Я хакер с самого детства и, с тех пор как в 12 лет купила свой первый компьютер, деконструирую технологии, чтобы их понимать и совершенствовать». Чтобы превратить свою историю в заявление о личной цели, вы можете воспользоваться следующим алгоритмом.

1. Какая идея лежит в основе вашего личного бренда? Сформулируйте ее как можно короче.
2. Выберите из списка одно или два главных увлечения, которые вы хотите подчеркнуть или которые лучше всего вписываются в вашу историю.
3. Сформулируйте заявление о цели, как было показано выше.
4. Отредактируйте заявление так, чтобы оно соответствовало вашей индивидуальности.
5. Попросите человека, которому вы доверяете, прочитать его и дать обратную связь. Вызывает ли оно желание узнать о вас больше?
6. При необходимости пересмотрите свое заявление. (Однако помните, что оно *ваше*, а не того человека, чье мнение вы спрашивали.)

Сформулировав заявление о цели, постарайтесь время от времени напоминать себе о нем. Поместите его там, где оно будет регулярно попадаться вам на глаза. Это может быть просто заметка на мониторе компьютера, или что-то художественное вроде настенного украшения, или что-то технологичное вроде сообщения, всплывающего на экране телефона или компьютера при входе в систему. Что бы вы ни выбрали, заявление о цели должно вдохновлять и напоминать вам о самом важном аспекте вашей карьеры.

4.3. Инвентаризация знаний и навыков

В предыдущем разделе вы определились с тем, что делает вас уникальным и ценным и что мотивирует строить карьеру в сфере безопасности. Теперь пришло время подумать о себе как о профессионале и объективно оценить ваши знания и навыки, что могут пригодиться в будущей работе.

Ранее мы обсудили технические и гибкие навыки, на которые чаще всего обращают внимание менеджеры по найму. Теперь давайте поговорим, как провести инвентаризацию ваших знаний, навыков и опыта.

Вам предстоит проанализировать собственные технические и гибкие навыки. Я покажу, как вывести из технического опыта, каким бы нерелевантным он вам ни казался, базовые навыки, актуальные для любой отрасли и любой должности. Если вы новичок в сфере кибербезопасности, нужно будет объяснить менеджеру по найму или рекрутеру, какими навыками, подходящими для должности, вас снабдила предыдущая работа — скажем, в качестве бариста в кафе. На первый взгляд такой подход кажется сомнительным, но опробовав его, вы обретете достаточную уверенность, чтобы представить убедительные аргументы.

В итоге вы получите ранжированный список способностей, который сможете использовать, чтобы планировать личное развитие и соотносить свои навыки с требованиями интересующих вас вакансий. Однако, прежде чем начать, важно разобраться с понятиями.

Способности — это совокупность знаний, навыков и опыта. Здесь «способности» и «набор навыков» — синонимы. Оба подразумевают комбинацию этих трех элементов, определяющих готовность человека выполнять конкретную работу. *Знание*, *навык* и *опыт* относятся к разным аспектам некоторой способности. *Знание* — это просто понимание определенных тем или концепций. Под *навыком* подразумевается умение применять это знание к задаче или ситуации. А *опыт* демонстрирует историю использования этого навыка.

4.3.1. Технические способности

Технические способности, вероятно, легче всего оценить с помощью самоанализа. О них большинство людей думают в первую очередь, когда пытаются определить, насколько они подходят для конкретной работы. Справедливости ради следует отметить, что большинство менеджеров по найму тоже уделяют им основное внимание, так что проанализировать свои технические способности — вполне уместная задача.

Однако, несмотря на это, мало кто из соискателей тратит время на инвентаризацию своих технических навыков. Большинство людей подходят к этому делу неформально: просматривают объявление о вакансии и просто отмечают те пункты обязанностей, которым удовлетворяют их способности. Однако лучше, особенно кандидату на должность начального уровня, провести формальную инвентаризацию своих технических способностей и соотнести их с требованиями по интересующей вакансии. Иногда вы можете не иметь того навыка или опыта, что требуется в конкретной вакансии, но при этом владеть смежным, не менее полезным. В следующем разделе я расскажу, как их соотнести между собой.

Единственного правильного способа провести инвентаризацию технических способностей не существует, но в любом случае крайне важно перечислить все ваши знания и опыт. Далее в этом разделе мы поговорим о том, как можно оценить их уровень. Однако для начала достаточно просто составить список навыков, которые вы в той или иной степени сумели развить на протяжении своей профессиональной и личной жизни.

Упражнение: составьте список технических способностей

Цель этого упражнения — составить исчерпывающий список технических способностей, охватывающих все релевантные знания, навыки и опыт. В дальнейшем вам предстоит обновлять этот список периодически или с поступлением новой информации.

Велика вероятность, что за один раз вам не удастся перечислить все свои технические способности. Скорее всего, создав первоначальный вариант списка, вы спустя время поймете, какими пунктами его необходимо дополнить. Кроме того, вы будете обновлять по мере роста и развития. Так или иначе, с чего-то нужно начать, и сделать это можно следующим образом.

1. Создайте таблицу с четырьмя столбцами: «Способности», «Знания», «Навыки» и «Опыт».
2. Сначала подумайте о своей текущей или последней работе и перечислите все задачи, которые вам приходилось решать, в столбце «Способности». Укажите как можно больше, но не тратьте на это более 10 минут.
3. Сделайте то же самое для каждой работы, что у вас когда-либо была.
4. Поставьте крестики в каждом из трех столбцов рядом с перечисленными способностями. Вы делали эту работу, следовательно, обладаете соответствующими знаниями, навыками и опытом.
5. Затем вспомните все формальные образовательные программы, какие вы проходили. Перечислите все дисциплины, которые еще не указаны

в столбце «Способности». Опять же, старайтесь не тратить на это более 10 минут.

6. Теперь вспомните, в каких из этих направлений вы развили навыки, а в каких у вас есть лишь знания, и поставьте крестики в соответствующих ячейках.
7. Наконец, подумайте о неформальном обучении или самообразовании. Дополните список способностей и снова поставьте крестики в соответствующих ячейках. Пример такого списка показан на рис. 4.4.

Способности	Знания	Навык	Опыт
Установка и настройка антивируса			×
Использование текстового редактора			×
Приготовление эспрессо			×
Работа на кассе			×
Выявление уязвимостей в веб-приложениях		×	
Использование фреймворка OWASP	×		
Реагирование на атаки программ-вымогателей	×		
Использование программы Nmap для обнаружения устройств в сети		×	

Рис. 4.4. Пример списка технических способностей

Теперь у вас есть список технических способностей. Многие из них, скорее всего, никак не связаны со сферой кибербезопасности, и это вполне нормально. Вы также оценили уровень владения каждой из способностей. Это пригодится вам в будущем. А сейчас с помощью этого списка вам предстоит выявить свои базовые навыки.

4.3.2. Базовые навыки

Итак, у вас есть длинный список технических способностей, многие из которых никак не касаются кибербезопасности. Следующий шаг — связать их с концепциями, актуальными для нее. Для этого нужно ввести понятие базовых навыков.

Здесь *базовыми навыками* называются элементы, на которые можно разложить каждую из технических способностей. Определив эти базовые навыки, вы сумеете обосновать, как ваш опыт, не связанный с безопасностью, подготовил вас к работе в желаемой должности.

Ранее я уже говорила, как можно связать опыт бариста с навыками, актуальными для кибербезопасности. Если мы глубже изучим эту гипотетическую ситуацию, вы лучше поймете концепцию базовых навыков и то, как их обнаружить в своем списке способностей.

Подумайте о бариста в оживленной кофейне. В чем суть его деятельности? Если мы рассмотрим его задачи в контексте работы кофейни, то получим довольно простой список. Он подает кофе, готовит эспрессо и другие напитки, пополняет запасы разных продуктов, моет посуду и так далее. Все это понятно, но как это соотносится с работой в сфере безопасности?

Чтобы ответить на этот вопрос, мы должны выявить базовые навыки. Возьмите тот список пунктов, что я привела выше, и представьте их в виде обобщенных формулировок, не связанных с приготовлением кофе. Подумайте, в чем состоит суть деятельности бариста. Очевидно, он получает некоторые входные данные, возможно, из разных источников. На их основе он составляет список задач. При этом он должен организовать свою деятельность так, чтобы заниматься несколькими задачами одновременно, то есть работать максимально эффективно. Кроме того, ему необходимо планировать и выполнять важные операции по техническому обслуживанию (заправка кофейных аппаратов, пополнение запасов, уборка), стараясь при этом, чтобы уровень обслуживания клиентов не упал.

Вы когда-нибудь думали об этой деятельности в таком ключе? Теперь базовые навыки, применимые к работе в области кибербезопасности, стали более очевидными. Например, подумайте о сотруднике SOC и примерьте предыдущее описание к его повседневным задачам. Содержит ли следующий список какие-то действия, которые не вписывались бы в работу этого специалиста?

— Обработка множества входных данных.
— Преобразование входных данных в планы реагирования.
— Приоритизация и организация этих планов для достижения максимальной эффективности.
— Планирование и выполнение важнейших операций технического обслуживания.
— Поддержание высокого уровня обслуживания клиентов.

А теперь подумайте, как те же навыки применить к другим ролям в сфере кибербезопасности, например пентестера, специалиста, отвечающего за реагирование на инциденты, или даже продавца средств защиты. Теперь вы знаете, как определить свои базовые навыки и с их помощью доказать, что вы готовы работать в совершенно иной сфере.

Это знание особенно ценно, если вы претендуете на должность начального уровня в той области, где не имеете опыта. Сейчас мы рассмотрим пошаговый алгоритм для выявления базовых навыков, а затем поговорим о том, как их представить в резюме и в ходе собеседования при приеме на работу.

Упражнение: выявите базовые навыки

Чтобы выполнить это упражнение, вам понадобится список способностей из предыдущего. Алгоритм может показаться очевидным, учитывая вышеописанный пример с бариста, но я все равно изложу его здесь шаг за шагом.

1. Из списка технических способностей выберите те, что не связаны с кибербезопасностью, но отмечены крестиком в столбце «Опыт», и поместите их в новый список.
2. Переформулируйте описание этих способностей, заменив отраслевые термины универсальными понятиями. Цель — обобщить описания настолько, чтобы их можно было применять повсеместно.
3. Изменив описания, разбейте их на отдельные навыки, как было показано в примере с бариста и сотрудником SOC.
4. Просмотрите получившийся список навыков и удалите повторяющиеся (скорее всего, их получится довольно много).
5. Попробуйте примерить каждый из навыков к обязанностям в двух или трех профессиях из различных областей. Если не сможете, попробуйте сделать описание навыка еще более универсальным. На рис. 4.5 показан пример списка базовых навыков.

Способность	Базовые навыки
Приготовление эспрессо	Обработка множества входных данных Преобразование входных данных в планы реагирования Приоритизация и организация этих планов для достижения максимальной эффективности Планирование и выполнение важнейших операций технического обслуживания Поддержание высокого уровня обслуживания клиента
Работа на кассе	Преобразование потребностей клиентов в продукты и услуги Ответы на вопросы клиентов Решение проблем, связанных с недостаточной удовлетворенностью клиентов

Рис. 4.5. Пример списка базовых навыков

Это упражнение может показаться чрезмерно упрощенным, но его результаты окажутся бесценны при собеседовании, когда вы будете пытаться обосновать, почему подходите на должность, даже если не имеете соответствующего опыта. Если вы сумели проделать все эти шаги в уме — замечательно. Однако большинству людей необходимо время и практика, чтобы этому научиться. Выполняя упражнение пошагово и письменно, вы добьетесь наилучшего результата.

Опасность такого подхода заключается в том, что, если преподнести обоснование неправильно, оно покажется преувеличением или проявлением отчаяния. Поэтому после составления списка базовых навыков вам необходимо потренироваться связывать их с той или иной гипотетической должностью. Здесь решающую роль играет уверенность. Если вы сможете донести свое сообщение с убежденностью и страстью, то его получатель, скорее всего, воспримет его всерьез.

Наконец, не путайте базовые навыки с гибкими. Это разные понятия. Базовые навыки связаны с конкретной задачей или способностью, востребованной в той или иной роли. Гибкие навыки в этом смысле не столь однозначны. Они связаны не с конкретными задачами, а с выполнением множества обязанностей. Поэтому список гибких навыков мы составляем в последнюю очередь.

4.3.3. Гибкие навыки

Как говорилось ранее, *гибкие навыки* — это способности, относящиеся не к конкретной задаче, технологии или системе, а к самой личности. Они позволяют человеку более эффективно выполнять свои профессиональные обязанности. При оценке кандидатов на должность менеджеры по найму уделяют гибким навыкам большое внимание. Например, при плохих коммуникативных навыках даже самый высококвалифицированный пентестер будет бесполезен в качестве консультанта по безопасности, работа которого предполагает общение с клиентом.

К сожалению, уровень развития гибких навыков трудно оценить самостоятельно. Чтобы увидеть свои сильные и слабые стороны, требуется высочайшая степень осознанности и объективности. Но как бы мы ни старались, мы всегда остаемся предвзятыми, поскольку просто не в состоянии посмотреть на себя со стороны. Поэтому оценка гибких навыков, как правило, страдает субъективизмом.

Объективные методы оценки гибких навыков не позволяют точно измерить уровень связанных с ними способностей. Например, чтобы объективно оценить навыки письменной коммуникации, можно

принять в расчет такие критерии, как скорость набора текста и соблюдение грамматических норм, но этого недостаточно. Человек может написать грамматически безупречный 30-страничный отчет за один день и получить высокие баллы по этим критериям. Однако, если его отчет будет читателям непонятен, посчитаем ли мы это показателем успеха?

Такова природа гибких навыков, и я с сожалением должна вам сказать, что мне так и не удалось найти решение этой проблемы. Мы должны признать, что, как бы мы ни старались, измерение гибких навыков все равно будет подвержено ошибкам и что мерило в конечном счете находится в умах окружающих нас людей. Тем не менее для оценки таких способностей годятся общие методы; вам будет полезно провести анализ, чтобы выявить сильные стороны и те области, которые требуют совершенствования.

Большинство гибких навыков можно улучшить с помощью практики. Однако то, сколько времени вы на это потратите, зависит от ваших врожденных способностей. Иногда достаточно знать о своих слабых местах, которые вы не в состоянии исправить, и компенсировать их чем-то другим.

Итак, уровень владения гибкими навыками трудно измерить. Так как же определить, способны ли вы их применять и демонстрировали ли вы это в прошлом? Поскольку красота в глазах смотрящего, именно с этого смотрящего и можно начать. Другими словами, в силу субъективности то, как человек оценивает то или иное качество, определяется его восприятием, ценностями и другими предрасположенностями. Поэтому, если вы хотите узнать, насколько хорошо вы демонстрируете владение тем или иным гибким навыком, вам следует обратиться к тем, кто в состоянии об этом судить.

Я не предлагаю опрашивать всех людей, с которыми вам доводилось работать, хотя это один из самых эффективных способов выявить свои сильные и слабые стороны. Однако вы, скорее всего, уже получали отзывы о себе. Если у вас уже есть какое-то карьерное прошлое, то наверняка вашу производительность оценивал менеджер. В счет идут даже неофициальные комментарии. Если же вы никогда не работали, то, вероятно, вам давали подобную обратную связь в ходе обучения, общения с друзьями, членами семьи и другими людьми.

Помните, что обратная связь может быть как положительной, так и отрицательной и не всегда дается напрямую. Люди редко говорят что-то вроде: «О, вы проявили такую чуткость, когда говорили со мной об этой проблеме». Вместо этого они делают разнообразные намеки, поэтому вам нужно вспомнить ситуации, в которых вы пытались использовать тот или иной гибкий навык, и что из этого вышло. Что ж, давайте составим список гибких навыков.

Упражнение: перечислите свои гибкие навыки

Описать этот процесс проще, чем выполнить. Несмотря на то что оценить уровень гибких навыков довольно сложно, задачу упрощает то, что мы в значительной степени полагаемся на мнение других людей. Итак, сделайте вот что.

1. Начиная с текущего или последнего места работы, подумайте о полученной положительной и отрицательной обратной связи, касающейся ваших гибких навыков. Составьте список таких навыков, но не тратьте на это более пяти минут. Список распространенных гибких навыков можно найти в главе 3.
2. Поставьте знак «плюс» рядом с положительными отзывами, а «минус» — рядом с отрицательными. Если отрицательных отзывов будет больше, ничего страшного. Это вполне нормально. Согласно исследованиям, люди замечают и запоминают отрицательную обратную связь гораздо лучше, чем положительную.
3. Теперь вспомните, что вам говорили друзья и близкие. Есть ли у вас определенные черты, которым они давали положительную или отрицательную оценку? Перечислите их.
4. Вспомните любые другие взаимодействия, при которых люди комментировали какие-либо ваши гибкие навыки, и перечислите эти навыки.

Итак, вы составили три подробных списка способностей, определяющих вашу готовность работать в сфере кибербезопасности. Но чего-то по-прежнему не хватает: нам нужно оценить ваш уровень владения каждой из них и выяснить, какие требуют совершенствования, а какие уже можно назвать вашими сильными сторонами.

4.3.4. Инвентаризация способностей

Все упражнения в этом разделе готовили вас к созданию *перечня способностей*; он будет состоять из трех частей, соответствующих трем уже подготовленным спискам. Вам предстоит использовать все, чему вы научились ранее, чтобы оценить уровень владения каждой из способностей. Именно на этот перечень вы будете опираться, чтобы соотносить свои навыки с требованиями желаемой должности, о чем мы поговорим в следующем разделе.

Такой перечень способностей пригодится вам не только при поиске работы. Он позволяет объективно оценить, на каком уровне вы находитесь. Немногие профессионалы тратят время на подобную инвентаризацию, из-за чего их суждения относительно своих навыков могут

оказаться неверными. Кроме того, они не знают, какие способности требуют улучшения, а потому не осваивают новые навыки, что может привести к разочарованию или стагнации.

Я рекомендую вам сохранить списки и обновлять их в процессе карьерного роста. Пункты, ставшие неактуальными, можете удалять. По мере развития навыков, связанных с обеспечением безопасности, и наработки опыта вы будете уделять все меньше внимания базовым навыкам и в какой-то момент, вероятно, вообще исключите их из перечня. Этот живой документ будет служить вам долгие годы. И его гораздо проще составить на начальном этапе и при необходимости обновлять, чем пытаться создать его спустя 5 или 10 лет после старта карьеры.

Упражнение: перечислите способности, связанные с кибербезопасностью

Возьмите списки своих технических способностей, базовых и гибких навыков и сделайте следующее.

1. Поскольку основная цель инвентаризации ваших способностей связана с поиском работы в сфере кибербезопасности, выберите только те способности, которые имеют отношение к этой области (остальные, как вы помните, указаны в качестве базовых навыков).
2. Замените каждый крестик в столбце «Опыт» числом лет опыта работы в соответствующей области.
3. Замените каждый крестик в столбце «Навык» оценкой уровня владения, используя четырехуровневую шкалу: «Начальный», «Продвинутый», «Всеобъемлющий» и «Экспертный».
4. Замените каждый крестик в столбце «Знания» оценкой уровня знакомства с соответствующей темой, следуя той же четырехуровневой шкале.
5. Просмотрите свои базовые навыки. Каждый из них вы получили, поскольку исполняли должностные обязанности, а значит, у вас есть соответствующий опыт. Укажите число лет опыта для каждого из навыков, при необходимости учитывая опыт на разных рабочих местах.
6. Ранжируйте свои базовые навыки в порядке убывания их уровня. Оценивайте их относительно друг друга — это поможет вам в дальнейшем примерить их к ролям в сфере кибербезопасности.
7. Дополните свой перечень гибкими навыками. Для тех, что отмечены знаком «плюс», укажите частоту положительных отзывов, используя трехуровневую шкалу: «Редко», «Обычно» и «Часто». Сделайте то же самое для навыков, отмеченных «минусом». На рис. 4.6 показан пример готового перечня способностей.

Способность	Знания	Навык	Опыт
Установка и настройка антивируса ① Использование фреймворка OWASP ③ Реагирование на атаки программ-вымогателей ④ Использование программы Nmap для обнаружения устройств в сети ②	Продвинутый Начальный	Продвинутый	1 год
Преобразование входных данных в планы реагирования ① Планирование и выполнение важнейших операций технического обслуживания ②			4 года 4 года
Презентационные навыки (+) Письменная коммуникация (+)			Редко Часто

Рис. 4.6. Пример перечня способностей

Замечательно! Теперь у вас есть подробный перечень способностей, который поможет вам выбрать подходящие для себя должности. Этот список позволит вам обосновать свою квалификацию перед рекрутерами и менеджерами по найму, а также составить план совершенствования своих навыков для подготовки к работе.

4.4. Соотнесение имеющихся способностей с желаемой должностью

Итак, вы нашли свою уникальную особенность, разобрались с тем, что мотивирует вас искать работу в сфере кибербезопасности, оценили свои способности и создали их перечень. Пришло время соотнести свои навыки и умения с желаемой работой. Все, что вы делали до сих пор, вело вас к этому моменту.

Теперь вам предстоит с помощью своего заявления о цели и перечня способностей определить подходящие для себя должности в сфере кибербезопасности, а также отсортировать по важности способности, которые вам необходимо усовершенствовать, чтобы лучше подготовиться к выполнению работы.

4.4.1. Выбор основного направления

Ранее вы составили заявление о личной цели, описывающее, что делает вас уникальным и чем вас привлекает сфера кибербезопасности.

Пришло время с помощью этой информации найти те роли, что соответствуют вашим увлечениям и способны вдохновить на долгосрочную карьеру. В заявлении о личной цели определены ваши основные ценности, которыми вы не должны поступаться ни при каких условиях. Игнорирование личных целей и увлечений способно привести лишь к разочарованию. С учетом того, сколько усилий вы вложили в подготовку к карьере в кибербезопасности, последнее, что вам нужно, — это пойти по пути, который противоречит вашим увлечениям и заставляет задумываться о кардинальной смене сферы деятельности.

Если вы уже выбрали одно-два направления, опираясь на свои интересы, то это очень хорошо. Однако в силу своей любознательности вы, возможно, обратили внимание на множество различных направлений. В этом случае сосредоточиться на чем-то одном вам поможет составленный список увлечений.

Теперь вам необходимо провести кое-какие исследования. Если вы уже представляете, должность какого типа хотите занять в сфере безопасности, просмотрите направления, подробно описанные в главе 2, и проанализируйте рабочие обязанности, соответствующие этой должности. Кроме того, поищите ее описания в интернете. Теперь сравните эти обязанности с увлечениями в самом верху списка, лежащего в основе вашего заявления о цели. Совпадают ли они? Если да, замечательно: вы выбрали одно или несколько направлений, которые могут вам подойти.

Если они не совпадают или вы не уверены в том, какая роль вас интересует, начните со своего заявления о цели и с наиболее важных для вас увлечений. Теперь перечитайте описания направлений кибербезопасности из главы 2. Поищите в интернете дополнительную информацию о различных ролях и сравните их обязанности со своими увлечениями. Попробуйте спросить знакомых в социальных сетях, какая роль, по их мнению, может подойти человеку с вашими интересами.

Фокусируйтесь на такой деятельности, какой вам будет интересно заниматься на протяжении длительного времени. Карьера должна способствовать развитию ваших увлечений. В конце концов выберите одно или два направления, на которых вы хотите сосредоточиться.

Смена направления

Выбор направления, определяющего ваш карьерный путь в сфере кибербезопасности, может показаться чрезвычайно серьезным шагом. Однако если позже выяснится, что оно не соответствует вашим увлечениям, как вы того ожидали, или если ваши увлечения со временем изменятся (бывает и такое), ничего страшного. Некоторые общие концепции применимы ко многим специальностям в сфере безопасности,

и некоторые знания или навыки, востребованные в одном направлении, могут оказаться ценными и в другом. Поэтому сменить специальность в сфере кибербезопасности гораздо проще, чем в других отраслях.

Имейте это в виду, чтобы не увязнуть в поиске единственно подходящей для вас роли. Найти правильный путь очень важно, однако со временем он может меняться; кроме того, технологии развиваются, в цифровом мире возникают новые потребности — и вместе с ними могут появляться новые пути. Если вы испытываете беспокойство или страх по поводу выбора правильного направления, постарайтесь отпустить ситуацию и понять, что ваш путь будет уникальным и, скорее всего, совершенно неожиданным, как часто и происходит в этой сфере.

4.4.2. Выявление пробелов и проблем

Вот и все. Вероятно, вы ждали этого момента на протяжении бóльшей части четвертой главы. Вы провели исчерпывающий самоанализ и выявили наиболее подходящие для себя карьерные пути в сфере кибербезопасности. Пришло время оценить, в какой степени вы готовы работать в этом направлении и какие навыки вам необходимо усовершенствовать, чтобы лучше соответствовать требованиям интересующей вас должности.

Этот процесс довольно прост. Он потребует от вас четкого понимания особенностей той деятельности, которая вас интересует. Для этого вам придется провести дополнительное исследование, но хорошая новость заключается в том, что это может быть довольно весело.

Упражнение: выявите пробелы в своих навыках

Пробел в навыках — это список способностей, которых у вас сейчас нет или которыми вы владеете недостаточно для того, чтобы выполнять интересующую вас работу. Ваш перечень способностей отражает то, в чем вы уже преуспеваете, так что вам нужно сопоставить его с теми требованиями, которые менеджеры по найму предъявляют к кандидатам. Итак, приготовьтесь: вы отправляетесь на поиски объявлений о вакансиях.

1. Составьте описания 10–15 должностей в выбранном направлении. Поищите на досках объявлений вакансии на должности начального уровня, если такие есть, или на должности, требующие минимального опыта.

2. На основе этих описаний составьте список уникальных требований. Подсчитайте, сколько раз в них упоминается каждое требование.

3. Для требований, которые предполагают определенный стаж, вычислите среднее число лет необходимого опыта. Мы стремимся получить хорошую выборку данных и до некоторой степени их нормализовать.

4. После составления списка выберите пять наиболее частых требований.

5. Сделайте то же самое для дополнительных или предпочтительных характеристик соискателя; составьте их список, подсчитайте, сколько раз они упоминаются в описаниях должностей, а затем выберите пять основных.

6. Сравните список из пяти обязательных и пяти предпочтительных характеристик с перечнем ваших способностей.

7. Начните со своих технических способностей: какие из них совпадают с требованиями? Обладаете ли вы необходимым опытом? Создайте новый список и включите в него те требования, которым вы полностью соответствуете, отметив их фразой «Полное соответствие». Затем включите в него те требования, которым вы отвечаете по уровню способностей, но не по опыту, отметив их фразой «Требуется опыт».

8. Те пункты из первой пятерки обязательных и предпочтительных характеристик, которые не соответствуют вашим техническим способностям, сравните со своими базовыми навыками. Добавьте совпадения в список и отметьте их фразой «Базовые навыки».

9. Проверьте, не относятся ли требования, которые так и не попали в ваш список, к гибким навыкам. Если относятся, то посмотрите, соответствуют ли они вашим положительно оцененным качествам. Если да, включите их в список и обозначьте их как «Положительно оцененные гибкие навыки». В обратном случае обозначьте их как «Отрицательно оцененные гибкие навыки».

10. Добавьте в список все оставшиеся требования или предпочтительные характеристики, которые не соответствуют никаким пунктам вашего перечня способностей, и отметьте их фразой «Не соответствует».

Итак, вы выявили пробелы в своих навыках. Пришло время подумать о расстановке приоритетов. В контексте плана личного развития (о котором мы подробно поговорим в главе 5), это можно сделать следующим образом.

- *Не соответствует*. Эти пункты имеют наивысший приоритет. Скорее всего, они описывают отсутствующие у вас технические способности, которые пользуются спросом среди работодателей. В следующей главе мы обсудим стратегии устранения этих пробелов.
- *Базовые навыки*. Эти пункты отражают возможности для развития технических способностей. Они также позволяют продемонстрировать вашу потенциальную готовность выполнять соответствующие обязанности, поэтому эта категория следующая в вашем списке приоритетов.
- *Отрицательно оцененные гибкие навыки*. Это те области, над которыми вам стоит поработать, однако при поиске работы вы можете присвоить им более низкий приоритет, учитывая, что на их совершенствование требуется время. Тем не менее, если вы часто получали отрицательную обратную связь относительно каких-то из этих гибких навыков, то им, возможно, стоит дать приоритет повыше.
- *Требуется опыт*. Если у вас нет опыта, то вам никак не удастся его продемонстрировать. Вы можете поработать над соответствующим навыками самостоятельно, однако это не должно быть приоритетом при наличии других, более важных задач.
- *Положительно оцененные гибкие навыки*. Хорошие новости: это ваши сильные стороны, которые вы можете подчеркнуть в своем резюме и в ходе собеседования. Продолжайте совершенствовать эти навыки, но не присваивайте этой задаче слишком высокий приоритет.
- *Полное соответствие*. Снова хорошие новости: вы полностью соответствуете этой квалификации. Поддерживайте свои способности на высоком уровне, но не делайте их развитие первоочередной задачей.

Расставив акценты, вы можете начать разрабатывать план личного развития. Теперь вы точно знаете, какие навыки необходимо усовершенствовать в первую очередь, чтобы получить желанную работу. В следующей главе мы рассмотрим, какие есть способы устранить пробелы и наработать необходимые навыки, чтобы подтвердить свою готовность занять интересующую должность.

ПОДВЕДЕНИЕ ИТОГОВ

- Начинающие специалисты по кибербезопасности сталкиваются с серьезными трудностями при поиске первой работы. Им сложно найти должности начального уровня, требования работодателей

часто бывают нереалистичными, а четких способов построить карьеру в этой сфере не существует.

— Заявление о личной цели связывает воедино уникальный аспект вашего личного бренда с вашими главными интересами. Оно может служить ориентиром при принятии карьерных решений.
— Базовые навыки, полученные при работе, не связанной с кибербезопасностью, могут подтвердить готовность соискателя войти в эту сферу.
— Составить перечень способностей чрезвычайно важно, чтобы понять, насколько хорошо вы готовы к работе в выбранном направлении.
— Выявить пробелы в навыках помогут описания реальных должностей: это мощный инструмент для планирования личного развития, позволяющий сопоставить свои способности с требованиями интересующей должности.

Глава 5
Устранение пробелов в способностях

В этой главе

- Знакомство с сертификатами по кибербезопасности, определение их ценности и целесообразности их получения
- Понимание того, как прохождение академических программ по кибербезопасности влияет на поиск работы
- Приобретение практических навыков с помощью менее формального и самостоятельного обучения

Меня, как наставника людей, желающих построить карьеру в сфере кибербезопасности, часто спрашивают, какую программу обучения или сертификации следует пройти. Готовясь начать карьеру, человек в первую очередь думает о технических навыках, необходимых для трудоустройства. В предыдущей главе вы научились проводить самоанализ, выбирать подходящее для себя карьерное направление и выявлять пробелы в навыках. Теперь, когда у вас есть четкое представление о том, какие технические способности требуют совершенствования, пришло время изучить способы устранить эти пробелы.

Ранее я уже говорила, что сообщество специалистов по безопасности не может предоставить тем, кто желает работать в этой сфере, четкого представления о том, как это сделать. Спросив разных специалистов, с чего лучше всего начать, вы наверняка получите разные ответы. Я считаю, что многие из этих людей искренне хотят помочь, но, к сожалению, не обладают достоверной информацией.

На протяжении многих лет лидеры в сфере кибербезопасности полагали, что талантов не хватает, поскольку нет соответствующих академических программ. Чтобы решить эту проблему, темы кибербезопасности включили в планы учебных курсов различных уровней вплоть до начального. Колледжи и университеты запустили полноценные программы, направленные на получение ученой степени в сфере кибербезопасности, а в некоторых случаях даже посвященные конкретным направлениям этой сферы. Однако из-за самой природы таких программ знания выпускников часто оказывались слишком общими или устаревшими.

В связи с этим некоторые опытные и благонамеренные наставники стали рекомендовать начинающим специалистам пройти сертификацию, чтобы получить навыки, необходимые для трудоустройства. И люди принялись получать сертификаты по кибербезопасности. Если это не давало нужного результата, они получали дополнительные сертификаты. Довольно быстро отрасль наводнили кандидаты на должности начального уровня, обладающие множеством сертификатов, но не имеющие опыта работы. В результате специалисты стали говорить им, что в сертификатах нет смысла без опыта, и рекомендовать применять знания на практике.

В последнее время опытные профессионалы советуют новичкам участвовать в учебных мероприятиях. Зачастую — в соревнованиях типа CTF (Capture the Flag), где участники или команды пытаются использовать уязвимости, чтобы найти скрытые флаги и заработать тем самым очки. Еще одна распространенная рекомендация — участвовать в хакатонах, где, как правило, целые группы реализуют инициативу, связанную с обеспечением безопасности. Некоторые специалисты предлагают новичкам создавать собственные виртуальные лаборатории, чтобы экспериментировать с защитными технологиями и методами наступательной безопасности.

К сожалению, в корпоративной среде, где описания должностей содержат требование опыта, рекрутеров интересует стаж, который трудно подтвердить участием в этих неформальных образовательных мероприятиях. В результате люди, желающие начать карьеру в сфере, где им не хватает навыков, не понимают, куда им идти.

Головоломка под названием «Мне нужен опыт, чтобы получить работу, но мне нужна работа, чтобы получить опыт» десятилетиями

осложняла поиск талантов в сфере кибербезопасности. К сожалению, несмотря на усилия многих специалистов, из-за громких случаев утечки данных требования компаний к кандидатам ужесточились, что только усугубило ситуацию.

Эта глава поможет вам взглянуть на такие трудности с точки зрения соискателя и преодолеть их. В частности, мы поговорим о навыках и опыте, представляющих наибольшую ценность для кандидата на должность начального уровня, и о лучших способах продемонстрировать эти навыки потенциальным работодателям.

5.1. Алфавитный суп из сертификатов по кибербезопасности

Если вы задумывались о карьере в сфере кибербезопасности, то наверняка знаете о существовании бесчисленного множества *сертификатов*. Различные звания, присваиваемые сторонними организациями профессионалу и подтверждающие его владение навыком или набором навыков, упоминаются в описаниях множества должностей. Многим новичкам кажется, что получить один, два или даже десять сертификатов — отличный способ подготовиться к работе. Однако, как было сказано в главе 3, результаты моего опроса свидетельствуют, что корреляции между наличием отраслевого сертификата и более коротким периодом трудоустройства нет.

Несмотря на это, сертификат играет большую роль при поиске работы, особенно первой. В конце концов, большинство работодателей просят, а многие даже требуют его наличия по тому или иному направлению — это ли не веская причина его получить. С учетом всего кажется, что пройти сертификацию — очевидный первый шаг для начинающего специалиста. Однако не все так просто.

В огромном количестве доступных вариантов очень легко запутаться. Чтобы выбрать сертификат, недостаточно найти самое часто упоминаемое звание в описаниях должностей. Во многих программах сертификации есть требования к знаниям, опыту и имеющимся сертификатам. Следующая диаграмма[9] может дать вам некоторое представление о сложности выбора подходящего сертификата по кибербезопасности.

[9] Указанные сертификационные организации являются иностранными, получение большинства указанных сертификатов является платным и на момент выхода книги может представлять сложность для специалистов из России. — *Прим. ред.*

Область	Организация	Начальный уровень	Продвинутый уровень
Общие знания	CompTIA	Security+	CASP+
	SANS Institute	GSEC	GISDP
	(ISC)²	SSCP	CISSP
Тестирование на проникновение	CompTIA	Pentest+	
	Offensive Security		OSCP OSWP OSWA
	SANS Institute	GPEN GWAPT	GXPN GMOB GCPN GAWN
Управление, риск-менеджмент и соблюдение требований	ISACA	CSXP	CISA CISM CRISC
Облачная безопасность	CompTIA	Cloud+	
	SANS Institute	GCSA	GCPN
	(ISC)²		CCSP
Безопасность приложений	(ISC)²		CSSLP
	SANS Institute	GWEB	GDAT GFACT

Рис. 5.1. На этой диаграмме перечислено множество распространенных сертификатов по кибербезопасности, актуальных на разных этапах карьерного роста

Выбрать сертификат гораздо сложнее, чем кажется, но этот выбор может стать важным шагом при поиске первой работы в сфере кибербезопасности. Поэтому имеет смысл рассмотреть наиболее распространенные сертификаты и понять, как они вписываются в общий процесс построения карьеры.

5.1.1. Обзор программ сертификации по кибербезопасности

Прежде чем обсуждать конкретные сертификаты, давайте поговорим о целях программ и о том, почему их так много. Кибербезопасность и ее предшественница информационная безопасность не всегда были общепризнанными дисциплинами, какими считаются сейчас. Многих из доступных сегодня формальных обучающих программ просто не существовало. Даже теперь они часто не позволяют должным образом подготовить специалистов по кибербезопасности, поскольку все меняется слишком быстро, а спектр тем в этой области чрезвычайно широк.

Из-за недостатка формальных образовательных программ такие организации, как (ISC)², ISACA и другие, стали искать способы формализовать знания, генерируемые ИБ-специалистами, и распространять их среди участников сообщества. В конце концов были разработаны программы сертификации, позволяющие профессионалам продемонстрировать свое владение предметом путем сдачи экзамена. Человек, набравший проходной балл, признается сертифицированным специалистом.

С развитием кибербезопасности возникало множество специализированных областей знания. Чтобы выделять профессионалов с опытом в этих областях, были учреждены дополнительные программы сертификации. Их разработали такие организации, как Ассоциация производителей вычислительной техники (CompTIA), SANS, Международный совет консультантов по электронной коммерции (EC–Council) и Offensive Security; их программы затрагивали не только специализированные темы, но и область общих знаний. В результате появился установленный способ оценки и подтверждения профессиональных навыков. Сертификаты превратились в инструмент, позволяющий рекрутерам и менеджерам по найму искать и оценивать потенциальных кандидатов.

Помимо этих организаций (многие из которых, будучи некоммерческими, имеют целью повысить уровень образования в области кибербезопасности) специальные программы сертификации учредили поставщики коммерческих средств защиты. Так, компания Cisco Systems предлагает множество сертификатов, подтверждающих умение не только профессионально обращаться с ее продуктами, но и использовать их в контексте конкретных дисциплин, например кибербезопасности. Некоторые из них перечислены на рис. 5.1.

По мере развития сферы кибербезопасности растет спрос на людей, обладающих подобными сертификатами, а также появляются образовательные программы и контент, призванные помочь профессионалам подготовиться к сдаче сертификационных экзаменов. Множество материалов и программ предоставляют сами сертифицирующие организации. Однако существуют и сторонние образовательные организации, построившие бизнес на помощи людям в подготовке к таким экзаменам. Материалы, курсы и программы, направленные на получение сертификатов по кибербезопасности, теперь все больше фокусируются не только на подготовке к экзамену, но и на отработке навыков, необходимых для его сдачи. Из-за такого смещения фокуса прохождение программ начали воспринимать как образовательный процесс, а не как возможность доказать владение навыками.

В результате многие профессионалы видят в программах сертификации основной способ приобрести новые умения. А значит — правильно это или нет, — что некоторые обладатели сертификатов не применяли

их за пределами классной комнаты или лаборатории. Большинство представителей отрасли ситуацию охарактеризовали отрицательно: по их мнению, в таком случае ценность самой сертификации падает. В ответ на это некоторые сертифицирующие организации ввели требования к опыту работы. По многим сертификатам требуется ежегодно подтверждать прохождение программ непрерывного образования. Кое-где есть даже фиксированный порядок выдачи сертификатов, то есть профессионалу не дадут пройти сертификацию более высокого уровня, если у него нет сертификата предыдущего уровня.

Все это, разумеется, влияет на то, какую сертификационную программу стоит выбрать начинающему специалисту. Нередко в вакансиях требуется наличие сертификатов, которые невозможно получить без опыта. Такие должности, даже начального уровня, оказываются недосягаемы для соискателей-новичков. Подробнее об описаниях должностей, а также о способах выявить и решить эти проблемы мы поговорим в главе 6. А пока давайте рассмотрим некоторые сертификаты, которые наиболее часто встречаются в объявлениях о вакансиях.

5.1.2. (ISC)² Certified Information Systems Security Professional

Один из старейших и наиболее широко признанных сертификатов по информационной безопасности — *CISSP* (Certified Information Systems Security Professional, «Сертифицированный специалист по безопасности информационных систем»), выдаваемый (ISC)² с 1994 года. Он фигурирует в объявлениях о вакансиях чаще всего. Изучив выборку объявлений на пяти крупнейших сайтах, посвященных поиску работы, я обнаружила, что более чем в 90% из них упоминается CISSP как необходимая или предпочтительная квалификация соискателя. В некоторых прямо указывалось, что наличие этого сертификата обязательно, а большинство содержало фразу вроде «сертификат CISSP или эквивалент».

Итак, что же собой представляет программа сертификации CISSP? Эта широко признанная программа охватывает темы по следующим восьми дисциплинам или областям знания:

— управление безопасностью и рисками;
— безопасность активов;
— архитектура и проектирование систем безопасности;
— коммуникации и сетевая безопасность;
— управление идентификацией и доступом (IAM);
— оценка безопасности и тестирование;
— операции по обеспечению безопасности;
— безопасность разработки программного обеспечения.

Как видите, в программе сертификации CISSP есть несколько весьма масштабных тем. А потому этот сертификат актуален практически для любого специалиста по кибербезопасности. Однако сложность его получения не ограничивается необходимостью продемонстрировать обширные знания при сдаче экзамена. Человек также должен подтвердить пятилетний опыт работы как минимум в двух направлениях. Это служит залогом того, что сертифицированные специалисты не просто прошли интенсивный подготовительный курс, а способны применять знания и навыки в реальных ситуациях.

$(ISC)^2$ прилагает большие усилия, чтобы гарантировать квалификацию обладателей ее сертификатов. Помимо соответствия основным условиям от специалистов она также требует, чтобы они подтверждали свое участие в программе непрерывного профессионального образования. Обладатели сертификатов CISSP должны пройти как минимум 120 часов обучения в рамках таких программ в течение трех лет, притом зарегистрировать их в $(ISC)^2$. Так организация сможет проводить аудит, чтобы гарантировать их соответствие утвержденным стандартам.

Наконец, давайте поговорим о стоимости. Эти сертификаты не бесплатны. Вам придется отдать деньги не только за прохождение экзамена и сам сертификат, но и за подготовительный курс или учебные материалы. На момент написания книги стоимость сдачи экзамена CISSP составляла 699 долларов США. Это немало, особенно для тех, кто только начинает карьеру. Ежегодная плата за подтверждение сертификата составляет 85 долларов. Стоимость подготовительных курсов сильно варьируется в зависимости от поставщика услуг, но может достигать 3000 долларов. Это большие деньги, которые необходимо потратить еще до начала работы.

Если вас как начинающего специалиста это устрашает, ничего удивительного. CISSP — престижное звание, присваиваемое признанным профессионалам в области информационной безопасности. Как видно из условий его выдачи и подтверждения, сертификат не подходит для тех, кто только входит в отрасль. Поэтому, увидев в объявлении о вакансии требование CISSP, имейте в виду, что получение этого сертификата — не тот путь, который вы можете выбрать на раннем этапе карьеры. Однако не расстраивайтесь: большинство объявлений содержит фразу «или эквивалент», на чем вам и следует сосредоточиться.

Теперь, когда вы осознали, что путь через сертификацию CISSP для начинающего профессионала нереалистичен, давайте поговорим о том, какие еще сертификаты вы можете получить, чтобы продемонстрировать свою квалификацию.

5.1.3. CompTIA Security+

Сертификат CompTIA *Security+* существует уже довольно давно, но получает гораздо меньше внимания по сравнению с CISSP. Эта программа, официально запущенная в 2002 году организацией CompTIA (**www.comptia.org**[10]), охватывает следующие шесть направлений:

- угрозы, атаки и уязвимости;
- технологии и инструменты;
- архитектура и дизайн;
- управление идентификацией и доступом;
- управление рисками;
- криптография и инфраструктура открытых ключей (PKI).

Несмотря на разницу в порядке тем, они в значительной степени пересекаются с темами программы CISSP. Цель CompTIA — оценить общие навыки, а потому ее сертификат актуален для широкого круга специалистов по кибербезопасности. На сайте CompTIA последняя версия этого экзамена описывается так:

> *Успешная сдача сертификационного экзамена CompTIA Security+ подтверждает наличие у кандидата знаний и навыков, позволяющих ему оценивать безопасность корпоративной среды, рекомендовать и внедрять необходимые защитные решения; контролировать и защищать гибридные среды, в том числе облачные, мобильные и IoT-среды; работать с учетом применимых законов и политик, включая принципы управления, риск-менеджмента и соблюдения требований; выявлять и анализировать события и инциденты безопасности, а также реагировать на них.*

Сертификат Security+ более доступен для начинающего специалиста по сравнению с сертификатом CISSP. Несмотря на то что CompTIA рекомендует кандидатам пройти сертификацию Network+ и иметь не менее двух лет опыта работы в сфере кибербезопасности, это не обязательное требование. Человек, получивший необходимые технические знания другими способами (например, освоив обучающий материал самостоятельно или по какой-либо программе), может сдать экзамен и получить сертификат Security+. Тем не менее здесь требуется проходить программу непрерывного образования. Чтобы подтвердить сертификат Security+, его держатель должен заработать 50 так называемых единиц

[10] На момент выхода книги сайт недоступен для пользователей из России. — *Прим. ред.*

непрерывного образования (CEU, continuing education unit) в течение трех лет.

В финансовом плане сертификат Security+ также более доступен. На момент написания книги пройти экзамен стоило 379 долларов. Это недешево, но более чем на 300 долларов дешевле, чем сдача экзамена CISSP. Ежегодная плата за продление сертификата Security+ составляет 50 долларов. Подготовительные курсы предлагают многие поставщики образовательных услуг, и они в целом также дешевле курсов по CISSP. Стоимость дистанционных курсов, предлагаемых непосредственно CompTIA, варьируется в диапазоне от 499 до 899 долларов. Обучение под руководством инструктора обойдется дороже, однако цена даже самого дорогого пакета не превышает 2000 долларов.

В целом сертификат Security+ позволяет оценить широкий спектр тем и знаний в области безопасности, а потому актуален практически для любого специалиста. В этом смысле он очень похож на CISSP. Тем не менее по затратам и требованиям это более подходящий начальный вариант для тех, кто ищет свою первую работу. Хотя на некоторых должностях, в частности государственных, сертификат CISSP необходим, большинство работодателей признают и другие, подтверждающие то, что кандидат обладает определенным уровнем знаний в области кибербезопасности и технологий.

Популярность программы Security+ среди людей, желающих начать карьеру в этой сфере, постепенно растет, но это не единственный доступный им вариант. Существуют и другие сертификаты, правда, более специализированные. Далее мы рассмотрим один из них.

5.1.4. EC–Council Certified Ethical Hacker

Программа сертификации *Certified Ethical Hacker* (CEH, «Сертифицированный этичный хакер»), запущенная в 2010 году организацией EC–Council, относительно новый вариант. Как следует из названия, она предназначена для оценки навыков этичных хакеров (которых обычно называют пентестерами или специалистами по тестированию на проникновение). Сертификация CEH претерпела множество изменений в плане как содержания, так и программ для управления ею. Многие из этих изменений, скорее всего, были обусловлены критикой со стороны представителей ИБ-сообщества, считавших процесс сертификации недостаточно строгим. Таким образом, хотя большинство работодателей воспринимает этот сертификат как доказательство, что у соискателя есть фундаментальные знания в области тестирования на проникновение, в целом он пользуется меньшим уважением по сравнению с другими.

С самого начала программа CEH предназначалась для специализированного обучения и для оценки способности применять инструменты, методы и концепции, относящиеся к тестированию на проникновение. Обратите внимание на слова «обучение» и «оценка». В отличие от многих других программ сертификации, включая обсуждавшиеся ранее, в рамках программы CEH обучение тесно связано с самим экзаменом. Сдать его можно и не проходя формальный курс обучения, но для этого организация EC–Council требует, чтобы у кандидата был двухлетний опыт работы в сфере ИБ. Чтобы подтвердить этот опыт, необходимо подать заявку, приложив свое резюме, и заплатить 100 долларов за ее проверку и за допуск к экзамену. Также следует отметить, что EC–Council — одна из немногих коммерческих сертификационных организаций.

Согласно документу EC–Council CEH Exam Blueprint version 3.0, экзамен позволяет оценить знания в следующих семи областях:

— общие знания;
— анализ/оценка;
— безопасность;
— инструменты/системы/программы;
— процедуры/методология;
— регулирование/политика;
— этика.

Сертификационные курсы CEH может пройти любой желающий. Несмотря на то что EC–Council дает некоторые рекомендации относительно того, кому следует записываться на них, обязательных требований к участникам она не предъявляет. Благодаря этому курсы доступны для начинающих профессионалов. Как и большинство других подобных проектов, CEH ставит непременное условие: участвовать в программе непрерывного образования. Чтобы подтвердить сертификат, EC–Council требует, чтобы его держатель заработал 120 кредитов непрерывного образования EC–Council (ECE) в течение трех лет.

В плане затрат программа сертификации CEH несколько отличается от тех, что мы рассматривали ранее. Получить допуск к экзамену, не проходя подготовительный курс, трудно, а потому трудно определить его итоговую стоимость. EC–Council требует, чтобы держатели сертификатов вносили ежегодный членский взнос 80 долларов США для поддержания их актуальности. Отличие здесь заключается в том, что членский взнос распространяется на все имеющиеся у человека сертификаты EC–Council (организация предлагает еще несколько более продвинутых и специализированных сертификатов). Стоимость подготовки к экзамену CEH варьируется от 1899 долларов США за дистанционный

курс для самостоятельного изучения до 2999 долларов США за курс очного обучения (цены актуальны на момент написания книги).

В целом, несмотря на доступность для начинающих специалистов по кибербезопасности, сертификат CEH имеет существенные недостатки. Главный из них — стоимость, если только вы уже не работаете в компании, готовой оплатить сертификацию, чтобы помочь вам перейти на более высокую должность. Другой недостаток — узкая специализация программы. Если вы уверены, что хотите заниматься тестированием на проникновение, то сертификат CEH может стать хорошей инвестицией. Однако, если в будущем вы захотите сменить направление деятельности, он может стать ограничивающим фактором.

5.1.5. Прочие сертификаты

Сертификаты, которые мы обсудили, самые распространенные среди начинающих ИБ-специалистов. Однако, как вы видели на рис. 5.1, существует множество других вариантов, предлагаемых различными организациями и продавцами продуктов. Надеюсь, приведенное выше описание сертификатов CISSP, Security+ и CEH дало вам более четкое представление о важных аспектах, которые необходимо учитывать при выборе программ сертификации. Все они различаются по объему оцениваемых знаний, стоимости и условиям, касающимся непрерывного образования. Некоторые из наиболее технически ориентированных даже требуют сдачи практического экзамена, где надо выполнять задачи в лабораторной среде на время.

Подробное описание всех сертификационных программ выходит за рамки этой главы и заслуживает отдельной книги. Однако сфера меняется так быстро, что гораздо важнее уметь анализировать и оценивать каждую из программ с точки зрения ваших собственных целей, чем знать все подробности о каждой из них. Тем не менее нам необходимо ответить еще на один вопрос, связанный с сертификатами.

5.1.6. Слишком много — это сколько?

Заголовок предыдущего раздела «Алфавитный суп из сертификатов по кибербезопасности» — отсылка к метафоре, которой многие представители ИБ-сообщества описывают длинные списки аббревиатур, что некоторые люди указывают рядом со своими именами в резюме, на визитных карточках и так далее. На самом деле многие нынешние специалисты по кибербезопасности имеют по 10, 15 и даже 20 сертификатов.

Кому-то может показаться, что больше — значит лучше, но так ли это на самом деле? Работает ли в этом случае закон убывающей отдачи? Как насчет сложностей, связанных с поддержанием актуальности сертификатов? А затраты? Все это необходимо учитывать, обдумывая, сколько вы хотите сертификатов. Однако такие вопросы станут актуальны на более позднем этапе карьеры. Сейчас важно определиться с тем, что нужно для ее начала.

Признаюсь, я еще ни разу не видела, чтобы в вакансии указывалось, что соискателю необходимо иметь более одного сертификата. Хотя иногда наличие нескольких ключевых сертификатов действительно может выделить вас на фоне остальных или повысить шансы на получение какой-то конкретной должности, как правило, это не обязательное требование. Для начала вам достаточно просто иметь сертификат. Многие работодатели этого требуют, другие просто считают преимуществом. Во всяком случае наличие сертификата говорит о том, что вы серьезно относитесь к развитию своих навыков и обладаете достаточными знаниями для того, чтобы сдать экзамен.

Это не означает, что вам хватит одного сертификата, чтобы найти работу. Необходимо учитывать и другие факторы. Как дополнительный сертификат может помочь вам в поиске? Если у вас есть Security+, повысит ли CEH или SANS GIAC Penetration Tester (GPEN) ваши шансы занять должность младшего специалиста по тестированию на проникновение? Возможно. Однако получение и подтверждение этих дополнительных сертификатов также требует вложений. Стоит ли оно того? Вам решать. Возможно, есть программа, позволяющая получить сертификаты Network+ и Security+ с меньшими затратами, чем если бы вы получали их по отдельности. В таком случае целесообразно было бы ею воспользоваться. Такого рода решения вам предстоит принимать по мере своего карьерного роста.

Однако слишком большое количество сертификатов может помешать вам в поиске работы, поскольку у менеджера по найму может сложиться впечатление, что вы потратили больше усилий на получение сертификатов, чем на обучение и применение знаний. Я сама не раз сталкивалась с подобным явлением во время собеседований с кандидатами на должности начального уровня. Хотя я никогда не исключала кандидатов только из-за того, что у них много сертификатов, в разговоре с ними я не раз убеждалась, что знания, проверенные экзаменами, они усвоили не в полной мере. Их хватило, чтобы пройти тест, но применить их в реальной ситуации эти люди были не способны.

Чтобы найти первую работу в сфере кибербезопасности, получить первый сертификат очень важно. Однако в случае последующих сертификатов отдача от инвестиций быстро снижается. Второй,

более специализированный, вероятно, поможет вам выделиться на фоне остальных соискателей, так что, может, было бы неплохо его получить. А вот приобретение дополнительных сертификатов — дорогостоящее мероприятие, которое вряд ли позволит достичь цели быстрее и даже способно навредить.

5.2. Академические программы по кибербезопасности

Как уже говорилось, пару десятилетий назад было очень мало формальных обучающих программ по информационной безопасности / кибербезопасности. Однако с тех пор ситуация кардинально изменилась, поскольку кибербезопасность превратилась не только в популярную новостную тему, но и в предпочтительное карьерное направление для многих людей.

Колледжи и университеты учредили программы для получения ученой степени и даже создали передовые исследовательские лаборатории, специализирующиеся на кибербезопасности. Сегодня студенты могут получить все виды ученых степеней в этой области, а также наработать навыки и опыт в лабораториях и в рамках исследовательских программ.

На первый взгляд кажется, что ученой степени по кибербезопасности достаточно, чтобы найти работу. Однако не спешите. Давайте разберемся в этом вопросе получше и посмотрим, насколько необходимо изучать такие программы, чтобы начать карьеру в сфере кибербезопасности.

5.2.1. Программы, направленные на получение ученой степени

Когда кибербезопасность превратилась в самостоятельное карьерное направление, бизнес начал оказывать все большее давление на систему образования, чтобы та обеспечила формальную подготовку специалистов. Многие учебные учреждения запустили программы для получения ученой степени в области кибербезопасности. Еще больше впечатляет, что многие средние школы сейчас тоже включают курсы по этой дисциплине в учебные программы, а иногда даже интегрируют соответствующие темы в экзамены по информатике Computer Science Advanced Placement (AP).

Учитывая, насколько огромное внимание уделяется программам, направленным на получение ученой степени в области кибербезопасности, человек, желающий начать карьеру в этой сфере, может посчитать,

что пройти такую программу необходимо. Однако опрос опытных специалистов по кибербезопасности, касающийся полученных ими ученых степеней, говорит, что это не так (рис. 5.2).

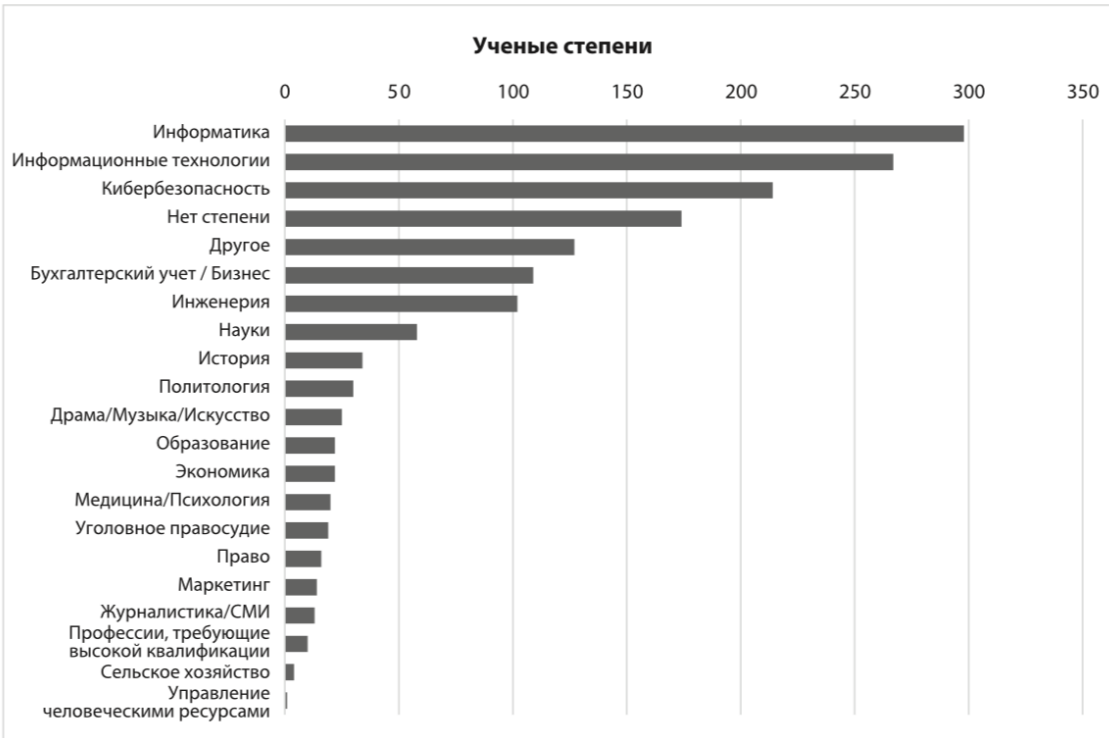

Рис. 5.2. Ученые степени опытных специалистов по кибербезопасности

Как и следовало ожидать, ученые степени, связанные с компьютерными технологиями, явно доминируют. В частности, степень в области кибербезопасности третья по распространенности. Это говорит о потенциальной ценности соответствующих учебных программ. Однако, если у вас степень в другой области или вообще нет степени, значит ли это, что вам непременно нужна степень в области кибербезопасности? Нет. Согласно результатам опроса (рис. 5.2), четвертым наиболее распространенным вариантом было отсутствие ученой степени! А далее перечислено множество иных направлений. Очевидно, что многие из этих ответов дали люди, перешедшие в сферу кибербезопасности из совершенно другой области.

Готовясь к написанию этой книги, я взяла интервью у нескольких опытных специалистов по кибербезопасности, в том числе у Алет Денис, с которой я познакомила вас в главе 4. Я обнаружила кое-что, что, впрочем, меня не особенно удивило: многие мои собеседники начинали

карьеру в областях, никак не связанных с компьютерами. Однако когда их работа соприкоснулась с темой безопасности, они обнаружили в себе интерес к ней и сменили направление деятельности. Очень часто профессионалы попадают в эту область совершенно случайно. Даже я изначально собиралась заниматься медициной. Только через несколько семестров в колледже я переключилась на компьютерные науки и занялась разработкой программного обеспечения. Я работала программистом почти десять лет, прежде чем перейти к кибербезопасности.

Как было сказано в главе 1, тема безопасности затрагивает практически все аспекты нашей жизни. Поэтому любой человек может легко перейти в эту сферу из другой области, напрямую не связанной с технологиями. Итак, какую же степень следует получить начинающему профессионалу? Как и во многих других случаях, ответ зависит от множества обстоятельств.

Как отмечалось ранее, внушительное число ИБ-специалистов вообще не имеют ученой степени. Однако это вовсе не означает, что начинающему специалисту по кибербезопасности рекомендуется вообще не получать высшее образование. Несмотря на то что многие организации не требуют от соискателя прохождения полноценной четырехлетней обучающей программы, в большинстве из них по-прежнему ожидают, что у кандидата есть либо степень, либо сопоставимый опыт работы в смежной области. Действительно, большинство опытных профессионалов без степени годами работали в той или иной связанной с технологиями области, прежде чем перешли в сферу кибербезопасности. Таким образом, начинающему специалисту и без опыта, и без степени найти работу будет сложно.

Итак, ученая степень необходима; означает ли это, что ее нужно получить именно в области кибербезопасности? Вовсе нет. Для тех, кто ищет первую работу и уже имеет степень, возвращаться в колледж нет особого смысла. Есть способы более эффективно использовать денежные и временны́е ресурсы, которых требует университетская программа. А вот для тех, кто только поступает в колледж и планирует работать в сфере кибербезопасности, соответствующая степень может оказаться более полезной. Это имеет смысл: вы же все равно идете учиться, — однако не обязательно.

Как видно из результатов опроса на рис. 5.2, наиболее распространены степени в области компьютерных наук и информационных технологий. Справедливости ради следует отметить, что эти результаты необъективны: многие опытные профессионалы пришли в сферу кибербезопасности еще до появления программ, позволяющих получить ученую степень в этой области. Однако даже сегодня работодатели, как правило, готовы принимать на работу ИБ-специалистов со степенями

в разных областях. На самом деле учебные программы по компьютерным наукам и информационным технологиям охватывают множество тем, которые могут быть полезны специалисту по кибербезопасности. Понимать, как функционируют сети, операционные системы, как разрабатывается программное обеспечение, а также уметь разбираться в других темах, раскрываемых в этих программах, для такого специалиста может быть очень важно.

А что же делать новичку? Как уже говорилось в главе 3, очень важно, чтобы вы выбрали учебную программу, которая лучше всего соответствует вашим интересам и увлечениям. Это поможет сохранять мотивацию и вовлеченность на протяжении всего обучения, что даст плоды после выхода на рынок труда. Итак, выделите время на то, чтобы внимательно ознакомиться с каталогом курсов. Изучите содержание каждой программы, направленной на получение степени, и выберите ту, что кажется вам самой интересной и захватывающей. Далее мы поговорим о других способах развить навыки, которые могут прибавить вам очков при общении с потенциальными работодателями.

5.2.2. Программы перспективных исследований

Большое значение имеет выбор не только программы для получения степени, но и университета или колледжа. Помимо учебного плана, важно оценить также вспомогательные мероприятия, предлагаемые учебным учреждением. Сейчас набирают популярность программы, которые предоставляют учащимся возможность приобрести практические навыки, выполняя реальные исследования в области кибербезопасности в рамках работы внешних исследовательских групп и лабораторий.

Одна из таких программ — Computer Security Group Калифорнийского университета в Санта-Барбаре, известная как SecLab. Команда SecLab реализует различные инициативы, связанные с «проектированием, созданием и проверкой безопасных программных систем». Характер ее деятельности на первый взгляд может показаться теоретическим, однако она имеет вполне практическое значение. Ее участники анализируют программное обеспечение с открытым исходным кодом, чтобы проверить, нет ли в нем уязвимостей. Обнаружив слабое место, они сообщают о нем не только специалисту, отвечающему за сопровождение этого ПО, но и отраслевым организациям, которые в итоге доносят информацию до всего ИБ-сообщества. Таким образом, работа SecLab помогает сделать программное обеспечение более безопасным.

Другие программы ориентированы на сотрудничество с отраслевыми организациями, работающими над разнообразными проектами

и исследованиями. Например, MITRE управляет различными исследовательскими центрами в США, финансируемыми за счет средств федерального бюджета. В рамках исследований она регулярно сотрудничает с университетами и другими академическими учреждениями. Ей это дает доступ к исследователям, а студентам — возможность приобрести практические навыки, которые им пригодятся при поиске первой работы.

При выборе учебного заведения и программы для получения степени важно разобраться в доступных возможностях. В частности, при получении степени, не связанной с кибербезопасностью, участие в такого рода исследованиях позволит выделить свое резюме на фоне остальных. Если же выбранная вами школа не предлагает таких программ, не отчаивайтесь. Вы можете наработать практические навыки в сфере кибербезопасности другими, менее формальными способами, которые тоже будет нелишним указать в резюме.

5.3. Менее формальные способы развития навыков

Активный обмен информацией и высокий спрос на квалифицированных специалистов по кибербезопасности создают множество возможностей для обучения. Это, конечно, не формальные программы для получения ученой степени, но они часто позволяют обрести актуальные и практические навыки, которые нельзя развить в рамках академического образования.

Проблема здесь в том, что подобные варианты сложно представить в резюме как доказательство наличия тех или иных способностей. Далее мы рассмотрим наиболее распространенные неформальные методы обучения и развития дополнительных профессиональных навыков.

5.3.1. Отраслевые конференции

Сообщество специалистов по кибербезопасности уже давно проводит конференции, позволяющие участникам обменяться информацией, развить навыки и наладить деловые связи. В ходе этих конференций опытные специалисты обычно делятся идеями, результатами последних исследований, исчерпывающими обзорами технологий и другими сведениями из области кибербезопасности.

Кроме того, участники часто могут посещать формальные тренинги или мастерские. В рамках многих мероприятий организуют так называемые *«деревни»* — центры практического обучения определенной технологии или технике. Например, как отмечалось в главе 3, большой

популярностью на многих конференциях пользуется «деревня взлома замков»: ее посетители могут узнать о конструкции физических замков и поучиться у опытных инструкторов их взламывать. Кроме замков в «деревнях» можно научиться взламывать все что угодно, начиная с автомобилей и промышленных систем управления и заканчивая системами голосования.

Существует множество различных типов конференций. Понимание целевой аудитории и тематики поможет вам выбрать ту, что наиболее интересна и ценна именно для вас. Отличные возможности для обучения предоставляют не только практические и специализированные конференции конкретно для ИБ-специалистов, но и конференции, напрямую не связанные с информационной безопасностью.

Практические конференции, как правило, ориентированы на тех, кто уже работает или хочет работать в организации, помогая создавать и поддерживать средства защиты. Их темы могут быть самыми разнообразными. Обычно основное внимание на них уделяется действиям, связанным с управлением безопасностью внутри организации. На ИБ-специалистов ориентированы, например, RSA, Black Hat и InfoSec World. Благодаря тому, что на них рассматривается широкий спектр тем, участники могут выбрать тренинги и выступления себе по интересам.

Кроме того, ежегодно проводится ряд специализированных конференций, посвященных обычно конкретному направлению сферы кибербезопасности. Одна из самых популярных и старейших — конференция хакеров DEF CON, учрежденная в 1993 году в Лас-Вегасе. За время своего существования она превратилась из неформальной встречи хакеров в одну из крупнейших конференций по кибербезопасности в мире. Изначально основное внимание здесь уделяли хакерскому сообществу и соответствующим темам. Однако со временем стали организовывать все больше различных «деревень», благодаря чему спектр рассматриваемых тем расширился. Другие известные хакерские конференции, такие как BSides, SchmooCon и THOTCON, посвящены наступательной безопасности.

Помимо хакерских, существует еще одна известная специализированная конференция — Layer 8. Понятие *Layer 8* («Восьмой уровень») относится к человеку как к элементу системы безопасности, поэтому конференция посвящена темам, связанным с социальной инженерией и сбором разведданных. Несмотря на то что организованные в ее рамках «деревни» и мастерские охватывают более широкий круг тем, фокус внимания самой конференции сосредоточен на человеческом факторе и соответствующих тактиках нападения и защиты.

Еще одна специализированная конференция — OWASP Global AppSec. OWASP — это отраслевая организация, занимающаяся безопасностью

приложений, защитой программного обеспечения и процессов его разработки. Опять же, хотя конференция в целом фокусируется на этой тематике, некоторые мероприятия и даже выступления спикеров касаются других аспектов или направлений сферы кибербезопасности.

О различных формах конференций и каждом отдельном мероприятии можно было бы написать целую книгу. Вам необязательно знакомиться со всеми темами и всеми существующими конференциями. Гораздо важнее понимать, как эти мероприятия способны помочь вам обогатить свои знания и развить навыки, которые пригодятся в карьере.

Во-первых, само по себе посещение одной из таких конференций предоставляет возможность обучения, и это можно указать в резюме, чтобы продемонстрировать наличие знаний в определенной области или областях. То, что вы присутствовали на подобном мероприятии, свидетельствует не только о ваших знаниях, но и о вашем желании учиться и расти профессионально. Для некоторых менеджеров по найму это важный фактор.

Во-вторых, на мастерских и тренингах, проводимых в рамках конференций, вы можете развить дополнительные практические навыки, а потом указать их в своем резюме. Демонстрация того, что вы потратили время не только на получение знаний, но и на их практическое применение, способно помочь при недостатке более формального опыта работы.

В-третьих, у большинства конференций есть важная особенность: возможность выступить с докладом и поделиться с другими участниками своими идеями, новыми данными и результатами исследований. Даже доклад на распространенную тему, преподнесенный нестандартным образом, может оказаться полезным, особенно на небольших конференциях для участников ИБ-сообщества.

Так или иначе, сведения о выступлении на одной или нескольких конференциях, включенные в резюме, способны привлечь внимание потенциального работодателя. Справедливости ради следует отметить, что для большинства начинающих профессионалов это довольно высокая планка. Однако если вы комфортно чувствуете себя на публике и у вас есть материал, которым вы готовы поделиться, будь то результат собственного или группового исследования, то эта задача вполне выполнима.

Одна из проблем с этими конференциями заключается в том, что за участие в них необходимо платить (если вы не докладчик или не владелец билета, полученного по стипендиальной программе). Кроме того, они проводятся в разных частях страны, поэтому если такое мероприятие организовано не поблизости от вас, то придется совершить поездку, а это дополнительные расходы.

Один из способов решить эту проблему — участвовать в конференциях BSides. Эти независимые конференции, проводимые под эгидой организации BSides, несколько отличаются друг от друга, но большинство из них охватывает довольно широкий спектр тем. Кроме того, большая часть таких конференций проводится в крупных городах по всему миру, что повышает шансы на то, что вам не придется далеко ехать. Многие ориентированы на небольшое количество участников, а значит, проще оказаться в числе докладчиков. В общем, участие в конференциях — это отличный способ получить знания и, вероятно, некоторые навыки, однако необходимо учитывать и связанные с этим затраты.

5.3.2. CTF-соревнования, площадки для хакеров и персональные лаборатории

Дополнительные знания и навыки в области кибербезопасности можно получить и более неформальными способами. Например, соревнования по захвату флага (CTF) проводятся в рамках как конференций, так и специальных мероприятий, спонсируемых отраслевыми организациями. В этих соревнованиях участники или команды выполняют различные задания, чтобы получить так называемые флаги. В таких заданиях может потребоваться применить методы наступательной безопасности, социальной инженерии, разведки по открытым источникам, а иногда и защиты. CTF-соревнования различаются по уровню детализации задач: самые экстремальные предоставляют только целевую среду, которую пользователь должен исследовать, и больше никаких инструкций.

Также мероприятия различаются по уровню подготовки участников. Ориентированные на новичков, как правило, фокусируются на обучении и руководстве, а значение соревновательного аспекта в них меньше. Обычно участники здесь получают подробные описания заданий и советы по их выполнению. Во многих случаях администраторы этих соревнований при необходимости готовы участникам помочь.

Другие же CTF-соревнования, в том числе проводимые в рамках крупных конференций вроде DEF CON, делают акцент именно на соревновательности. Однако не стоит сбрасывать эти состязания со счетов, особенно если они командные. Если вам удастся найти команду, готовую принять нового человека, желающего учиться, они могут принести вам огромную пользу. В любом случае участие в CTF-соревнованиях — то, что определенно стоит включить в свое резюме. Подробнее об этом мы поговорим в главе 6.

Еще один отличный способ приобрести опыт в области кибербезопасности — использовать специализированные площадки вроде

Hack The Box (*HTB*), где можно выполнять задания, связанные со взломом различных серверов, или смотреть, как их выполняют другие. Задания и серверы регулярно обновляются, как и рейтинг пользователей, основанный на количестве набранных ими очков. У площадки HTB есть важная особенность: работодатели размещают на сайте объявления о вакансиях, которые сопоставляются с пользователями на основе их места в рейтинге. Эта площадка все еще развивается, но если вас интересует тестирование на проникновение и исследование уязвимостей, то, используя ее, вы получите отличный шанс продемонстрировать свои навыки потенциальным работодателям.

Существуют и другие площадки, например намеренно уязвимое приложение от OWASP под названием WebGoat. Вы можете установить его на свой компьютер и практиковать различные типы атак, понимать которые полезно не только пентестерам, но и специалистам, занимающимся защитой ПО. Помимо этой есть и другие доступные намеренно уязвимые среды. С некоторыми можно работать через интернет, но многие требуют настраивать среду на своем компьютере.

Это подводит нас к теме персональных лабораторий. *Виртуализация*, то есть создание виртуального компьютера, работающего как программное обеспечение на вашем персональном компьютере, позволяет легко (и, что более важно, без особых затрат) настраивать небольшие сетевые среды. Создав на домашнем компьютере небольшую сеть в виртуальной среде, вы сможете проводить эксперименты и исследования с использованием множества сетевых и защитных технологий. Это отличный способ получить новые знания, особенно для тех, кто имеет склонность к экспериментам. Даже сама настройка такой среды позволит вам приобрести ценные навыки. А если у вас возникнут вопросы, вы сможете найти нужную информацию с помощью Google, YouTube и других интернет-ресурсов.

5.3.3. Вебинары, подкасты и прямые трансляции

К последней категории неформальных способов обучения, о которой мы поговорим, относятся такие онлайн-медиа, как вебинары, подкасты и прямые трансляции. Бесплатные вебинары часто проводят поставщики средств защиты и даже отраслевые организации. Подкасты почти всегда бесплатны для прослушивания, обычно их создают видные представители ИБ-сообщества. Постепенно набирают популярность прямые трансляции и видеоролики, где люди проводят бесплатные практические и обучающие занятия.

Чтение, просмотр и прослушивание подобного контента вы, скорее всего, не станете включать в свое резюме. Однако он ценен по многим

причинам. Во-первых, так вы следите за тенденциями, темами, технологиями и дискуссиями, ведущимися в сфере кибербезопасности. И благодаря этому можете получить достаточно знаний, чтобы вести более содержательные разговоры в процессе собеседования. Кроме того, такой контент способен натолкнуть вас на идеи для дальнейшего самостоятельного обучения.

Во-вторых, благодаря этим ресурсам вы можете познакомиться с множеством выдающихся представителей ИБ-сообщества и с разными способами решения проблем. Вы также начнете усваивать профессиональную лексику, что, опять же, выделит вас на фоне остальных соискателей в процессе собеседования.

В-третьих, эти занятия позволят вам освоить новые навыки. Поставщики продуктов в основном проводят вебинары, чтобы раскрыть для пользователей возможности своих инструментов или показать, как с их помощью можно решать определенные задачи. Прямые трансляции часто представляют собой обучающие или демонстрационные видеоролики с участием ИБ-специалистов. Даже в подкастах иногда встречается образовательный компонент, когда авторы обсуждают особенности своей работы или результаты исследований. В конечном счете эти бесплатные ресурсы помогут вам сформировать более компетентное мнение по поводу тех или иных целей, связанных с обеспечением кибербезопасности.

5.3.4. Прочие встречи участников сообщества

Еще один способ приобрести новые навыки — приходить на встречи участников местного ИБ-сообщества. Многие национальные и международные организации имеют отделения в разных городах. В этих отделениях регулярно проводятся собрания и другие менее формальные встречи, где участники могут обсудить интересующие их вопросы. Некоторые из этих мероприятий предусматривают выступления с докладами на темы, связанные с кибербезопасностью. В рамках других иногда организуют мастерские или интерактивные занятия, чтобы помочь участникам овладеть какими-то навыками. Третьи, еще менее формальные встречи, проводят, чтобы наладить связи между членами сообщества.

Все эти мероприятия предоставляют возможность получить знания, а иногда и отработать новые навыки. Ниже приведен список некоторых национальных и международных сообществ, в местных отделениях которых регулярно проводятся собрания:

— Cloud Security Alliance (CSA);
— DEF CON Groups;

— Information Systems Security Association (ISSA);
— InfraGard;
— International Association for Healthcare Security and Safety (IAHSS);
— ISACA;
— (ISC)²;
— Open Web Application Security Project (OWASP);
— Women in Cybersecurity (WiCyS);
— Women of Security (WoSEC).

ПОДВЕДЕНИЕ ИТОГОВ

— В сфере кибербезопасности есть широкий спектр программ сертификации, охватывающих различные направления деятельности. При выборе подходящего сертификата важно найти правильный баланс между ценой и качеством.
— Наличие множества сертификатов не облегчает поиск работы. Один или два сертификата позволят вам соответствовать требованиям большинства вакансий, и в начале карьеры этим вполне можно ограничиться.
— Чтобы получить работу в сфере кибербезопасности, вам необязательно иметь ученую степень в этой области. Важнее получить степень в той области, которая вас по-настоящему интересует.
— Программы, позволяющие в реальных условиях развивать практические навыки в сфере кибербезопасности, предлагают различные учреждения.
— Конференции, мастерские, CTF-соревнования, лаборатории и даже онлайн-ресурсы способны стать мощными обучающими инструментами; можно указывать в резюме свое участие в них или использовать их, чтобы приобрести знания в области кибербезопасности.

Глава 6
Резюме, заявления и собеседования

В этой главе

- Составление резюме и его адаптация под системы управления кандидатами
- Выбор подходящих для отклика вакансий
- Указание в резюме неформальных способов обучения и развития навыков
- Подготовка к прохождению отбора, технических и групповых собеседований
- Способы избежать распространенных ловушек, подстерегающих кандидатов
- Обсуждение и принятие условий, содержащихся в предложении о работе

До сих пор мы рассматривали ландшафт сферы кибербезопасности, распространенные в ней роли и необходимые для них навыки. Мы говорили о вас, о том, как выявить свои интересы и привести свои навыки в соответствие с желаемой должностью. Мы также обсудили множество препятствий, преграждающих путь к первой работе. Пора переходить к действиям. В этой главе мы обсудим ключевые аспекты поиска работы и стратегии, позволяющие добиться успеха и избежать распространенных ловушек.

Процесс поиска работы состоит из трех основных этапов: составления резюме, выбора вакансий и отклика на них и прохождения собеседования. Далее мы обсудим каждый из них и поговорим о том, как занять максимально выигрышное положение. Мы также рассмотрим распространенные ошибки соискателей и способы их избежать. Начнем с резюме.

6.1. Навык составления резюме

Что такое резюме? Многие люди сказали бы, что это документ, где перечислены сведения о навыках соискателя, его опыте работы и образовании. Все правильно. Однако я рекомендую относиться к своему резюме как к портфолио.

Ваше резюме призвано произвести первое впечатление на потенциального работодателя еще до того, как он сможет поговорить с вами лично. В нем описаны все ваши профессиональные достижения, и это необязательно должен быть один документ, прилагаемый к заявке на вакансию. Восприятие своего резюме как портфолио позволяет пойти по творческому пути. Подойдя к составлению резюме творчески, вы сможете выразить себя и отразить свою уникальность и таким образом выделиться на фоне остальных соискателей.

6.1.1. Одного документа недостаточно

Многие начинающие специалисты по кибербезопасности рассказывали мне, как они рассылали свои резюме большому количеству потенциальных работодателей. И каждый раз повторялась одна история. Они тратили уйму времени на создание идеального резюме, следуя всем советам, которые только сумели найти. Они формулировали, переформулировали, исправляли, редактировали и корректировали его, чтобы получить безупречно составленный и отформатированный документ. Затем они рассылали его работодателям, у которых были открыты интересующие их вакансии, и недоумевали, почему им так редко перезванивают.

Они составили единственный документ — вот в чем заключалась их главная ошибка. За свою жизнь я прочитала множество советов о том, как нужно писать резюме. Почти в каждой статье, заметке и колонке предполагалось, что соискатель создает одно-единственное универсальное резюме. На первый взгляд это имеет смысл, верно? Вам необходимо написать о себе, и неудивительно, что вы хотите достичь в этом идеала. Но это неправильный подход. Вам следует составить несколько версий резюме. Давайте разберемся, зачем и как это делать.

Ваше резюме действительно должно представлять вас. Но это не автобиография. Как я уже говорила, ваше резюме формирует первое впечатление о вас у работодателя, на чью вакансию вы откликаетесь. Однако работодателей не интересуют все те замечательные вещи, которые сделал соискатель за свою жизнь. Просматривая резюме, они пытаются понять, как этот человек может быть полезен их компании. Таким образом, ваше резюме — это ваш первый шанс рассказать, как вы собираетесь принести им эту пользу, заняв вакантную должность.

В одном из эпизодов моего подкаста мы с соведущими имели честь поговорить с Джейком Уильямсом, уважаемым членом ИБ-сообщества. Он рассказал, какой стратегии придерживается, когда обучает людей составлять резюме. Стратегия выглядит примерно так. Сначала он предлагает сделать краткую самопрезентацию. Человек должен за одну-две минуты убедить его, что именно он подходит для вакантной должности, и объяснить, как собирается принести пользу его команде. По истечении этого времени Уильямс просит человека указать, где в резюме перечислено все, что было в рассказе, и, если чего-то из рассказа там не хватает, дополнить документ. Кроме того, он предлагает удалить из резюме сведения, не попавшие в самопрезентацию.

Мне очень нравится этот подход: он подчеркивает идею, что ваше резюме — это ваша первая краткая самопрезентация. Это ваш шанс за короткое время завоевать симпатию человека, который позже может рассмотреть вас в качестве кандидата на вакантную должность. Тем не менее здесь упущен один чрезвычайно важный аспект: лучшая презентация всегда адаптирована под аудиторию. Вашего резюме это тоже касается.

Каждая вакансия, на которую вы претендуете, уникальна. Даже если у должностей одинаковые названия и требования к навыкам и опыту, они все разные. Каждая компания и каждая команда пытается наймом нового человека решить свои проблемы. Как соискателю вам следует потрудиться, чтобы понять эти проблемы и составить резюме, где вы предстанете тем, кто способен помочь с ними справиться.

Каким бы безумным это ни выглядело, вам необходимо подготовить отдельную версию резюме для каждой вакансии, на которую вы претендуете. На первый взгляд может показаться, что это требует огромной работы. Однако зачастую достаточно составить несколько версий для интересующих вас типов должностей и немного их менять, чтобы адаптировать под конкретную вакансию. Вы можете сохранять все версии и отталкиваться от них, чтобы откликаться на похожие вакансии в других местах. Имея это в виду, давайте посмотрим, какие ключевые аспекты надо учитывать при составлении резюме.

6.1.2. Формат

Все соискатели в той или иной степени понимают, что резюме — их первый шанс представиться и выделиться на фоне остальных. Некоторые «эксперты» советуют делать резюме необычным и приятным глазу. С точки зрения читателя, это иногда хорошая идея. Чтобы персонализировать резюме, вы можете добавить немного графики, цвета, разделить текст на несколько столбцов и даже включить свою фотографию. Все это замечательно, только такой совет не учитывает один главный элемент современного процесса найма: *систему управления кандидатами* (ATS, applicant tracking system).

Сегодня многие организации взаимодействуют с соискателями через них. Вы легко их распознаете: зачастую это те самые сайты вакансий, которые просят вас загрузить свое резюме, а затем пытаются (с переменным успехом) проанализировать его и внести ваши данные в базу. Этот этап имеет решающее значение, потому что именно по информации, внесенной такой системой, работодатель будет в первую очередь судить о вашей квалификации. Чем лучше ATS обработает резюме, тем лучших результатов вы можете ожидать.

Так что, обдумывая формат, придерживайтесь принципа простоты. Подумайте, как сделать так, чтобы ATS было проще прочитать и правильно обработать ваше резюме. При этом следует учитывать несколько факторов.

- *Общий формат:* не разделяйте текст на столбцы, пишите в одном.
- *Графика:* не используйте графику, она ничего не даст ATS и лишь усложнит обработку документа автоматическим анализатором.
- *Шрифты:* используйте легко читаемый и распространенный шрифт вроде Arial, Times New Roman или Calibri.
- *Простой заголовок:* сделайте простой заголовок над блоком с вашей контактной информацией.
- *Заголовки разделов:* четко формулируйте и форматируйте заголовки разделов.
- *Стандартные разделы:* включите в резюме такие стандартные разделы, как «Образование», «Навыки», «Опыт работы» и «Сертификаты».

Все отлично, но что, если вы хотите иметь запоминающееся резюме, которое можно было бы вручить кому-нибудь? На этот случай создайте две версии: одну с интересным форматированием для отправки работодателю перед собеседованием и вторую для систем управления кандидатами.

Еще немного о формате. Обычно люди спрашивают, насколько объемным должно быть резюме. Это дело вкуса. Однако я как менеджер по найму могу поделиться своим мнением. Лично для меня чтение резюме длиннее двух страниц — обременительное и скучное занятие. Если ваше резюме настолько длинное, велика вероятность, что в нем слишком много нерелевантной информации. В таких случаях следует оценить все приведенные в нем сведения и оставить только те, что представляют вас идеальным кандидатом на интересующую вас должность.

6.1.3. Соответствие требованиям

Одна из самых больших сложностей при подаче заявки на вакансию — составить резюме так, чтобы оно прошло отбор ATS и попало в руки рекрутеру, а затем и менеджеру по найму. В предыдущем разделе я поделилась простыми советами о том, как следует форматировать резюме, чтобы система управления кандидатами правильно обработала информацию о вас. Я также упомянула, что важно адаптировать резюме под интересующую вакансию. Вероятно, это один из самых эффективных инструментов, позволяющих гарантировать, что ваше резюме пройдет все этапы отбора и в итоге окажется во входящих письмах у менеджера по найму.

Ранее я уже говорила, что ATS анализирует информацию в вашем резюме и вносит конкретные сведения в базу. Помимо этого, ATS выполняет еще одну важную функцию: оценивает каждую обработанную заявку. Система сопоставляет данные из вашего резюме с требованиями вакансии, на которую вы откликнулись, и в зависимости от результатов присваивает заявке оценку. Просматривать полученные заявки рекрутеры начнут, скорее всего, с тех, что набрали в ATS самые высокие баллы. Так что знать о том, как улучшить эту оценку, чрезвычайно важно.

О выборе подходящих вакансий мы поговорим в разделе 6.2, а пока будем исходить из того, что вы такую уже нашли. Вы знаете, что у вас есть навыки и опыт, необходимые для работы в этой должности, и теперь вам нужно сделать так, чтобы ATS правильно представила вас рекрутеру и менеджеру по найму. Для этого необходимо адаптировать свое резюме под конкретную вакансию, методично сопоставив информацию в нем с требованиями к кандидату.

Изучив объявление о вакансии и, в частности, список требований, вы без труда выделите в них ключевые слова. Именно на них и нужно сосредоточиться. Этими ключевыми словами могут быть названия конкретных технологий, навыков, сертификатов, ученых степеней и других важных характеристик. Нужно, чтобы адаптированное резюме

максимально соответствовало найденным ключевым словам. Далее мы рассмотрим простой процесс, который позволяет этого достичь.

Составьте список ключевых терминов

Ваш первый шаг — составить перечень ключевых терминов в описании вакансии. Просмотрите каждое требование; обычно они собраны в простой маркированный список, так что вы без труда его обнаружите. Попробуйте понять суть каждого требования, то есть что в первую очередь интересует компанию.

Во многих случаях вы выявите ключевые термины, просмотрев пункты списка. Это могут быть технологии, например брандмауэры, контейнеры или брокеры безопасности доступа к облаку (CASB), или названия конкретных продуктов, например Splunk, Kubernetes или Burp Suite. Составьте из них перечень. Каждый термин вроде Burp Suite (названия из двух и более слов) следует указывать в своем отдельном пункте.

Иногда одно требование содержит несколько ключевых терминов: например, два-три похожих продукта или связанные между собой технологии. Если в пункте больше одного ключевого термина, сделайте каждый из этих терминов отдельным пунктом. В описании вакансии они могут быть объединены по какой-то причине, но это не значит, что вам нужно указывать их вместе в своем резюме. Главное, чтобы вам было проще продемонстрировать, что у вас есть ключевые качества, интересующие работодателя.

В табл. 6.1 для примера приведены несколько требований из реальных описаний должностей и ключевые термины, которые можно внести в перечень.

Табл. 6.1. Примеры требований из описаний должностей и ключевых терминов

Требование из описания должности	Ключевой термин
Глубокие практические знания о методах и инструментах управления уязвимостями	Управление уязвимостями
Знания, касающиеся выделения, проектирования, создания и обслуживания базовых вычислительных экземпляров Azure	Azure
Опыт в обеспечении соблюдения таких нормативных требований, как ITAR, PCI или HIPAA	ITAR PCI HIPAA
Опыт работы с инструментом SOAR, например Demisto, Splunk или Swimlane	SOAR Demisto Splunk Swimlane

Если вам сложно выявить ключевой термин для конкретного требования, удалите вспомогательные слова, которые не описывают конкретный навык, технологию или качество.

Например, в первом пункте табл. 6.1 мы видим фразу «глубокие практические знания о». Эти слова определяют необходимый уровень опыта / владения навыком, но не описывают сам навык, поэтому их можно исключить. Слова «методы и инструменты» предоставляют дополнительную информацию, но навык, технологию или качество тоже сами по себе не описывают. После того как вы их отбросите, у вас останется «управление уязвимостями» — это и есть ключевой термин для этого требования.

Определите частоту упоминания ключевых терминов

При составлении перечня вы можете обнаружить, что некоторые ключевые термины повторяются. Это указывает на навыки или опыт, интересующие менеджера по найму больше всего.

Вы можете включить в перечень одинаковые пункты, а затем объединить их в один, подсчитав количество повторов, или, чтобы сэкономить время, оставить один пункт и просто отмечать повторы галочками. В целом вам нужно выявить наиболее важные требования, если они есть, и уделить им первостепенное внимание на следующем этапе, когда вы начнете сопоставлять свое резюме с ключевыми терминами.

Сопоставьте резюме с ключевыми терминами

Настало время сопоставить ваше резюме с перечнем требований. Посмотрите, какие знания, навыки и опыт вы включили в список. Обведите ключевые слова, которые встречаются в вашем резюме. Этим критериям вы соответствуете. При оценке вашего резюме ATS распознает эти ключевые слова и присвоит вашей заявке более высокий балл.

Обведя все ключевые термины, которым соответствует ваше резюме, посмотрите, для каких требований совпадений не нашлось. Есть ли в перечне термины, соответствующие вашим знаниям, навыкам или опыту, но, возможно, представленные в резюме как-то иначе? По возможности перефразируйте их описание, чтобы оно соответствовало содержанию объявления о вакансии.

При этом вы, разумеется, должны быть честны с собой и потенциальным работодателем. Не включайте в резюме ключевые слова для способностей, которых у вас нет. Вам нужно просто привести формулировки в резюме в соответствие с запросами работодателя. Если вы попытаетесь обмануть систему и добавить ключевые термины, не отвечающие вашим способностям, рекрутер легко это поймет и работу вы точно не получите.

После этого обязательно обведите в списке ключевые термины, добавленные в резюме. Теперь еще раз взгляните на перечень и на еще не обведенные ключевые термины. Описывает ли какой-нибудь из них вашу способность, выявленную в главе 4? Поищите способы включить их в резюме. Опять же, речь идет о знаниях, навыке или опыте, которыми вы владеете. Обязательно обведите их в перечне требований.

Добавьте варианты ключевых терминов

Наконец взгляните на резюме и на список ключевых терминов. Можете ли вы указать какие-то из терминов несколько раз? Возможно, вы применяли какой-то навык на нескольких предыдущих должностях. Поищите способы указать эту информацию, при этом отдавайте предпочтение вариантам ключевого термина. Большинство ATS — системы интеллектуальные. Они распознают варианты ключевого термина и присвоят более высокую оценку вашей заявке. В резюме крайне важно сначала указать прямое соответствие, однако наличие дополнительных релевантных терминов демонстрирует более высокий уровень владения способностью, и ATS это заметит.

Итак, просмотрите перечень еще раз. Доведите до максимума количество упоминаний каждого из ключевых терминов. В результате вы получите резюме, адаптированное под конкретную вакансию, а значит, позволяющее ATS и рекрутеру увидеть в вас кандидата, удовлетворяющего требованиям.

6.1.4. Вычитка

Последний шаг перед отправкой резюме — вычитка. Грамматические и орфографические ошибки воспринимаются как признак непрофессионализма, а еще они могут сбить с толку ATS, отчего та снизит оценку.

Идеально было бы попросить человека, которому вы доверяете, прочитать ваше резюме. Это стандартная практика среди писателей: она позволяет посмотреть на текст свежим взглядом и проверить его на ошибки. Еще лучше — обратиться к человеку, далекому от сферы кибербезопасности и даже информационных технологий. Он с большей вероятностью заметит слова и фразы, способные сбить с толку рекрутера, который также может не иметь опыта в сфере кибербезопасности.

Если вам некому дать свое резюме, сделайте перерыв на несколько часов (или на ночь, если возможно), а затем снова внимательно прочитайте его от начала до конца. Особенно полезно делать это вслух. Поскольку вы, вероятнее всего, не озвучивали свои мысли, когда набирали

текст, это поможет вам еще раз обдумать содержание резюме и сократить вероятность того, что вы пропустите очевидную ошибку.

6.2. Выбор вакансии и отклик на нее

Кому-то может показаться, что при трудоустройстве на рынке с миллионами свободных рабочих мест этап отклика — самый простой. Однако среди кандидатов на должности начального уровня распространенная проблема — неспособность найти подходящую для отклика вакансию. Иногда люди подают заявку на работу, для которой недостаточно квалифицированы, но в большинстве случаев не понимают, на какую вакансию стоит откликаться.

Но на этом сложности не заканчиваются. При отклике соискатели часто допускают ошибки, из-за которых их заявки не доходят до рекрутеров. А если и доходят, то из-за еще одного ряда распространенных ошибок не ведут к приглашению на собеседование. Итак, давайте рассмотрим некоторые стратегии решения этих проблем.

6.2.1. Использование инструментов для поиска работы

Что делать, если вы хотите найти работу в сфере кибербезопасности? Большинство людей обычно для начала смотрят сайты с вакансиями. Они удобны тем, что позволяют вести поиск среди множества объявлений в единой базе. Возможно, вы решите посетить два или три таких сайта. В этом случае вы заметите, что большое число объявлений размещено сразу на нескольких площадках. Вы также заметите, что некоторые вакансии, опубликованные на одном сайте, отсутствуют на другом. Чего вы не заметите, так это того, что каких-то вакансий нет ни на одном из этих сайтов.

Однако сейчас давайте сделаем шаг назад и остановимся на моменте, предшествующем поиску вакансий на подобном ресурсе. Итак, вы собираетесь взяться за серьезную задачу — поиск своей первой работы в сфере кибербезопасности. Без плана невозможно преодолеть ни одно серьезное препятствие на карьерном пути. В предыдущих главах было показано, что методичность позволяет расходовать силы более эффективно. Это касается и поиска работы. От того, как вы его организуете, во многом будет зависеть успех всего начинания.

Ранее я уже упоминала сайты с объявлениями о вакансиях. Это мощные инструменты для поиска работы, подходящей вам по способностям. Такие сайты собирают вакансии различных организаций в единую базу

с возможностью поиска. Некоторые из них специализируются на определенных отраслях или даже на определенных типах должностей в той или иной отрасли. Вы можете найти вакансии в сфере кибербезопасности как на сайтах с фокусом на ИТ, так и на ресурсах, посвященных исключительно кибербезопасности. Существуют даже специализированные сайты с вакансиями на государственные должности. У каждого сайта своя база и свой способ сопоставлять кандидатов с опубликованными вакансиями. Таким образом, наиболее эффективно будет обращаться к различным ресурсам.

Несмотря на то что эти сайты — великолепный инструмент и они содержат огромное число вакансий от различных компаний, далеко не все организации их используют. Кто-то не использует их вообще, кто-то использует лишь некоторые или публикует на них только определенные вакансии. Где же искать остальные?

На сайте почти каждой организации есть страница с информацией о карьерных возможностях. Хотя на это уйдет дополнительное время, при поиске работы полезно составить список сайтов известных вам компаний, чьи представительства находятся рядом с вами или где вы хотели бы работать, и посетить их, чтобы ознакомиться с открытыми вакансиями. Некоторые организации даже позволяют подать заявку на работу без указания конкретной должности. Конечно, это не очень успешная стратегия, но по крайней мере она позволит занести свое имя и резюме в базу данных компании и, возможно, повысить шансы на трудоустройство в будущем.

Помимо сайтов с вакансиями и корпоративных сайтов вам доступны и другие ресурсы. Если вы недавно закончили или скоро закончите учебу, то с поиском работы вам наверняка может помочь ваше учебное заведение. Во многих университетах есть центры содействия трудоустройству, а некоторые из них даже поддерживают отношения с местными компаниями и устраивают туда студентов на стажировку. Эти центры могут быть особенно полезны при поиске должностей начального уровня. Поскольку они ориентированы на недавних выпускников, то часто лучше осведомлены о таких вакансиях.

Разумеется, если вы не выпускник, а просто хотите сменить карьерное направление, вы можете не иметь доступа к этим ресурсам. Тем не менее вы вправе обратиться в местные университеты и узнать, нет ли у них подобных общедоступных сервисов. Некоторые учебные учреждения готовы оказывать определенную помощь в этом вопросе.

Вам также могут помочь рекрутеры, получающие плату от потенциальных работодателей. У них есть информация о множестве открытых вакансий, и при подборе тех, что соответствуют вашей квалификации, они сделают за вас большую часть работы.

К сожалению, у взаимодействия с рекрутерами есть обратная сторона: вашим навыкам придется пройти дополнительную проверку, и в результате, вероятно, какие-то из них вам придется совершенствовать. Рекрутеры, оказывающие подобные услуги, обычно получают комиссию, когда кандидат устраивается на работу. Поэтому они, хотя и действуют в ваших интересах, обычно не склонны рисковать и часто выбирают те должности, на которые вас примут с высокой вероятностью. Если вы не претендуете на дефицитные должности начального уровня, такой подход вполне может сработать. Однако иногда стоит рискнуть и попытаться добиться своего.

Наконец, не стоит забывать о социальных сетях. Такие хештеги, как #infosecjobs, часто помогают отыскать сообщения или твиты, касающиеся доступных вакансий. Некоторые участники ИБ-сообщества периодически создают треды, где просят подписчиков делиться информацией о вакантных должностях. Если вы пользуетесь социальными сетями, то даже можете связаться с кем-то из них: они с радостью сообщат о ваших потребностях своим подписчикам, чтобы помочь вам в поисках. Я не считаю такие методы поиска работы основными, но вам следует хотя бы иметь их в виду.

Приняв все это во внимание, вы можете решить, к каким методам обратитесь в первую очередь. В конечном счете ваш успех в большой степени зависит от того, как вы используете инструменты, имеющиеся в вашем распоряжении. Составьте план и решите, с каких ресурсов начнете. Чтобы увеличить шансы на успех, убедитесь, что в своей стратегии вы опираетесь на разнообразные источники. Теперь, когда вы знаете, где искать вакансии, давайте поговорим о том, как из них выбрать самые подходящие.

6.2.2. Поиск подходящих должностей

В главе 4 вы определились со своими интересами и с тем, какие должности в сфере кибербезопасности хотели бы занимать. Этой информации вполне достаточно, чтобы приступить к поиску работы. Однако вам также нужно определиться с тем, что именно вы ищете. Дело в том, что компании в сфере кибербезопасности не используют стандартные названия должностей. Например, в некоторых объявлениях специалист по тестированию на проникновение может называться пентестером, аналитиком информационной безопасности, этичным хакером или тестировщиком безопасности. Многие крупные сайты вакансий пытаются сопоставлять запросы с похожими ключевыми словами, но обычно у них получается не очень хорошо.

Из-за этого инструменты поиска на сайтах вакансий могут вас разочаровать. Важно понять и принять тот факт, что за один подход вы никогда не достигнете идеального результата: вам придется повторить поиск несколько раз, чтобы набрать как можно больше подходящих вакансий. Чтобы получить исчерпывающий список, перебирайте разные варианты названий должностей. Кроме того, просмотрите перечень своих способностей, составленный в главе 4, и настройте поиск по своим ключевым навыкам или опыту. Это позволит расширить список подходящих вакансий и вполне может оказаться более эффективной стратегией, чем поиск по конкретной должности.

Локация, локация и еще раз локация

При поиске по местоположению на сайтах вакансий могут возникнуть дополнительные сложности, поэтому здесь важно иметь в виду следующее. Многие площадки требуют от работодателей указывать местоположение в публикуемых объявлениях. Некоторые позволяют указывать только одно, а другие — несколько. На одних сайтах можно размещать объявления об удаленной работе (то есть о работе из дома), на других — нет. Некоторые сайты позволяют пользователям искать удаленную работу, другие — нет. Одни требуют указывать местоположение в процессе поиска, другие — нет.

Удаленная работа стала обычным явлением в сфере кибербезопасности. Хотя этот формат не особенно свойствен должностям начального уровня, такие вакансии есть, и они вполне могут вас заинтересовать.

Чтобы обойти ограничения, существующие на некоторых сайтах, компании публикуют одну и ту же вакансию с несколькими местоположениями. Если вы видите такие объявления, это может означать, что компания ищет сотрудников в разные офисы или даже для удаленной работы. Помните об этом при поиске вакансий.

В процессе вам также следует менять местоположение, насколько это позволяет сайт. Попробуйте указать только ваш регион. Если вы живете недалеко от границы между двумя регионами, попробуйте указать соседний. Если есть возможность искать без указания местоположения, попробуйте и это, однако не увлекайтесь, чтобы в итоге список вакансий не получился слишком длинным.

К поиску, как и ко всем остальным задачам, я предлагаю подходить методично. Составьте список интересующих вас должностей. Кроме того, просмотрите перечень своих способностей и выделите те, что, по вашему мнению, лучше всего соответствуют роли, на которую вы

претендуете. Начните с опыта, затем перейдите к навыкам и, если необходимо, выберите что-то из знаний. Так вы получите план поиска и гарантированно найдете вакансии, соответствующие вашим интересам и способностям.

6.2.3. Анализ требований

На каком-то этапе поиска вы начнете просматривать списки результатов и выбирать интересные варианты. Возможно, это будут вакансии из вашего района или из компаний, о которых вы слышали, а может, вы сфокусируетесь на определенных названиях должностей. Вы столкнетесь с тем, что списки требований в них разные, так что ваша задача усложнится. Вы можете даже расстроиться: кажется, вы не соответствуете ни одной из них.

В подобной ситуации кто-то решит вообще не откликаться ни на одну из них. Кто-то будет откликаться лишь на такие, какие покажутся наиболее соответствующими ему по навыкам, но при этом не особенно ему подходящие. А кто-то станет откликаться на все подряд и надеяться на лучшее, зная, что в худшем случае просто получит отказ. Однако все эти подходы хаотичны и неструктурированны. Неужели нет способа повернее? Разумеется, есть, и далее мы его рассмотрим.

Помните перечень способностей, который вы создали в главе 4? Здесь он вам снова пригодится. Только не сам перечень, а методы, с помощью которых вы его составляли. Описания должностей бывают довольно сложными, и для соискателей это проблема. Оценивая соответствие своей квалификации той или иной вакантной должности, вы должны уметь анализировать список требований и определять наиболее важные.

Итак, вы нашли несколько вакансий, которые кажутся вам интересными и на первый взгляд подходят вам по способностям. Теперь важно понять структуру их описаний. Обычно такие объявления состоят из нескольких распространенных разделов. В них обязательно есть такие основные сведения, как местоположение и название должности, а часто и ее общее описание. Часто оно сопровождается списком повседневных обязанностей, которые должен выполнять работник.

Однако нас больше всего интересуют разделы «Требования» и «Дополнительная квалификация». В первом перечислены минимальные требования, которым должен соответствовать кандидат. У этого раздела бывают разные названия: «Требования», «Минимальная квалификация» или что-то похожее. В разделе «Дополнительная квалификация» обычно перечислены прочие способности, которые могут пригодиться

человеку при работе в указанной должности. Их иметь необязательно, но тот, у кого они есть, будет считаться более квалифицированным. Этот раздел также иногда называется «Предпочтительный опыт», «Дополнительные навыки» или как-то в этом роде.

Но это все в идеальном мире, а настоящие описания до идеала часто недотягивают. В некоторых списки требований пугающе объемны. Обычно это значит, что компания включила в перечень не только самые необходимые условия. Также вы можете встретить в списках требований название конкретной квалификации с пресловутой припиской «или эквивалент». Например, «степень бакалавра или эквивалентный опыт работы» или «сертификат CISSP или эквивалент». Анализируя требования, важно выявить наиболее важные, и в этом вам помогут несколько подсказок.

Во-первых, обратите внимание на порядок требований. Это не всегда показатель, однако постарайтесь поставить себя на место менеджера по найму или специалиста из отдела кадров, составляющего описание вакансии. Он садится, обдумывает должность и пытается определить перечень требований для нее. При этом первым делом вспоминаются либо очевидные общие условия (наличие ученой степени и сертификатов), либо самые важные навыки, необходимые человеку для работы в конкретной должности. Поэтому, столкнувшись с длинным списком требований, особое значение придавайте его первым пунктам.

Еще один способ определить наиболее важные требования — изучить, как они связаны с перечисленными здесь же обязанностями. Ищите общее в используемых терминах. При необходимости запишите каждое требование, а затем отметьте, сколько раз все, что с ним связано, упоминается в описании должности или в списке обязанностей. Чем конкретнее требование, чем более узко оно сформулировано, тем меньше вероятность того, что оно будет иметь большое значение при принятии решения.

Наконец, поищите взаимосвязи между списком требований и списком дополнительных или предпочтительных квалификаций. Во многих случаях следом за общими понятиями, в разделе о дополнительной квалификации, упоминаются конкретные технологии или навыки. Например, вы можете обнаружить фразу: «Знание лучших практик в сфере облачной безопасности», а в разделе о дополнительной квалификации увидеть что-то вроде «Опыт работы с облачной архитектурой Google Cloud или Microsoft Azure». Это явно указывает на то, что умение кандидата работать с облачными технологиями особенно важно.

И последнее о требованиях. Конечно, вы хотите соответствовать как можно большему их числу, однако не думайте, что вам нужно отметить

каждый пункт, чтобы откликнуться на вакансию. Помните: в худшем случае вам просто ответят отказом. Я не призываю вас откликаться на все вакансии подряд; разумеется, здесь следует проявлять разборчивость. Однако, к сожалению, соискатели часто не подают заявку на работу, для которой они вполне подходят просто потому, что их квалификация отвечает не всем требованиям в списке.

Чем больше требований в описании должности, тем меньше вероятность, что какой-то кандидат будет полностью им соответствовать. Так что не думайте, что кто-то другой подходит для работы полностью, а вам не стоит даже пытаться ее получить. Не попадайте в эту ловушку.

6.2.4. Офисный, удаленный или гибридный формат работы

Многие люди впервые попробовали работать удаленно во время пандемии коронавирусной инфекции. Когда компании были вынуждены закрыть офисы, многим специалистам внезапно пришлось выделять место дома под мобильный офис, чтобы продолжать работать, используя такие решения для удаленного доступа, как виртуальные частные сети (VPN) и виртуальные рабочие места.

Когда офисы снова начали открываться, многие обнаружили, что предпочитают работать из дома. В результате организации перевели деятельность целого ряда специалистов в удаленный формат, а для некоторых разработали гибридный, чтобы часть рабочего времени человек проводил в офисе, а часть — дома.

Теперь эти новые условия рабочей среды стали важным фактором в процессе трудоустройства. Некоторым очень нравится идея работать полностью удаленно. Нет нужды тратить время на дорогу, обстановка вокруг комфортная и знакомая, меньше отвлекающих факторов, в организации личных встреч появляется дополнительная гибкость — все это кажется чрезвычайно привлекательным. Другим же не хочется все время находиться дома. Многие из тех, кто думал, что им понравится удаленный формат, обнаружили, что им не хватает таких аспектов работы в офисе, как общение лицом к лицу с коллегами или доступ к каким-то удобствам или оборудованию.

Важно честно изучить свои склонности и выяснить, какой режим труда подходит именно вам. Достаточно ли вы дисциплинированны, чтобы сопротивляться отвлекающим факторам домашнего офиса? Можете ли организовать себе специальное место? Есть ли у вас все необходимое, в том числе надежное подключение к интернету и телефонная связь? Рассматривая полностью удаленный или гибридный формат работы, важно учитывать все это.

Организация домашнего офиса

Ниже приведен список того, что необходимо учитывать, если вы склоняетесь к удаленному или гибридному формату.

- У вас должно быть выделено пространство для работы. Это может быть целая комната или просто письменный стол в дальнем углу. В любом случае постарайтесь сделать его постоянным рабочим местом, если это возможно (не используйте для этого кухонный стол).
- В зависимости от должности вам может понадобиться уединенное место, где другие не смогут подслушать конфиденциальный разговор. При выборе рабочего места учитывайте и это.
- Вам также потребуется стабильный и быстрый интернет. Через многие системы, к которым вы будете подключаться, проходит гораздо больше данных, чем через браузеры при посещении сайтов. Системы для видеоконференций и другие подобные инструменты особенно нуждаются в стабильном и быстром соединении.
- Надежная телефонная связь также будет иметь большое значение для работы некоторых специалистов. Есть ли у вас стационарный телефон или возможность его установить? Есть ли у вас надежная сотовая связь? Некоторые компании предоставляют программные телефоны, которые работают через компьютер.
- Будет ли у вас потребность что-нибудь распечатывать, и если да, то есть ли у вас принтер? У многих людей принтера дома нет, и этот момент они часто упускают из виду. Если вы не собираетесь работать в офисе, но вам будет нужно распечатать какие-то бланки или документы, об этом также следует позаботиться.

Впрочем, готовность работать полностью удаленно открывает больше возможностей. Если компания, в которую вы хотите устроиться, находится в другом регионе, очевидно, что вам потребуется либо переезжать, либо выбирать удаленный формат. Кроме того, для дисциплинированных и независимых людей работа в домашней обстановке может быть идеальным вариантом. Так или иначе, вам стоит определиться, какой вариант больше всего подходит именно вам.

6.3. Успешное прохождение собеседований

Итак, вы дошли до этого этапа. Вы узнали, какие есть роли в сфере кибербезопасности. Выбрали одно или два направления, на которых

хотите сосредоточиться. Провели самоанализ и инвентаризацию своих способностей. Откликнулись на несколько вакансий. И вот наконец получили письмо от одного из рекрутеров, где вас приглашают на первичное собеседование!

Благодаря проделанной работе вы сумели донести до работодателя, что вы именно тот, кого он ищет. Однако важно помнить, что собеседование — двусторонний процесс; вы можете выяснить, подходит ли вам работа, корпоративная культура и размер предлагаемой зарплаты. К сожалению, в попытках произвести впечатление на компанию очень легко забыть, что компания тоже должна произвести впечатление на вас.

Во время собеседования вы, вероятно, будете чувствовать смесь волнения и беспокойства. Этот процесс сопряжен с высоким уровнем стресса; вы захотите говорить и делать правильные вещи, чтобы повысить шансы на трудоустройство. Вам предстоит познакомиться с компанией, где вы можете провести следующие 2 года, 4 или даже 10 и больше лет. Без сомнения, это важный момент в вашей жизни. Поэтому давайте поговорим о том, как проходить собеседования.

У каждой организации свой подход к ним. Некоторые ограничиваются несколькими неформальными беседами, а другие проводят целые марафоны, иногда с оценкой технических навыков. Однако, несмотря на различия между работодателями, существуют общепринятые практики, с которыми вам будет полезно ознакомиться.

Подавляющее большинство организаций начинают с кадрового скрининга. Затем обычно следует собеседование с менеджером по найму, а после него, возможно, серия технических и групповых собеседований — на них надо быть готовым продемонстрировать владение ключевыми навыками. Также есть вероятность, что вы встретитесь с будущими коллегами по команде, сотрудниками других отделов организации или с кем-то из руководителей. Чтобы добиться успеха, крайне важно понимать формат каждой из этих встреч, их цели и способы подготовиться к ним.

6.3.1. Кадровый скрининг

Почти всегда первый разговор с соискателем, подавшим заявку, проводит рекрутер, отвечающий за начальный этап отбора. Если рекрутер связался с вами, значит, он — и, вероятно, менеджер по найму — уже просмотрел ваше резюме и решил выяснить, подходите ли вы для вакантной должности. Цель рекрутера здесь — выявить любые проблемы или пробелы в ваших навыках и опыте, позволяющие отбросить вашу кандидатуру.

Разговор с рекрутером обычно длится не больше 30 минут и почти всегда проходит по телефону. При этом интервьюер, скорее всего, потратит некоторое время, чтобы рассказать об организации и должности, на которую вы претендуете, и выразит готовность ответить на ваши вопросы.

Вероятнее всего, рекрутер спросит вас о вашей готовности работать, опыте и, возможно, желаемой заработной плате. В зависимости от организации он может захотеть узнать подробнее о ваших навыках, но обычно эта тема поднимается при разговоре с менеджером по найму или в ходе следующих собеседований. Рекрутер также должен рассказать вам о льготах и других формах вознаграждения, на которые вы можете рассчитывать.

Наконец, он обязан кратко описать весь процесс собеседования. В некоторых случаях он может сказать, что вы переходите на следующий этап отбора. Однако, как правило, рекрутеры стараются не давать каких-либо обещаний на этот счет, поскольку их действия обычно проверяют другие сотрудники организации.

С учетом этого в разговоре с рекрутером вы должны быть готовы рассказать о своем опыте, о навыках и о том, почему вы откликнулись именно на эту вакансию. Вас могут спросить, почему вы хотите сменить работу, так что приготовьте хороший и честный ответ. В основном такие интервью максимально непринужденные. Рекрутер просто пытается выяснить, достаточно ли у вас навыков, чтобы удовлетворить минимальным требованиям должности. Вероятно, он сравнит вас с другими кандидатами и пропустит на следующий этап тех, кто соответствует требованиям, а уже менеджер по найму решит, стоит ли проводить дополнительные собеседования.

Вам следует и самому подготовить вопросы: об организации, социальном пакете и самой должности. Интервьюер может переадресовать некоторые из них менеджеру по найму, однако всегда лучше спросить и получить ответ чуть позже, чем промолчать и упустить важные моменты. Кроме того, если рекрутер не рассказывает о порядке собеседования или о том, чего вам ожидать, поинтересуйтесь об этом сами. Эта информация не должна быть секретной.

Как говорилось ранее, это собеседование — ваш шанс взять интервью у организации. Точно так же, как она пытается определить, подходите ли вы для работы в ней, вы должны решить, соответствует ли эта организация вашим потребностям. Обращайте внимание на то, что рекрутер говорит о компании. Почему эта должность оказалась вакантной? Она появилась недавно из-за расширения команды? Тот, кто занимал ее, получил повышение? Ответы на эти вопросы могут многое рассказать об организации. Кроме того, отмечайте для себя то, насколько

структурированным или непринужденным кажется разговор, — это может дать вам представление о корпоративной культуре компании.

Чтобы подготовиться к собеседованию, тщательно изучите организацию и поймите, чем она занимается. Выясните, какие продукты или услуги она предлагает. По возможности узнайте о команде, к которой собираетесь присоединиться, и о том, как ее работа вписывается в общий бизнес. Нелишним будет посетить сайты с обзорами работодателей. Посмотрите, какие комментарии о компании оставили нынешние и бывшие сотрудники. Вероятно, у вас возникнут вопросы, которые вы захотите задать в ходе собеседования.

При наличии времени вы можете поискать в социальных сетях информацию о сотрудниках организации, чтобы выявить ее ключевых руководителей. Продемонстрировав в ходе собеседований, что вы знакомы с организацией, вы выделитесь на фоне остальных кандидатов. Это покажет не только вашу заинтересованность в работе, но и вашу организованность и подготовленность.

В конце интервью убедитесь, что вы знаете, чего ожидать. Скорее всего, интервьюеры скажут, что они обсудят результаты встречи между собой и свяжутся с вами по поводу дальнейших шагов. Они должны сообщить вам приблизительные сроки ответа. Если не сообщат, спросите об этом сами. В любом случае вам следует ожидать ответа и знать, когда будет уместно обратиться за ним, если вы его не получите.

Вопрос о зарплате

В разговоре с рекрутером, а иногда и в ходе последующих собеседований, вас могут спросить, какую вы ожидаете получать заработную плату в случае, если займете вакантную должность.

При этом вас не должны спрашивать о том, сколько вы зарабатываете сейчас. Хотя раньше такая практика была довольно распространена, она постепенно теряет популярность среди рекрутеров, и во многих местах потенциальные работодатели вообще не имеют права интересоваться, сколько человек зарабатывал раньше. Вам следует ознакомиться с соответствующими местными законами и, если вопрос о прежней зарплате все-таки поступит, вежливо перевести обсуждение в русло того, сколько вы ожидаете получать в новой должности.

Вы должны идти на собеседование с четким представлением о желаемом размере зарплаты. К сожалению, несмотря на то что организации обязаны открыто сообщать о своих диапазонах зарплат, лишь немногие из них предоставляют эту информацию по собственной воле. Вы можете самостоятельно провести небольшое исследование. Диапазоны

зарплат публикуются на некоторых сайтах с вакансиями. Иногда они основаны на обзорах заработных плат для схожих вакансий, а иногда — на опросах сотрудников конкретных организаций.

Проанализируйте объективно собственную квалификацию и сопоставьте ее с полученной информацией; так вы узнаете реалистичный размер зарплаты, на который можете претендовать. Помните: если вам все-таки предложат работу, эта цифра станет предметом переговоров, поэтому называйте разумную сумму, которая входит в диапазон зарплат, соответствует вашей квалификации и притом позволяет получать максимальный доход.

6.3.2. Собеседование с менеджером по найму

Во многих организациях после интервью с рекрутером проводится собеседование с менеджером по найму. Это ваш шанс по-настоящему блеснуть: в конце концов, именно он принимает решение о приеме кандидата на работу. Это также ваш шанс познакомиться с потенциальным начальником. Несмотря на свое желание продемонстрировать уверенность и профессионализм, постарайтесь вести себя непринужденно, чтобы почувствовать, каким будет повседневное взаимодействие.

Менеджер по найму почти наверняка захочет подробно поговорить о вашем опыте, умениях и подходе к работе. Он также, скорее всего, расскажет вам о своих ожиданиях, о методах управления командой и о наиболее важных навыках, которые вам потребуются в новой должности.

Однако в ходе этого собеседования вы должны не только ответить на множество вопросов относительно своих навыков и опыта работы, но и задать конкретные вопросы о предстоящих обязанностях, если они оказались вам непонятны из описания должности. Вы также можете спросить об отношениях между коллегами по команде и о месте этой команды в организации.

К этому собеседованию очень важно подготовиться. Как только встреча с менеджером по найму будет назначена, найдите его в социальных сетях. Узнайте больше об этом человеке, о его опыте и взглядах на темы, связанные с кибербезопасностью, если он публикует такие сообщения. Ищите точки соприкосновения или темы, на которые вы сможете с ним поговорить. Если найдете видео с его выступлениями, его статьи или посты в блогах, просмотрите их, чтобы лучше узнать потенциального начальника как человека.

Все это поможет вам понять, чем мотивированы задаваемые им вопросы, и подготовить ответы. При этом я не призываю вас подстраиваться или отвечать нечестно в попытке соответствовать чужим убеждениям. Будьте аккуратны, ссылаясь в разговоре на материалы, опубликованные вашим собеседником: достаточно сделать это один или два раза при обсуждении релевантных тем. Если же вы станете упоминать их слишком часто, вас примут скорее за преследователя, чем за организованного и информированного кандидата.

К концу собеседования у вас должно сложиться представление о том, как будет выглядеть ваша повседневная работа и межличностное взаимодействие с потенциальным начальником. Прежде чем завершить собеседование, убедитесь, что вы получили информацию о дальнейших шагах, о том, когда вам ожидать ответа и с кем следует связаться (скорее всего, это будет рекрутер, а не менеджер по найму).

Стратегический подход к вопросам

На каждое собеседование следует приходить с подготовленными вопросами. Задавать правильные вопросы иногда более эффективно, чем демонстрировать свои навыки и опыт. Задавая вопросы, показывающие вашу осведомленность об особенностях бизнеса и/или вакантной должности, вы выделяетесь на фоне остальных кандидатов.

Задавая хорошие вопросы, вы демонстрируете, что уже думаете о работе и потенциальных проблемах.

Например, если у вас есть опыт обращения с технологиями, перечисленными в описании должности, вы можете спросить, какие конкретно функции использует организация или с какими проблемами при этом сталкиваются ее сотрудники. Если в описании упоминаются конкретные ИБ-фреймворки или нормативные требования, вы можете поглубже изучить, насколько хорошо организация им соответствует.

Повторюсь: это отличный способ выделиться и продемонстрировать не только понимание предстоящей работы, но и свой энтузиазм. Будучи менеджером по найму, я всегда уделяла особое внимание вопросам от кандидатов. По ним я формировала представление о том, насколько человек предан делу и организован, а также о его поведении в тех или иных ситуациях.

6.3.3. Техническое собеседование

После разговора с рекрутером и менеджером по найму вам, скорее всего, предложат пройти техническое собеседование. Иногда оно может

состояться даже до встречи с менеджером по найму. Технические собеседования вызывают у кандидатов больше всего беспокойства. В ходе этой встречи ваши навыки будут проверять, и вам, вероятно, придется разговаривать с человеком или даже несколькими людьми, чей опыт значительно превосходит ваш. Однако пусть вас это не пугает. Помните, что вам удалось дойти до этого этапа благодаря тому, что вы уже сделали, и навыкам, которые вы развили и указали в резюме.

Как я уже говорила, во время технического собеседования вы, вероятно, встретитесь с одним или несколькими сотрудниками организации. Это могут быть члены команды, к которой вы собираетесь присоединиться, или сотрудники из других подразделений. Как следует из названия, цель технических собеседований — оценить технические способности кандидата. При групповом собеседовании интервьюеры также могут оценить, насколько хорошо вы вписываетесь в команду. Так или иначе, ведите себя непринужденно, постарайтесь расслабиться и получить удовольствие от процесса.

Формы собеседования в организациях разные. Иногда встречи проходят по определенной программе. Интервьюеры могут подготовить список вопросов, делать по ходу заметки и даже ставить вам оценку, исходя из ваших ответов. В других случаях процесс протекает более непосредственно, а опрос больше напоминает обсуждение гипотетических ситуаций, чем викторину. Характер ваших ответов будет зависеть от типа вопросов.

Если на техническом собеседовании вам задают прямые вопросы, как в тесте, постарайтесь давать на них краткие и прямые ответы. При этом предоставьте достаточное количество деталей, но не отходите от темы и не пытайтесь заполнить время, говоря о том, в чем вы не вполне уверены. Стремитесь отвечать максимально подробно, однако в случаях, когда чего-то не знаете, честно в этом признавайтесь.

Если же на техническом собеседовании вы слышите гипотетические вопросы, начинающиеся со слов «Расскажите о том случае…» или «Как бы вы поступили, если бы…», постарайтесь предоставить более развернутый ответ. Задавая подобные *поведенческие вопросы*, интервьюеры хотят, чтобы вы продемонстрировали свои навыки и в то же время поведали больше о своих поведенческих привычках. Для ответа на них часто используется методика STAR.

Рис. 6.1. Методика STAR для составления ответов на поведенческие вопросы

Методика STAR (Situation, Task, Action, Results) — это простая схема для составления ответов на поведенческие вопросы. Она наиболее эффективна, когда вы опираетесь на свой

опыт, однако ее также можно использовать при описании своих действий в гипотетической ситуации. Цель в том, чтобы нарисовать для интервьюера мысленную картину того, как вы вели себя в прошлом или как поступили бы в той или иной ситуации, если бы она возникла. Эта методика предусматривает следующие шаги.

— *Ситуация:* создайте контекст для ситуации, которую вы собираетесь описать.
— *Задача:* опишите проблему или свои ожидания.
— *Действие:* подробно расскажите о том, что вы сделали или собираетесь делать.
— *Результаты:* поделитесь фактическими или ожидаемыми результатами.

Подготовка к техническому собеседованию — сложная задача. Чтобы ее упростить, сразу после назначения встречи попросите рекрутера поделиться советами относительно подготовки или уточните, какие вопросы вам могут задать. Я сделала так однажды во время собеседования на должность, и в итоге рекрутер запланировал для меня 30-минутное подготовительное телефонное интервью, которое снабдило меня большим объемом информации о том, чего стоит ожидать. Такого рода запрос не только позволяет вам лучше подготовиться к собеседованию, но и демонстрирует вашу заинтересованность и организованность.

Вам также следует потратить некоторое время на изучение людей, которые будут участвовать в собеседовании. Используйте социальные сети и другие ресурсы, чтобы узнать, какой у них опыт, какими темами или технологиями они интересуются, как подходят к решению различных технических проблем. Это поможет вам понять, какие вопросы они, вероятнее всего, зададут, а также воздержаться от обсуждения слишком сложных для вас тем.

Технические собеседования могут быть особенно утомительными. Иногда они длятся более часа. Относитесь к ним как к сдаче выпускного экзамена. Выспитесь, спланируйте день так, чтобы избежать лишнего стресса, и постарайтесь максимально расслабиться и сосредоточиться.

Хотя цель такого собеседования — объективно оценить ваши навыки, в процессе у вас, вероятно, будет шанс задать и свои вопросы. Если вам доведется поговорить с коллегами по команде, вы сможете узнать больше о своем потенциальном начальнике. Спросите о том, какие повседневные обязанности необходимо выполнять в должности, на которую вы претендуете, о работе команды, о том, как она взаимодействует с менеджером и с какими сталкивается проблемами. Это один из самых

подходящих моментов для знакомства с внутренней культурой организации и команды.

В конце собеседования вам, опять же, следует узнать, каковы ваши дальнейшие шаги и когда будет известен результат. Если у интервьюеров нет этой информации, вам, возможно, придется связаться с рекрутером. В любом случае убедитесь, что вы знаете, когда ждать обратной связи и когда будет уместно напомнить о себе.

Что, если вы просто не знаете

Честность — это не просто этическое правило, которого необходимо придерживаться в процессе собеседования; она может быть эффективным инструментом, помогающим выделиться на фоне остальных кандидатов. Например, если вы не знаете ответа на вопрос, то лучше честно признаться в этом, чем пытаться обмануть собеседников. Хорошие интервьюеры способны быстро распознать такой обман. Поэтому, если вы не уверены в ответе, признайтесь в этом, а затем постарайтесь дойти до него логически с помощью имеющихся знаний.

Например, в ходе одного из технических собеседований меня спросили о программной атаке под названием «загрязнение прототипа», о которой я никогда не слышала. Я сразу сказала, что не знакома с этим типом атак. Затем я отметила, что в контексте разработки программного обеспечения под прототипом понимается объект или метод, а «загрязнение» предполагает его злонамеренную модификацию или внедрение в него вредоносного содержимого.

Этот подход оказался эффективным: так я продемонстрировала, что, хотя и не знала о таком типе атак, я имела достаточно фоновых знаний, чтобы понять, о чем речь. Я также проявила способность логически обдумывать проблему и приходить к разумному выводу. После того как меня приняли на ту работу, человек, задавший этот вопрос, сказал мне, что мой ответ его сильно впечатлил.

6.4. Рассмотрение предложения о работе

Итак, это случилось. После всей проделанной работы и успешного прохождения собеседований вам наконец позвонили и сказали, что вас готовы нанять. Вероятно, вам уже прислали электронное письмо с официальным предложением. На этом процесс не заканчивается, так как вам, возможно, еще придется провести переговоры, чтобы обеспечить себе наилучшие условия.

6.4.1. Не торопите события

Для начала, когда вам звонят и предлагают работу, вы вовсе не обязаны это предложение принять. Если к тому моменту у вас возникли сомнения по поводу обязанностей, людей, культуры или чего-то еще, нет никаких причин, по которым вы были бы вынуждены согласиться на должность. Звонок с предложением работы, скорее всего, поступит от рекрутера, менеджера по найму или от них обоих. Они, вероятно, расскажут вам о заработной плате, бонусной программе и соцпакете, включающем отпуск и больничные. Большинство компаний отправляет кандидатам официальное письмо с подробным описанием всех условий.

Когда вам позвонят, проявите любезность и поблагодарите за предложение и предоставленную возможность. Однако я настоятельно рекомендую вам попросить некоторое время на обдумывание. Не стоит опасаться, что эта просьба покажется проявлением неблагодарности или незаинтересованности. Вы даже можете сказать, что очень рады, но вам нужен день или два на то, чтобы прочитать условия предложения (если вам предоставят его в письменной форме) или чтобы обдумать их до того, как вы официально с ними согласитесь.

Если у вас есть сомнения по поводу работы или предложения, которое вам сделали, у вас будет шанс собраться с мыслями и решить, чего хотите: сразу его отклонить или договориться о более выгодных условиях. Даже если вы довольны условиями, полезно выделить время на то, чтобы еще раз спокойно и тщательно их обдумать. Вероятно, в этот момент вы будете испытывать эмоциональное возбуждение, и такой шаг назад поможет вам избежать неожиданностей.

Если вам прислали предложение в письменном виде, найдите возможность полностью его прочитать. Узнайте о заработной плате, других видах компенсации (включая бонусный пакет или подписной бонус), льготах и так далее. Если у вас есть конкретные вопросы о соцпакете, самое время получить ответы на них. Потратьте хотя бы несколько часов или даже пару дней на то, чтобы обдумать предложение и убедиться, что оно вас устраивает. Определитесь, сколько времени вам нужно, притом помните, что на должность могут претендовать и другие кандидаты, которым организация, ожидая вашего решения, еще не ответила. Обычно вполне приемлемым сроком для рассмотрения предложения считаются один-два рабочих дня.

6.4.2. Переговоры по поводу улучшения условий

Предложение о работе — это не что-то окончательное. По словам Кирстен Реннер, специалиста по подбору сотрудников на должности в сфере

кибербезопасности, «все обсуждаемо». Если вас не устраивает предложенная зарплата, вы можете попросить ее увеличить. Если количество дней отпуска кажется вам недостаточным, попросите больше. В конце концов, вам необходимо убедиться, что вас устраивает предложение, а не соглашаться на то, что не соответствует вашим потребностям.

Однако имейте в виду, что переговоры предполагают взаимные уступки. Иногда компания не может изменить определенные условия, но готова компенсировать это другими способами. Например, предлагаемый размер зарплаты находится у верхней границы допустимого для этой должности диапазона, и компания не готова его увеличивать. В этом случае она может предложить вам подписной бонус, дополнительные дни отпуска или более высокую премию.

Если вы решили договориться о более выгодных условиях, определитесь, что для вас наиболее важно. Будьте реалистами и поймите, что вы можете не получить все, что хотите. С другой стороны, не бойтесь хотя бы попросить. Хуже всего — принять не устраивающее вас предложение, потому что вы боитесь, что компания его отзовет и наймет кого-то другого. Такое случается редко, а если и случается, то обычно служит признаком токсичной культуры, в которой вы, вероятнее всего, в любом случае не захотели бы работать.

При переговорах первым делом следует перечислить условия, которые вас не устраивают, и предложить разумный компромисс. Не начинайте с отклонения. После того как вы откажетесь от работы, у компании не останется перед вами никаких обязательств, и она, скорее всего, прекратит общение с вами. Если вам повезет, у вас спросят о причинах отказа, но лучше не рисковать. Вместо этого поблагодарите, а затем объясните, какие из условий вас не устраивают, и озвучьте вариант изменения.

Ключ к успешным переговорам при приеме на работу — разумность и готовность к сотрудничеству. Будьте уверены в себе и добивайтесь той зарплаты, на которую вы вправе рассчитывать, но не ведите себя высокомерно и не выдвигайте нереалистичные требования. Это быстро сведет переговоры на нет. Помните, что в случае успеха вам предстоит ежедневно работать с этими людьми. Поэтому будьте тверды, но вежливы и сохраняйте профессионализм.

6.4.3. Трудовое соглашение

Наконец, следует выяснить, нужно ли вам подписывать трудовое соглашение. Во многих организациях необходимо подписать соглашение, которое может содержать пункты о неконкуренции и непереманивании сотрудников.

Пункты о *неконкуренции* обычно включают условия, запрещающие вам работать на конкурентные организации в течение определенного времени после ухода с нынешнего места. В пунктах о *непереманивании сотрудников* обычно указывается, что в течение определенного периода после увольнения вы не должны пытаться склонить к уходу других сотрудников компании. Соглашение также иногда содержит пункты, где говорится, как вам можно и как нельзя взаимодействовать с клиентами компании в конкретный промежуток времени. Узнайте об этих правилах заранее, поскольку в будущем, если вы решите уволиться, они станут для вас ограничивающим фактором.

Условия трудового соглашения традиционно не подлежат обсуждению: подписать его обязан каждый сотрудник компании. Вы можете попробовать договориться о компромиссе, если вас не устраивает конкретный пункт, но работодатели редко делают исключения. Вам также следует помнить о местных законах. Где-то не разрешается включать пункты о неконкуренции, а значит, эта часть соглашения может оказаться недействительной. В конечном счете вы подписываете контракт, и, если вас что-то беспокоит, имеет смысл посоветоваться с юристом.

ПОДВЕДЕНИЕ ИТОГОВ

- При составлении резюме убедитесь, что оно форматировано так, чтобы система управления кандидатами с легкостью его обработала, а также что оно содержит ключевые слова, которые система без труда сопоставит с требованиями из описания должности.
- При выборе подходящих вакансий необходимо оценить свои личные цели и соответствие навыков должностным обязанностям. Кроме того, вам следует проанализировать перечисленные требования и выявить те, что наиболее важны для менеджера по найму.
- Базовые навыки должны быть представлены в резюме так, чтобы они правдоподобно совпадали с должностными обязанностями. Покажите, как навыки, полученные при деятельности, не связанной с кибербезопасностью, подготовили вас к работе в интересующей должности.
- Готовьтесь к каждому собеседованию с учетом его типа. Предварительные исследования играют здесь решающую роль.
- Избегайте ловушек: не стесняйтесь подавать заявки на работу, будьте честны и не скрывайте пробелы в технических знаниях.

Часть III

Обеспечение долгосрочного успеха

Сейчас вы, вероятно, думаете: о чем еще здесь можно говорить? Вы узнали о сфере кибербезопасности и карьерных направлениях в ней. Провели самоанализ, чтобы выбрать то, что подходит именно вам, и вооружились знаниями, необходимыми для успешного поиска работы. Тем не менее последнее, что нужно любому человеку, — начинать карьеру, которая быстро завершится. Вкладывая силы в свое будущее в кибербезопасности, вы, вероятно, рассчитываете на продолжительный путь. Именно об этом мы и поговорим в третьей и последней части этой книги.

В главе 7 речь пойдет о важности наставничества и нетворкинга[11]. В ней вы познакомитесь со стратегиями для выстраивания сети профессиональных контактов с помощью инструментов, имеющихся в вашем распоряжении. Вы также узнаете о проверенных методах поиска наставника и выборе наиболее ценных для себя видов наставничества.

В главе 8 вы найдете исчерпывающий разбор так называемого синдрома самозванца — серьезного карьерного препятствия, с которым вы наверняка столкнетесь. Здесь не только дано определение этого синдрома и его причины, но и описаны инструменты, помогающие нивелировать негативное влияние этого синдрома на карьеру.

---

[11] Сеть полезных связей в профессиональном кругу. — *Прим. ред.*

И в завершение мы поговорим о долгосрочном успехе: глава 9 посвящена карьерным целям. В ней мы также поговорим о смене направления в сфере кибербезопасности и подготовке к этому. В самом конце руководства вы узнаете, как применить все полученные знания на практике.

Итак, вы почти у цели. Разумеется, завершение чтения для вас лишь начало. Я уверена, что это руководство будет приносить вам пользу на протяжении многих лет. А теперь устройтесь поудобнее и приготовьтесь узнать, в чем залог успешной и длительной карьеры в сфере кибербезопасности. Вы этого ждали — и время наконец пришло.

Глава 7
Мощь нетворкинга и наставничества

В этой главе

- Инструменты для создания сети профессиональных контактов
- Поиск наставника с правильными характеристиками и чертами
- Формирование наставнических отношений на основе реалистичных ожиданий
- Вежливое прекращение наставнических отношений

В главе 6 мы обсудили, как подготовиться к поиску работы, а также как повысить шансы на то, что вас пригласят на собеседование, и как провести эффективные переговоры по поводу условий труда. Эти стратегии должны помочь вам найти и занять выгодную позицию, но иногда этого оказывается недостаточно. Именно здесь в игру вступает ваша сеть деловых контактов и профессиональное развитие через наставничество.

Чтобы лучше проиллюстрировать, почему важно иметь обширную сеть профессиональных контактов, я расскажу о собственном опыте. Недавно я заняла новую должность, благодаря чему достигла одной из моих высочайших карьерных целей. Однако эту вакансию я нашла не в интернете: информация о ней вообще не публиковалась в сети.

Я узнала о ней от директора по информационной безопасности, с которой общалась через LinkedIn, Twitter и в ходе виртуального круглого стола. Именно в разговоре об этой роли, а также о моем опыте и целях мне стало известно о такой возможности. Собеседница представила меня менеджеру по найму, и, как только вакансия была официально опубликована, меня пригласили на собеседование.

Как говорится в старой поговорке, важно не *что* вы знаете, а *кого* вы знаете. Это особенно верно в контексте трудоустройства в сфере кибербезопасности. Мощная сеть деловых контактов: взаимодействие с профессионалами через социальные сети, в ходе встреч и других мероприятий — способна открыть перед вами новые горизонты так же, как это было в моем случае.

Преимущества сети не ограничиваются трудоустройством. Вы получите доступ к профессионалам — потенциальным наставникам. Наставника можно найти во множестве мест, причем необязательно даже работать с ним в одной области. Это человек, который помогает вам профессионально развиваться, делится своим мнением и знаниями, чтобы вы достигли успеха в интересующей должности. Итак, давайте поговорим о том, что могут дать вам нетворкинг и наставничество, и об эффективном использовании этих инструментов.

7.1. Создание сети профессиональных контактов

Если вы проведете некоторое время на профессиональной платформе вроде LinkedIn, то наверняка столкнетесь с обсуждением нетворкинг-мероприятий. Это неудивительно, учитывая, сколько внимания в деловом мире уделяется выстраиванию сетей профессиональных контактов. Встречи профессионалов для обмена знаниями — мощный инструмент для тех, кто заинтересован в развитии своей карьеры.

Однако для человека, ищущего первую работу в новой для себя отрасли, создать и развить такую сеть может оказаться сложно. Наладить взаимодействие с представителями сферы гораздо проще, когда вы уже сами в ней работаете. Тому, кто находится за ее пределами, вероятно, будет трудно даже решить, с чего начать. К счастью, есть практики и методы, помогающие преодолеть это препятствие.

7.1.1. Социальные сети

Социальные сети играют в нашей жизни огромную роль. Задумавшись о профессиональном нетворкинге, вы, скорее всего, первым делом

вспомните о них. С одной стороны, это прекрасный инструмент: социальные сети упрощают путь к достижению цели и позволяют обойти многие барьеры, описанные далее. С другой — с ними связаны определенные проблемы, которые вам необходимо осознать и решить, чтобы эффективно использовать этот инструмент для нетворкинга.

Одна из замечательных особенностей социальных сетей — то, насколько через них легче взаимодействовать с людьми по всему миру, разделяющими ваши интересы. В нашем случае этот интерес — кибербезопасность или даже ее конкретное направление (возможно, то, которое вы указали в своем заявлении о личной цели в главе 4).

Что бы вы ни решили по поводу нетворкинга, главное — действовать сознательно. Нельзя пускать все на самотек или надеяться на счастливый случай. Если сочтете, что вам это нужно, тщательно обдумайте, какие аспекты кибербезопасности вас интересуют и как вы будете взаимодействовать с людьми со схожими интересами.

Но как выбрать нужных людей и как с ними связаться? Вне зависимости от платформы один из самых простых способов — найти относительно известных людей и подписаться на них или обратиться к ним напрямую. Это может быть журналист, написавший статью на интересующую вас тему, связанную с кибербезопасностью, или популярный участник ИБ-сообщества, специализирующийся на ней или выступивший с соответствующим докладом. Так или иначе, цель — не столько ознакомиться с позицией этого человека по тому или иному вопросу, сколько обратить внимание на людей, которые комментируют и распространяют его материалы.

Это важно по двум причинам. Во-первых, так вы найдете разделяющих ваши интересы людей, на которых также можете подписаться. Это простой способ наполнить свои ленты на разных платформах комментариями тех, с кем вы, вероятно, захотите пообщаться в будущем. Во-вторых, это окно для взаимодействия. Чтобы приступить к созданию сети контактов, достаточно лишь прокомментировать чей-нибудь пост и поделиться своими мыслями или задать вопросы по теме этого поста. Вам может ответить если не сам автор, то кто-то из его подписчиков — так вы начнете общаться с этим человеком или даже установите с ним более близкий контакт.

Ключ к успешному нетворкингу в социальных сетях — взаимодействие. Чем активнее вы будете в киберпространстве, тем больше людей увидят вас и поймут, что вас интересуют такие-то темы. Чем больше сообщений тех, на кого вы подписаны, попадет в вашу ленту, тем лучше вы их узнаете.

Есть даже вероятность, что вы наткнетесь на пост об открытой вакансии. Если кто-то достаточно хорошо с вами знаком и в курсе, что вы

ищете работу, он может обратиться с предложением конкретно к вам. Налаживая связи, вы будете находить все больше тех, с кем стоит установить контакт. Это произойдет относительно быстро, если вы готовы посвящать всего пару часов в неделю общению с профессионалами в интересующей вас области.

7.1.2. Отраслевые группы и нетворкинг-мероприятия

Как я уже говорила, деловой мир уделяет большое внимание профессиональному нетворкингу. Сфера кибербезопасности — не исключение. Многие группы и организации предоставляют людям, которые в ней работают или интересуются ею, возможность построить сеть профессиональных контактов и обменяться знаниями.

У разных групп разные цели. Некоторые представляют собой профессиональные организации общей направленности, которые занимаются концептуальными вопросами кибербезопасности. У других техническая специализация, и они фокусируются на обмене информацией и развитии навыков своих участников. Третьи сосредоточены на том, чтобы удовлетворить конкретные потребности ИБ-сообщества, в частности, привлечь больше женщин и представителей этнических меньшинств. Но одна вещь объединяет большинство из них: они все готовы принять в свои ряды новых участников.

Сеть профессиональных контактов способна сыграть в этом свою роль. Общаясь с представителями отрасли в социальных сетях, вы, несомненно, будете узнавать о встречах и других нетворкинг-мероприятиях. Это поможет определиться с тем, к какой организации вы хотите присоединиться. Некоторые национальные и даже международные организации имеют местные отделения. Количество таких отделений в разных регионах разное. Имеет смысл изучить доступные варианты и найти для себя наиболее интересные.

Одна из проблем заключается в том, что интровертам — тем, кто испытывает неловкость при общении или страдает более серьезными социальными тревожными расстройствами, — скорее всего, будет сложно ориентироваться внутри таких групп. Однако даже они могут здесь найти для себя нечто полезное. Если вы из их числа, попробуйте поискать местное отделение или группу, которые уделяют основное внимание развитию навыков. Они иногда проводят соревнования типа CTF или мастер-классы, посвященные конкретному инструменту или технике. На встречах такого типа круг людей для общения сильно ограничен, так что участники испытывают меньше напряжения, чем на более масштабном мероприятии.

Помимо специфических местных групп, существует несколько международных организаций в сфере информационной безопасности: вы можете обратиться в их отделения.

Группы DEF CON

Появившиеся благодаря одноименной хакерской конференции, *группы DEF CON* — это локальные организации, распространенные по всему миру. Хотя у каждой из них свой подход к проведению встреч и мероприятий, они предоставляют отличную возможность для взаимодействия с другими ИБ-специалистами, энтузиастами и хакерами. В США для обозначения этих групп используются телефонные коды городов; например, DC414 — это группа DEF CON в Милуоки, штат Висконсин. Той же практики придерживаются и на международном уровне, но, разумеется, коды варьируются в зависимости от страны. Как правило, встречи, организуемые группами DEF CON, бесплатны для посещения.

Организация OWASP

Международная организация *Open Web Application Security Project* (OWASP) фокусируется на безопасности программного обеспечения и его разработке. У нее есть локальные отделения по всему миру, где регулярно проводятся различные мероприятия. В некоторых случаях их участники привлекаются к работе над какими-то из проектов OWASP. В других отделениях мероприятия больше напоминают собрания, где просто обсуждаются текущие темы, касающиеся информационной безопасности.

Если вы найдете местное отделение, свяжитесь с его руководителями, чтобы узнать, как оно работает, и решить, насколько оно вам подходит. Некоторые группы OWASP принимают в свои ряды только зарегистрированных участников проекта OWASP, хотя иногда для посещения их собраний членство в нем не требуется. Все подробности вы также можете выяснить у руководителей.

Организация ISACA

ISACA — это международная организация, сертифицирующая специалистов в области кибербезопасности. Она фокусируется скорее на специалистах-практиках, на людях, отвечающих за защиту компаний, чей бизнес может и не иметь отношения к кибербезопасности. У нее есть филиалы по всему миру. Однако за вступление в нее взимается плата, а членство в местном отделении обычно требует дополнительных взносов.

Вы можете узнать больше, если обратитесь к руководству местного отделения или даже посетите собрание в качестве гостя. Так вы поймете, насколько вам это интересно, прежде чем заплатите за годовое членство.

7.1.3. Другие встречи, конференции и мероприятия

Помимо вышеперечисленных, у участников ИБ-сообщества есть множество других возможностей для общения. По количеству международных, национальных и локальных конференций кибербезопасность опережает большинство других отраслей. Эти мероприятия часто организуют участники сообщества, чтобы специалисты развивали свои навыки и налаживали сеть профессиональных контактов. В некоторых случаях собственные конференции проводят поставщики продуктов и услуг в сфере кибербезопасности. Как было сказано в главе 5, это прекрасный способ потренироваться, а также установить деловые связи — особенно если вы общительны.

Кроме того, поставщики продуктов и услуг, группы ИБ-специалистов и другие организации проводят разовые встречи и мероприятия, позволяющие участникам расширить свою сеть контактов. Это может быть что угодно: от семинаров с приглашенными докладчиками до круглых столов и даже дегустации вин. Обращайте внимание и на такие встречи. Возможно, на многих из них вам придется выслушать небольшую рекламную презентацию, но в то же время вы получите шанс встретиться с другими представителями отрасли и познакомиться с ними.

7.1.4. Как обеспечить продуктивность сети контактов

Ключ к созданию работающей сети профессиональных контактов — наличие плана и намерения. Как и в случае с большинством других проектов, это дело также требует постоянного вложения сил и внимания; просто построить сеть и забыть о ней — не вариант. Чтобы она развивалась, вы должны быть ее активной частью. Если вы перестанете взаимодействовать с участниками своей сети, то связи, которые вы наладили, могут постепенно сойти на нет.

Разработайте план и поставьте цели по развитию своей сети. Убедитесь, что они реалистичны, и с их помощью поддерживайте свою мотивацию. Вы должны взять на себя обязательство делать то, что нужно, и нести ответственность за достижение целей.

Строя сеть контактов, старайтесь повысить свою вовлеченность. Нетворкинг — это двусторонний процесс. Ожидая помощи от участников своей сети, не забывайте сами помогать тем, с кем общаетесь. Чем больше людей будут знать вас как отзывчивого человека, тем охотнее они будут отвечать вам взаимностью.

Тем не менее не стесняйтесь обращаться за помощью. Попросите тех, чьему мнению вы доверяете, просмотреть ваше резюме. Свяжитесь с теми, с кем хотите работать, и узнайте, есть ли в их организации какие-либо вакансии. Даже если вакансий нет, там вас могут направить к людям, нуждающимся в ком-то вроде вас.

Все это кажется очевидным, но иногда начинающие и даже опытные профессионалы создают отличную сеть контактов, а потом боятся прибегать к ее помощи. Вспомните, зачем вы потратили время, чтобы ее развить, а затем извлеките из нее пользу.

7.2. Роль наставничества

В общем смысле *наставник* — это опытный человек, который может стать для вас советником и помогать вам принимать ключевые решения или продвигаться по карьерной лестнице. Тема наставничества часто поднимается в ИБ-сообществе, особенно в контексте поддержки новых профессионалов при входе в отрасль.

Однако наставничество ценно во всех отраслях и на каждой ступени карьерной лестницы. Многие топ-менеджеры известных организаций до сих пор работают с наставниками, чтобы развиваться и совершенствовать свои навыки. Важно помнить, что такие отношения могут и должны приносить удовольствие обеим сторонам.

Найти наставника порой трудно, и есть разные подходы к решению этой задачи. Лично у меня наиболее продуктивные отношения такого типа формировались сами собой. Я не искала человека специально: просто долго работала с ним и обнаружила в нем замечательного наставника.

Однако есть и более формальные способы найти себе наставника. Некоторые организации даже разработали для этого специальные платформы, позволяющие связать молодых или начинающих профессионалов с наставниками в выбранном ими направлении кибербезопасности. Существует несколько таких платформ, и некоторые из них взимают за пользование довольно высокую плату. Cyber Mentor DoJo (https://cybermentordojo.com) — хорошая бесплатная платформа. Вы можете создать там учетную запись и просмотреть список наставников, чтобы найти самого подходящего.

Если вы предпочитаете менее формальные методы, то можете использовать хештег #CyberMentorMonday в Twitter, чтобы найти наставника или объявить, что вы его ищете. Какой бы способ вы ни выбрали, важно знать, на какие качества стоит обращать внимание, чтобы убедиться, что наставник вам подходит.

7.2.1. Качества хорошего наставника

При поиске и выборе наставника, очень важно удостовериться, что этот человек обладает определенными качествами. Некоторые из ключевых характеристик хорошего наставника вполне ожидаемы, а другие менее очевидны.

Первое качество хорошего наставника — это *честность*. Вы ищете человека, способного честно и прямо сообщать как хорошие, так и плохие новости. Это не значит, что он должен предоставлять обратную связь чрезмерно прямолинейно; важно, чтобы он указывал на те области, которые требуют совершенствования. В конце концов, именно для этого и нужны наставники. К сожалению, у некоторых наставников навык межличностного общения развит недостаточно, чтобы обратная связь от них была продуктивной и честной. Общаясь с участниками своей сети контактов, примечайте тех, кто способен сообщать суровую правду так, что она вдохновляет вас на действия.

Энтузиазм — еще одно важное качество хорошего наставника. Такой человек не просто увлечен кибербезопасностью: он также с готовностью делится знаниями и помогает обучать других. Многие участники ИБ-сообщества не стремятся формировать отношения такого типа. При поиске наставника обращайте внимание не только на то, с какой страстью человек обсуждает темы кибербезопасности, но и на то, насколько активно он делится своими знаниями и идеями.

Также любой хороший наставник имеет свою *мощную сеть профессиональных контактов*. Хороший наставник — не тот, кто знает все, что вы хотите знать, а тот, кто при необходимости свяжет вас с людьми, обладающими знаниями в интересующей вас области. Ваш наставник должен быть в состоянии указать правильное направление, когда вам потребуется помощь. Идеально, если он может познакомить вас с нужными людьми, когда вы решите углубиться в конкретную тему.

Прежде чем предлагать кому-то стать вашим наставником, оцените связи этого человека с представителями отрасли. Однако имейте в виду, что искать наставников только среди ИБ-специалистов не надо. Важно, чтобы человек был способен помочь вам вырасти как профессионалу, как лидеру или как предпринимателю, а для этого разбираться в кибербезопасности необязательно.

Наконец, навыки хорошего наставника *дополняют ваш набор навыков*, то есть у него есть умения, которые вы хотите развить. Если вы стремитесь к лидерству, вам, вероятно, стоит найти того, кто достиг в этом больших успехов. Если желаете расширить знания и умения, связанные с цифровой криминалистикой, найдите того, кто долго работал в этой области. Все это очевидные вещи, однако начинающие профессионалы нередко ожидают от своего наставника того, что он просто не может им дать.

7.2.2. Чего ожидать от наставника

Вступая в наставнические отношения, вы должны четко понимать, чего от них ждете. Для начала убедитесь, что ваши ожидания реалистичны. Наставник — это человек, который направляет вас и дает советы, а не учит всему, что вам понадобится в определенной должности. Он должен быть способен указать вам на подходящие образовательные ресурсы и помочь составить план обучения, но не заниматься с вами ежедневно.

Вы вполне можете ожидать объективности и конструктивности. Наставник — это человек, который готов вас слушать и проявлять к вам сочувствие, если вы сталкиваетесь с проблемами. Вы также вправе требовать от него последовательности. Если наставник не соблюдает этические принципы и не следует сам тому, что проповедует, он не сможет надлежащим образом направлять вас в вашей карьере.

В конечном счете наставничество состоит из пяти ключевых элементов: предоставлении совета, помощи в планировании, мотивации, передаче опыта и поддержке (рис. 7.1). Наставник способен дать совет относительно ситуаций, с которыми вы сталкиваетесь, карьерных решений, которые вы рассматриваете, и новых идей, которые вы развиваете. Также ваш наставник должен помогать вам составлять план развития, то есть определять карьерные цели и намечать пути к ним. Еще одна важная функция любого наставника —мотивировать: пестовать вашу страсть и помогать поддерживать концентрацию в периоды упадка сил. Большое значение имеет и его опыт. Вам следует убедиться, что ваш наставник действительно разбирается в том, что вас интересует, будь то технические навыки в кибербезопасности, лидерские качества или просто профессиональная компетентность. Наконец, наставник — это тот, кто всегда готов вас поддержать. Это ваш сторонник, человек, который активно помогает вам создавать сеть деловых контактов и искать работу, а по возможности даже рекомендует вас на должность.

Рис. 7.1. Чего вы вправе ожидать от наставника

В августе 2021 года я опросила более 1500 опытных и начинающих специалистов по кибербезопасности, чтобы узнать их мнение относительно наставничества. В частности, им предложили оценить важность каждого из его пяти элементов по пятибалльной шкале. Сначала результаты казались довольно скучными, поскольку оценки были примерно одинаковыми, как показано на рис. 7.2.

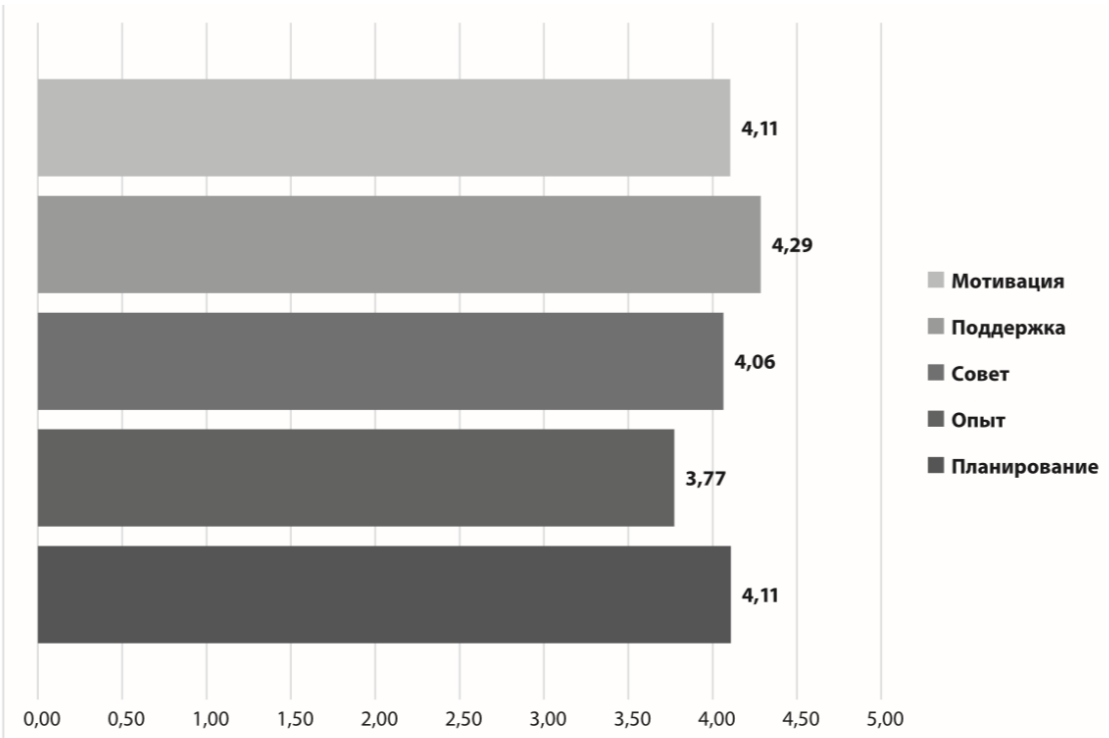

Рис. 7.2. Результаты опроса относительно важности элементов наставничества

Возможно, я могла бы улучшить результаты опроса, если бы предоставила более широкую шкалу, однако, как выяснилось, даже эти результаты содержат интересные данные. Несмотря на то что *средние баллы* каждого из пяти элементов были примерно равны, оценки, которые элементам присваивали *отдельные респонденты*, сильно различались и укладывались в максимальный диапазон от 1 до 5.

Что это значит для вас? Это значит, что наставничество — вещь индивидуальная. Все пять элементов должны присутствовать в отношениях с каждым наставником, однако их относительную ценность будете определять вы. Имейте это в виду.

7.2.3. Ожидания наставника

Важно не только понимать свои ожидания от наставника, но и четко представлять, чего он ожидает от вас. Как я уже говорила, наставничество — это двусторонний процесс, и оно должно приносить пользу и удовольствие обоим участникам. Информированность об ожиданиях вашего наставника будет гарантией продуктивных и мотивирующих отношений для вас обоих.

Для начала важно понять, почему люди вообще выбирают роль наставника. Что им это дает? При опросе я также уточнила у своих респондентов, выступали ли они когда-либо в качестве наставника. Тем, кто ответил положительно, затем был задан вопрос относительно их мотивации. Результаты опроса представлены на рис. 7.3.

Рис. 7.3. Ответы респондентов на вопрос о том, почему они стали наставниками

Как видите, подавляющее большинство наставников видели в таких отношениях возможность отдавать. Это важно осознать: в основном люди, играя роль наставника, стремились скорее помочь другим, а не извлечь выгоду для себя. Даже то, что это благодарная работа, не мотивировало так сильно, как желание способствовать чужому росту. Отсюда можно заключить, что наставники существуют для того, чтобы помогать вам расти. А значит, они ожидают, что вы в этом заинтересованы. Теперь давайте поговорим о том, как продемонстрировать эту заинтересованность.

Хороший наставник ожидает, что у вас есть хоть какой-то карьерный план. Вам необязательно тщательно его продумывать, однако для продуктивной работы с наставником очень важно иметь конкретные цели. Вооружившись результатами упражнений из главы 4, вы можете предоставить наставнику достаточно информации, чтобы он понял, чего вы надеетесь достичь, а затем подробно рассказал, как вам к этому прийти. Помните, работа наставника — указать вам путь, но цель вы выбираете сами.

Ваш наставник также ожидает от вас конкретных вопросов относительно ваших потребностей в развитии. Если на встрече вы спросите: «Можете ли вы научить меня хакингу?» — или заявите нечто вроде: «Я хочу знать о кибербезопасности все», — он не сможет дать вам какой-либо совет. Как уже говорилось, наставник — это не инструктор, готовый научить вас всему, что вам необходимо для работы. Его задача — посоветовать вам, как лучше действовать в определенной ситуации, и помочь развить навыки, указывая на нужные ресурсы или отвечая на конкретные вопросы.

Наконец — и это, пожалуй, самое важное, — наставник ожидает, что вы будете уважать его время. Помните: он, скорее всего, имеет работу. Кроме того, он может играть роль наставника и для других людей, а еще у него наверняка есть личная жизнь. Не требуйте к себе слишком много внимания. После того как наставник укажет вам направление, будьте готовы самостоятельно изучать интересующую вас тему. Предоставьте человеку достаточно времени, чтобы ответить на ваши сообщения. Как и у всех остальных, у него есть выходные, и он вряд ли захочет на отдыхе читать еще одно электронное письмо. Уважайте его личное пространство так же, как свое.

7.2.4. Сколько наставников должно быть у человека

Иметь несколько наставников вполне допустимо и часто даже необходимо. Однако сколько именно их должно быть, никто не скажет: единственно верного ответа на этот вопрос не существует. Наставнические отношения, как я уже говорила, часто возникают сами по себе. Если один наставник, подкованный технически, помогает вам развивать навыки для рутинной работы, а другой — навыки трудоустройства, то это совершенно нормально. В конечном счете вам нужно, чтобы в наставников превратились участники вашей сети контактов: чтобы они способствовали вашему росту, а их навыки дополняли ваши.

Однако наставников может быть слишком много. Наставничество — это ценный инструмент профессионального развития, но он лишь один

из многих. Встречаясь с разными наставниками несколько раз в неделю, можно легко угодить в ловушку. В какой-то момент вам следует спросить себя: сколько времени вы тратите на разговоры с наставниками, а сколько — на непосредственное развитие навыков?

Вы можете стать настолько зависимы от наставников, что перестанете совершенствоваться. Поэтому обращайте внимание на то, как развиваются эти отношения. Если вы больше не видите ценности в некоторых из них, возможно, пришло время сократить ваш круг наставников.

7.3. Регулирование взаимоотношений с наставником

Итак, вы нашли потенциального наставника. Вам комфортно с ним общаться, вы доверяете его советам и готовы следовать его руководству. Теперь пора признать, что у каждых наставнических отношений своя, уникальная формула успеха. У них нет единственно правильной структуры; формировать и развивать их должны вы оба.

7.3.1. Формы наставнических отношений

Наставники бывают разными. Как я уже говорила, вы можете иметь несколько наставников, помогающих вам с разными аспектами карьеры. Например, я регулярно работаю с человеком, который учит меня ориентироваться в теме корпоративного лидерства. Она руководит крупной торговой организацией и не обладает техническими знаниями в области кибербезопасности. Она направляет меня в движении по карьерной лестнице, но я не ожидаю от нее помощи в решении технических проблем. За этим я обращаюсь к другим наставникам, у которых внушительный багаж знаний в разных направлениях кибербезопасности. Возможно, при развитии наставнических отношений вы захотите следовать такой модели.

Некоторые наставники могут больше помогать вам даже не развивать рабочие навыки, а формировать сеть контактов. Когда я хочу связаться с кем-то из представителей отрасли, я первым делом обращаюсь к участникам своей сети, которых считаю наставниками. Они обладают обширными связями и, как правило, оказываются способны познакомить меня с тем, с кем я пытаюсь связаться. Итак, помните, что наставнические отношения не всегда сводятся к формальному карьерному коучингу: иногда все может быть гораздо проще.

7.3.2. Система наставнических отношений

Способ работы с наставником может меняться в зависимости от типа отношений, от того, как они сформировались, и от ваших целей. Иногда у наставничества есть четкая система: регулярные встречи, целеполагание, выполнение конкретных действий. Иногда вы просто получаете ответы на специфические вопросы. Главное — выбрать формат, который подходит обоим и благодаря которому отношения приятны и ценны и для вас, и для вашего наставника.

Регулярные встречи характерны для более формальных наставнических отношений. Такую структуру часто предпочитают те, кто нашел наставника через специальный сервис или через коллег. Встречи с наставником раз в неделю, раз в две недели или раз в месяц могут быть весьма полезны. Регулярность позволяет запланировать обсуждение конкретных тем и рассказывать о своем прогрессе, а кроме того, развивает ответственность, что позже пригодится вам в карьере.

Однако иногда наставничество носит ситуативный характер, особенно когда оно формируется спонтанно. Здесь наставником может быть человек, с которым вы взаимодействуете при необходимости. Например, звоните ему, чтобы обсудить конкретную ситуацию, или отправляете вопрос по электронной почте. Отношения, выстроенные по такому принципу, потенциально столь же ценны, как и более формальные периодические встречи, кроме того, так ваш наставник тратит меньше времени. Какой бы способ взаимодействия вы ни выбрали, важно обсудить его с наставником и согласовать правила.

Формат встреч тоже бывает разный (рис. 7.4). Лучшие наставнические отношения у меня складывались с теми людьми, которым я могла просто позвонить, чтобы пригласить на чашку кофе. Такие встречи позволяли нам наверстать упущенное, поговорить о проблемах, с которыми столкнулись, или о достигнутых успехах. Это отличный способ научиться видеть в своем наставнике прежде всего человека.

Ситуативный	Неформальный	Формальный
• Общение в основном с помощью электронной почты, телефона или текстовых сообщений • Отсутствие четкого графика взаимодействия • В основном краткие сессии вопросов и ответов • Фокус на предоставлении советов	• Встречи за чашкой кофе, обедом и так далее • Нерегулярное общение • Беседы в свободной форме • Фокус на мотивации и поддержке	• Спокойная профессиональная обстановка • Регулярные встречи • Заранее определенная повестка дня • Фокус на планировании и передаче опыта

Рис. 7.4. Различные форматы наставнических отношений

Однако вы также можете извлечь пользу из телеконференций: структурированных, с формальной повесткой и даже постановкой задач в конце встречи. Как я уже говорила, ваша цель — найти такую схему, которая устраивает и вас, и вашего наставника.

То, какой формат вы выберете, — ваше личное дело. Главное, чтобы он подходил вам обоим. К слову, в этот момент вы можете понять, станет ли тот или иной человек для вас хорошим наставником. Если вас интересуют формальные отношения, а потенциальный наставник не готов брать на себя соответствующие обязательства, вы, вероятно, решите поискать того, чья рабочая нагрузка не столь велика. При опросе, посвященном наставничеству, респондентов спросили, какой тип отношений они считают наиболее эффективным. Должна признаться, результаты меня слегка удивили (рис. 7.5).

Рис. 7.5. Результаты опроса, посвященного предпочтению типов наставнических отношений

Подавляющее большинство людей не стремятся к формальным наставническим отношениям. Это удивительно, поскольку многие дискуссии о наставничестве, которые я наблюдаю, посвящены как раз им. Так что, договариваясь о наставничестве, стоит рассматривать неформальный или даже ситуативный тип связи: он более гибкий и создает меньше напряжения. Признайтесь честно, что подходит вам лучше всего, и помните: если ваши ожидания не оправдались или ситуация изменилась, вы всегда можете пересмотреть договоренности.

И последнее, что следует сказать о формате наставнических отношений. В этой главе я подразумевала под наставничеством контакт один на один. Однако, проводя опрос, я узнала, что некоторым кажется

эффективным общение в группах, когда один наставник встречается с несколькими подопечными одновременно. Это свойственно учебным и другим подобным форматам, где общение с наставником — лишь часть общего процесса. Для кого-то присутствие других подопечных сделает обстановку менее пугающей. Кроме того, дополнительные точки зрения и опыт могут оказаться полезны, особенно если основное внимание уделяется расширению технических знаний и развитию соответствующих навыков. Таким образом, крайне важно объективно оценивать не только потенциального наставника, но и формат отношений с ним.

7.3.3. Прекращение отношений с наставником

Иногда вы понимаете, что наставнические отношения исчерпали себя и пришло время их завершить. Определить это не всегда бывает легко, кроме того, порой в этом трудно признаться самому себе. Вы долго работали с этим человеком, и он во многом вам помог. В итоге у вас может сформироваться чувство привязанности, что способно затруднить выход из отношений.

Важно регулярно проверять ценность взаимодействия с наставником. Не изнурительны ли для вас занятия? Не кажется ли вам, что в разговоре наставник ведет себя отстраненно или даже раздраженно? Способствует ли он развитию ваших навыков? Направляет ли он вас при продвижении по карьерной лестнице? Сохраняя объективность, вам нужно поймать момент, когда ответы на эти вопросы станут сигнализировать, что наставнические отношения просто подошли к концу. Как и любые другие отношения в вашей жизни, они не вечны. Вы можете остаться коллегами или даже друзьями, просто аспекта наставничества в вашем взаимодействии больше не будет.

Прекращение наставнических отношений не должно вызывать у вас страх или вину. Однако делать это, как и в случае с любыми другими отношениями, следует достойно и уважительно. Если вы общались с наставником скорее ситуативно, вероятно, будет достаточно просто не планировать очередную встречу. Настоящая проблема может возникнуть в случае, когда вы захотите выйти из более формальных отношений. Просто помните: говоря, что вы больше не получаете того, что получали раньше, вы не должны испытывать ни стыда, ни вины. Поблагодарите человека. Будьте вежливы, но честны. Даже если формально этот человек перестал считаться вашим наставником, он по-прежнему ценный участник вашей сети профессиональных контактов, и эту связь лучше не терять.

7.4. Построение деловых отношений

Теперь, когда вы поняли, какую роль в развитии карьеры играет мощная сеть деловых контактов и наставничество, пора приступать к работе. Создайте учетные записи в социальных сетях, если вы этого еще не сделали. Начните взаимодействовать с коллегами по отрасли и с теми людьми, чья работа кажется вам интересной или впечатляющей. Поищите местные сообщества ИБ-специалистов.

Присмотритесь к коллегам и поищите среди них тех, кому вы доверили бы роль наставника. Возможно, вам стоит поискать первого наставника на онлайн-ресурсах. Начинать этот поиск или формировать сеть профессиональных контактов никогда не бывает слишком рано.

ПОДВЕДЕНИЕ ИТОГОВ

- Социальные сети, отраслевые группы и местные мероприятия — отличные инструменты для создания сети профессиональных контактов.
- Сеть контактов следует целенаправленно наращивать и развивать.
- Рассматривая человека в качестве потенциального наставника, следует обращать внимание на такие ключевые характеристики, как честность, энтузиазм, наличие мощной сети контактов и навыков, дополняющих ваши.
- Наставнические отношения могут принимать разные формы, но они должны приносить пользу и удовольствие обеим сторонам.
- Прекращение наставнических отношений — необходимый шаг, если они исчерпали себя или не дали ожидаемых результатов, однако завершать их следует уважительно и изящно.

Глава 8
Угроза синдрома самозванца

В этой главе

- Что такое синдром самозванца, почему важно о нем знать и кто в группе риска
- Самоанализ для выявления причин синдрома самозванца
- Предотвращение или преодоление синдрома самозванца
- Объективное признание и празднование своих достижений

До сих пор основное внимание мы уделяли подготовке и поиску первой работы в сфере кибербезопасности. Теперь пришло время поговорить о препятствиях, возникающих уже после того, как вы ее получили. Согласно результатам различных исследований в области медицины, психологии и карьерного развития, примерно 70–85% людей сталкиваются с таким явлением, как *синдром самозванца*.

Как было сказано в главе 2, сфера кибербезопасности все еще страдает от культа рок-звезд ИБ. Учитывая, как много здесь крупных мероприятий, известных личностей и экспертных направлений, неудивительно, что синдром самозванца очень распространен. Хорошо, скажете вы, но что это такое и почему он должен меня волновать? Ответы на эти и другие вопросы вы найдете в этой главе.

8.1. Определение синдрома самозванца

В ИБ-сообществе, на конференциях и в социальных сетях ведется много дискуссий о людях, страдающих от синдрома самозванца и его негативных последствий. Это вполне реальная проблема, способная разрушить карьерные устремления многих представителей этой отрасли. Для успешной борьбы с ней нам необходимо осознать суть синдрома самозванца и важность, а также понять, кто в группе риска.

8.1.1. Что такое синдром самозванца?

Простыми словами *синдром самозванца* — это убежденность в том, что ваши достижения не такие ценные или впечатляющие, какими их считают другие. Это ощущение, что вы не так квалифицированны, как думают остальные. Это особое состояние сознания. Многие люди, страдающие синдромом самозванца, описывают его как страх быть разоблаченным и уличенным в мошенничестве. В профессиональном смысле они склонны преуменьшать важность или значимость своих достижений и уровень своей квалификации.

В сфере кибербезопасности синдром самозванца также может проявляться в виде сомнения в собственных знаниях. На рис. 8.1 показано, как мы обычно воспринимаем свою компетентность в сравнении с компетентностью других представителей отрасли.

Рис. 8.1. Графическое представление того, какой рисует картину собственных знаний в сравнении со знаниями других людей синдром самозванца

Многие специалисты по кибербезопасности считают, что они гораздо менее компетентны, чем другие представители отрасли. Иногда это происходит потому, что они склонны приписывать каждому человеку по отдельности наличие всей совокупности знаний, которыми делятся разные люди. И нам кажется, что наши знания — лишь подмножество этого более крупного множества.

Однако это не соответствует действительности. Гораздо более реалистичная картина представлена на рис. 8.2.

Рис. 8.2. Графическое представление того, как знания о кибербезопасности распределены среди представителей отрасли

На самом деле окружающие обладают собственным подмножеством знаний, но никто не знает и не может знать о кибербезопасности все. Это просто невозможно.

Кроме того, как видно на рис. 8.2, знания каждого отдельного человека пересекаются со знаниями других людей, включая ваши, но лишь частично. Между базами знаний разных людей существуют четкие различия, и каждый человек обладает их уникальным набором.

И хотя пересечение наборов знаний придает нашим способностям глубины, именно благодаря уникальности каждого из них появляется множество точек зрения, усиливающее отрасль в целом. Очень важно осмыслить эту концепцию, чтобы продуктивно бороться с синдромом самозванца.

8.1.2. Почему мы обращаем внимание на синдром самозванца?

Все это очень хорошо, но какое отношение эта информация имеет к карьерному успеху в сфере кибербезопасности? Синдром самозванца — мощный фактор, способный оказать пагубное влияние на ваш карьерный рост. У него далеко идущие и разнообразные последствия. Ущерб, который они наносят людям в плане как мотивации, так и психического здоровья, не стоит недооценивать.

Один из наиболее очевидных разрушительных эффектов заключается в том, что страх быть разоблаченным удерживает нас от риска. Когда человек недооценивает свои достижения или преуменьшает свою роль в них, это подрывает его уверенность в себе. Он может отказаться от шанса продвинуться по карьерной лестнице, считая, что его квалификации недостаточно и опасаясь разоблачения. Этот распространенный эффект был задокументирован в разных исследованиях этого явления. Важно признать, что так на вас влияет синдром самозванца, и начать бороться с ним, а не позволять ему сдерживать ваш рост.

Синдром самозванца может нанести ущерб и психическому здоровью. Представьте сценарий, схематично изображенный на рис. 8.1; убежденность, что все ваши коллеги обладают внушительным багажом знаний, которых вам недостает, способна породить огромную тревогу. Вообразите, насколько ошеломляющей выглядит задача получить все эти недостающие знания. Она монументальна и почти невыполнима; она грозит отбить у вас желание использовать будущие возможности и даже спровоцировать пренебрежение к своей текущей роли. В худшем случае вы вообще откажетесь строить карьеру в сфере кибербезопасности.

Также синдром самозванца способен вызвать ненависть к себе. Если человек считает себя в целом недостаточно квалифицированным, то видит в этом свой недостаток. Об этом часто рассказывают люди в ходе исследований и даже в неформальных обсуждениях в социальных сетях. Здесь вы рискуете попасть в порочный круг, где ваше чувство неполноценности заставляет вас принижать себя, что усугубляет чувство неполноценности.

Опять же, если с таким самовосприятием ничего не делать, из-за него вы можете отказаться от своих карьерных притязаний. Поэтому, если вы хотите добиться успеха в своих начинаниях, важно признавать влияние этого фактора и активно с ним бороться.

8.1.3. Кто подвержен синдрому самозванца?

Если вы просмотрите статьи и публикации на тему синдрома самозванца, то обнаружите, что это явление встречается практически

повсеместно. В той или иной степени с ним сталкиваются почти все опрошенные, вне зависимости от уровня должности, объема знаний или публичного имиджа. Как уже было сказано, согласно результатам многих исследований, от 70 до 85% профессионалов сообщают, что испытывают подобные чувства.

Потому-то очень важно признать тот факт, что синдром самозванца может затронуть любого. Неважно, начинающий вы специалист или уже зарекомендовали себя как профессионал, сомнения в себе и ощущение собственной неполноценности может стать для вас проблемой. Как ни странно, судя по дискуссиям в ИБ-сообществе, от синдрома самозванца страдают даже признанные лидеры. Мне самой пришлось бороться с ним на протяжении почти двух десятилетий работы в отрасли.

Позвольте мне еще немного поделиться опытом. Я начала работать в сфере кибербезопасности в 2006 году в качестве пентестера. Я никогда не рассматривала хакерство как карьеру и вдруг вошла в группу тестировщиков безопасности одной крупной финансовой компании. Спустя год я возглавила эту группу. К 2010 году, отчасти благодаря поглощению, я уже руководила не только этой командой, но и всей программой управления уязвимостями в этой финансовой организации, в которой работало 35 000 человек и которая на тот момент входила в топ-200 списка 500 крупнейших компаний по версии журнала Fortune. В свои тридцать с небольшим я уже играла заметную роль в управлении операционной безопасностью в этой глобальной организации.

Это кажется впечатляющим карьерным достижением, не так ли? Однако на протяжении многих лет после ухода из той компании я отказывалась воспринимать его или говорить о нем в таком ключе. Наоборот, я приуменьшала его значение.

Я списала достижение, которым имела полное право гордиться, на слепую удачу. Даже в своем резюме я приуменьшала круг своих обязанностей в той должности. Я редко говорила о том, что регулярно отчитывалась о состоянии безопасности компании перед ее руководством. Я не описывала, как работала с руководителями, чтобы обеспечить финансирование дополнительных инициатив в области безопасности и решить проблемы ограниченного бюджета. Я даже стеснялась рассказывать, в какой степени взаимодействовала с разными подразделениями, чтобы убедиться, что выявленные уязвимости устранены.

Я приуменьшала свои достижения, вспоминая о той помощи, какую получила от своих бывших менеджеров, включая того, кто привел меня в сферу кибербезопасности. Я рассматривала поглощение компании, благодаря которому получила повышение, как счастливую случайность, умаляя при этом ценность всего того, что делала в этой должности.

Успех каждого человека обусловлен особым сочетанием его навыков, риска, на который он идет, помощи, получаемой от других, и в большинстве случаев некоторого влияния удачных обстоятельств. Однако ценность достижений не измеряется этими факторами, поскольку успех зависит от того, как мы реагируем на открывающиеся возможности.

Мне потребовалось много времени, чтобы это осознать, из-за чего в начале карьеры я не пользовалась шансом продвинуться дальше. Понимание, что через это проходят многие, поможет вам лучше справиться с сомнениями в себе. Подробнее об этом мы поговорим далее в главе.

8.2. Почему возникает синдром самозванца

Многие академические исследования и статьи в СМИ рассказывают о синдроме самозванца, о его причинах и о том, кто ему подвержен. Я не буду повторять их выводы, а вместо этого расскажу о тех причинах, о которых узнала из собственного опыта и обсуждений с другими людьми. Если вы хотите углубиться в формальные академические исследования, вы сможете легко найти их в интернете, здесь же мы рассмотрим тему в контексте кибербезопасности.

8.2.1. Перфекционизм

Одна из наиболее распространенных причин синдрома самозванца — чрезмерные или даже нереалистичные ожидания от самого себя. Некоторые мои коллеги сказали, что они не привыкли делать что-то наполовину. Мне тоже это не свойственно. Когда я берусь за новую задачу, я делаю все, чтобы показать должный уровень знаний и компетентности.

Например, много лет назад, когда я увлеклась фотографией, я не просто купила камеру и отправилась делать снимки. Сначала я несколько недель изучала технические аспекты работы фотоаппаратов. Я узнала о взаимосвязи между выдержкой, диафрагмой и светочувствительностью. Я поучаствовала в нескольких форумах, посвященных фотографии, и освоила профессиональный сленг, что помогло мне разобраться с такими концепциями, как f-число и компенсация экспозиции. Однако техническими деталями дело не ограничилось. Я изучила и художественные аспекты фотографии, в том числе то, как освещение, композиция, цветовой баланс и кадрирование могут повлиять на настроение снимка. Наконец, я исследовала характеристики множества камер, чтобы выбрать ту, что позволит реализовать мои творческие замыслы.

Занявшись новым хобби, я установила для себя высокую планку — и как раз такую склонность ожидать от себя слишком многого описывали люди с синдромом самозванца. Нередко мы ожидаем от себя того, на что просто не способны. Мы ставим перед собой чрезмерно высокие цели и, когда нам не удается их достичь, позволяем неудаче убедить нас в том, что это дело нам не по силам. Вместо того чтобы оставить место для роста и обучения, мы становимся несправедливы и чрезмерно требовательны к себе. Такой перфекционизм — основная причина формирования синдрома самозванца.

8.2.2. Отраслевые ожидания

Формированию синдрома самозванца могут способствовать не только наши собственные ожидания. Примерно так же на нас нередко влияет сама сфера кибербезопасности. Как уже было сказано в главе 3, от практиков в этой области с самого начала ожидают умений высокого уровня. Специалисты по кибербезопасности ощущают большое давление, поскольку чувствуют, что они должны обеспечить стопроцентную защиту вверенных им систем. Учитывая, насколько важно обеспечить безопасность нашего цифрового образа жизни, отдельным специалистам или организациям отрасль редко прощает их несовершенство.

К сожалению, это обрекает нас на неудачу. В мире технологий ошибки неизбежны. Странная дихотомия заключается в том, что специалисты по кибербезопасности признают эти цели нереалистичными, но все равно пытаются их достичь. Мы часто слышим, что злоумышленники обязательно найдут уязвимости в наших системах и воспользуются ими. В наших силах в лучшем случае быстро и успешно выявлять атаки и утечки и реагировать на них, однако не стоит думать, что то, что мы создали, в принципе невозможно взломать. Проблема в том, что в сфере кибербезопасности успех измеряют через показатели, которые нельзя назвать ни разумными, ни достижимыми.

В результате, когда инцидент действительно случается, ИБ-специалисты склонны принимать все на свой счет. Нередко профессионалы рассматривают взлом как признак собственной неудачливости или некомпетентности, вместо того чтобы признать: технологии никогда не перестают развиваться, что усложняет задачу обеспечивать ее защиту. Это может подорвать уверенность в себе и вызвать ощущение безнадежности и тревоги, влияющее на способность выполнять повседневные обязанности еще более негативно.

Для успешного карьерного роста и сохранения психического здоровья очень важно научиться иначе относиться к таким проблемам.

Специалисты по кибербезопасности должны воспринимать их не как признак отсутствия квалификации или некомпетентности, а скорее как опыт, который можно использовать для обучения и развития. Понимание, что мы растем благодаря неудачам, признак истинной профессиональной зрелости. Если бы мы всегда справлялись с поставленными задачами, то никогда бы не сталкивались с проблемами и, следовательно, никогда не добивались бы успеха, который можно было бы отпраздновать.

8.2.3. Сравнение себя с другими

Как было показано на рис. 8.1 и 8.2, синдром самозванца в большой степени вырастает из сравнения себя с другими. Когда вы только входите в отрасль, вы можете установить контакт с другими профессионалами, которые начинают карьеру в области кибербезопасности примерно одновременно с вами. Эти отношения очень важны и могут сослужить вам хорошую службу в процессе вашего роста и профессионального развития. Однако также они могут создавать проблемы и вызывать ощущение собственной неполноценности. Наблюдая за достижениями коллег, вы рискуете сосредоточиться на их успехах и решить, что их карьера развивается быстрее вашей.

Подобное сравнение изначально ошибочно. В реальности ваши коллеги, как правило, действительно добиваются успехов, которыми не можете похвастаться вы, однако, скорее всего, и вы достигаете чего-то, чего не достигли они. В такой ситуации вы оказываетесь неспособны осознать собственную ценность и вместо этого зацикливаетесь на том, чего еще не добились. Вполне вероятно, что чужие достижения даже не соответствуют вашим целям. Тем не менее, наблюдая за ними, вы все равно можете почувствовать себя менее успешным.

Проблема сравнения также связана с культом рок-звезд информационной безопасности. Вы наверняка уже знаете имена нескольких известных и опытных представителей ИБ-сообщества. Вы можете восхищаться их достижениями и навыками. Возможно, им удалось быстро достичь тех карьерных высот, на которые нацелились вы сами. Это хорошо и полезно, если мотивирует вас расти и достигать значительных результатов. Однако если чужие достижения давят на вас и вызывают непреодолимую тревогу, это становится проблемой.

Вы можете смотреть на все, что они сделали, и чувствовать безнадежность. Вам может казаться, что вы никогда не достигнете такого же уровня мастерства или успеха или что вы в чем-то отстаете от этих людей. Но верить в это не стоит. Помните, что люди обычно выставляют напоказ свое лучшее «я». Большинство демонстрируют только эту свою часть.

Скорее всего, вы не увидите трудностей и неудач, с которыми они столкнулись и продолжают сталкиваться на своем пути. Вы сильно удивитесь, узнав, что некоторые из них тоже недовольны своими достижениями.

Поэтому очень важно признать, что каждый из нас идет собственным путем и что адекватно сравнить успехи разных людей нельзя. За карьерные достижения человек может расплачиваться неудачами в других сферах жизни. Иногда профессионал достигает вершины благодаря привилегиям или преимуществам, недоступным другим, вынужденным из-за этого преодолевать дополнительные трудности. Вот почему меры успеха должны быть сугубо индивидуальными. Определяя вехи собственного пути, необходимо учитывать множество личных аспектов, влияющих на ваши карьерные и профессиональные успехи.

8.2.4. Недостаточная представленность

В главе 1 мы говорили о важности разнообразия в сообществе кибербезопасности, которого здесь явно не хватает. Женщины, этнические меньшинства и другие демографические группы представлены в ней недостаточно. Это сильно усложняет поиск примеров для подражания, то есть людей, которые достигли такого успеха, к какому стремимся мы, и с которыми мы бы себя идентифицировали.

Например, темнокожему человеку, стремящемуся занять высокую руководящую должность, может быть сложно найти темнокожего руководителя, способного стать для него наставником или источником вдохновения. Согласно результатам «Глобального исследования рабочей силы в области информационной безопасности», проведенного организацией (ISC)² совместно с компанией Frost & Sullivan и другими (**http://mng.bz/06wm**), только 9% специалистов по кибербезопасности были афроамериканцами или темнокожими людьми. Среди них лишь 23% занимали руководящие должности. Логика подсказывает, что среди руководителей высшего звена представителей этой группы еще меньше.

Мы можем верить, что этническая принадлежность, раса, пол и сексуальная ориентация людей не имеют значения при выборе образцов для подражания. Однако более прагматичный анализ ситуации говорит о том, что, если члены этих групп не видят своих представителей в интересующей их сфере, это способно вызвать у них ощущение непричастности к ней. Это ощущение усугубляет и без того тяжелые чувства, порождаемые синдромом самозванца; кроме того, у человека может сложиться впечатление, что он не на своем месте, хотя в противном случае он не испытывал бы таких сомнений. Чтобы обеспечить разнообразие в ИБ-сообществе, нам еще предстоит проделать большую работу, и учитывая

это, очень важно, чтобы вы, особенно если вы относитесь к недостаточно представленной группе, осознать внутри себя, что вам не только можно, но и нужно при необходимости прокладывать новые пути.

8.2.5. Обесценивание своих достижений

Я уже рассказывала о личном опыте обесценивания собственных достижений. Из-за того, что я получала помощь от других людей и использовала множество открывающихся передо мной возможностей, я преуменьшала ценность своих карьерных успехов. Как оказалось, такой образ мышления распространен среди целеустремленных людей, особенно в сфере кибербезопасности. Создается ошибочное впечатление, будто те, кто продемонстрировал наивысший уровень достижений, попали на вершину сами, без всякой помощи. Однако в реальности все обстоит с точностью до наоборот.

Люди крайне редко достигают больших успехов, работая и преодолевая трудности в одиночку. Спортсмены взаимодействуют с тренерами, инструкторами, диетологами и другими специалистами. Это позволяет им достичь оптимальной спортивной формы. Они учатся у других и открывают для себя новые возможности через тех, с кем работают. Еще один пример — музыканты: они проводят бесчисленные часы играя с другими музыкантами и учась у них. Благодаря им они осваивают теорию музыки или обретают вдохновение. Чтобы один человек написал для песни слова, сочинил музыку и выпустил трек, — такое происходит очень редко.

Кроме того, ни спортсмены, ни музыканты, ни другие успешные и узнаваемые личности обычно не достигают высот без некоторой доли везения. Для учащегося в колледже бейсболиста это может быть присутствие профессионального скаута на важнейшей игре сезона. А для музыкальной группы — присутствие руководителя звукозаписывающей компании в клубе в вечер ее выступления.

То же самое относится и к вашей карьере в сфере кибербезопасности. У вас появятся наставники, коллеги и другие люди, благодаря которым ваша база знаний будет расти, а ваши навыки — развиваться; перед вами могут открыться новые двери. Несомненно, те самые удачные обстоятельства, что позволят вам принять новый вызов или сыграть новую роль, не обойдут вас стороной. В конце концов вы обнаружите, что успех приходит тогда, когда вы используете эти внешние факторы и возникающие возможности в своих интересах. Именно умение идти на риск и преследовать очередную, еще более амбициозную цель часто отличает быстрый карьерный рост от медленного.

Поэтому неправильно думать, что стороннее влияние на вас или кого-то другого делает ваши или чужие достижения менее ценными или впечатляющими. Чтобы развивать свою карьеру, вам следует рассматривать эти события более объективно и с готовностью отдавать себе должное за то, как вы использовали представившиеся возможности для роста и продвижения вперед. Ведь именно поэтому ваши успехи стоят того, чтобы ими гордиться.

8.3. Преодоление синдрома самозванца

Теперь, когда вы в курсе, что такое синдром самозванца и насколько пагубно он может повлиять на вашу карьеру, пора обсудить способы, как уменьшить это влияние или даже вовсе его избежать. Поскольку вы понимаете, что ему подвержены все люди, вы знаете, что этого чувства не нужно стыдиться.

Не все переживают синдром самозванца одинаково, потому и способы избежать его или преодолеть будут для каждого уникальны. Единственно правильного метода не существует. Более того, методы, которые кажутся эффективными сегодня, могут со временем измениться.

Неизменной останется лишь потребность активно бороться с синдромом самозванца. Для этого необходимо признать, что он существует и способен на вас влиять. Поняв, как увидеть себя, свой путь, свою борьбу и свои достижения в другом свете, вы обретете необходимое оружие, чтобы победить этого врага. Итак, давайте рассмотрим, какие тактики вам могут пригодиться в случае, если синдром самозванца попробует помешать вам добиться желаемого успеха.

8.3.1. Избегайте конкуренции

Как уже было сказано, во многих случаях синдром самозванца и связанные с ним проблемы появляются из-за непомерно высоких ожиданий от себя и сравнения себя с другими людьми. Помимо всего прочего, он может порождать конкуренцию. Мы хотим достичь цели быстрее остальных. Мы хотим получить больше полномочий, чем есть у коллеги. Хотим знать о той или иной теме больше, чем другие. Этот список можно продолжать бесконечно.

К сожалению, ИБ-сообщество нередко стимулирует проявление этой естественной склонности. Мы регулярно организуем такие мероприятия, как CTF-соревнования, где участники или команды соревнуются во взломе систем. Предполагается, что самые способные решат задачу

быстрее остальных и выиграют приз. Эти соревнования нельзя назвать плохими или нездоровыми, но если использовать их, чтобы измерять уровень собственных навыков, а не чтобы учиться и расти в интересной соревновательной среде, они могут оказаться токсичными. Если вы решите участвовать в таких мероприятиях, постарайтесь увидеть в них самую суть. Как и спорт, они могут породить чрезмерную конкуренцию среди участников. Старайтесь получать от них удовольствие и поймите, что поражение — ваше или вашей команды — не делает вас менее ценной частью сообщества.

Конкуренция в сфере кибербезопасности также может проявляться в обнаружении уязвимостей. Открытие новых дыр в безопасности, которые мы называем *уязвимостями нулевого дня*, часто выступает мерилом профессионализма. Такие уязвимости обычно публикуются в базе данных CVE, поэтому некоторые склонны судить о навыках хакера или исследователя по количеству уязвимостей, о которых он сообщил.

Это опасно по многим причинам. Во-первых, выявление уязвимости нулевого дня имеет значение, но не большее, чем обнаружение в системе или приложении общеизвестных уязвимостей. Есть мнение, что второе более ценно с точки зрения безопасности технологий. Во-вторых, многие хакеры и исследователи (включая меня) работают в организациях, тестируют и защищают их системы. Бреши, обнаруженные в них, могут относиться к уязвимостям нулевого дня, но, поскольку выявляются в программном обеспечении самой организации (а не в коммерческом ПО), не включаются в базу данных CVE.

Суть в том, что у вас наверняка возникнет соблазн конкурировать с коллегами во многих аспектах и сравнивать себя с ними. Однако к этой конкуренции следует относиться с осторожностью. Ее стоит использовать в качестве развлечения или мотивации для собственного роста и развития карьеры. Когда же конкуренция из источника удовольствия превращается в мерило собственной ценности, она начинает влиять на вас разрушительно. Будьте осторожны и помните: тот факт, что вы не выиграли какой-то приз, не получили какую-то награду или не увидели где-то свое имя, вовсе не означает, что вы не вносите свой вклад в развитие сферы.

8.3.2. Ставьте цели и вырабатывайте собственное определение успеха

С темой конкуренции и сравнения тесно связана идея измерения собственного успеха. Победа в CTF-соревновании и обнаружение уязвимости становятся мерилом успеха для некоторых людей потому, что эти

достижения легко продемонстрировать другим. На самом деле, определяя собственный успех степенью получаемого признания, вы можете угодить во множество карьерных ловушек, в том числе связанных с синдромом самозванца. Такой способ оценки успеха токсичен. Поскольку путь каждого уникален, у человека должно быть собственное мерило успеха. Оценка своих достижений через их восприятие другими людьми, а не через то, что значимо для вас лично, заставляет гнаться за постоянно меняющимися и принципиально недостижимыми целями.

Если ваши мотивы для достижений основаны на стремлении возвыситься в чужих глазах, то такая цель незначительна и даже опасна. Помните, что всем не угодишь. Каким бы впечатляющим ни был ваш успех, всегда найдутся те, кто станет критиковать вас и сомневаться в вас. К сожалению, это неотъемлемая часть человеческой натуры, которая проявляется и в ИБ-сообществе.

Кроме того, поскольку наша сфера развивается динамично, нет никаких гарантий, что цель, кажущаяся другим впечатляющей сегодня, будет считаться такой же после реализации. Стремление к успеху ради известности, признания, славы или чего-то еще оставляет вам слишком мало места для маневра. При этом все, кроме принадлежности к небольшому проценту успешных людей, кажется неудачей. Это нездоровая точка зрения.

Вместо этого следует ставить цели, важные именно для вас. Какое значение вы им придаете? Почему хотите достичь именно этого? Вы стремитесь стать руководителем высшего звена? Почему? Если вы просто хотите, чтобы другие уважали вас как лучшего эксперта, то, когда вы станете директором по информационной безопасности, вас может настигнуть разочарование. Почитайте публикации в соцсетях или новости и обратите внимание, как часто к таким руководителям относятся с пренебрежением. Не стоит стремиться к этой цели, чтобы кого-то впечатлить. С другой стороны, если вы хотите занять эту должность, потому что готовы нести ответственность за защиту организации от киберугроз или чувствуете, что способны разрабатывать стратегии и взаимодействовать с другими руководителями, тогда эта цель может быть вполне подходящей для вас.

Однако, как вы увидите в главе 9, постановка целей не должна ограничиваться определением пункта назначения. Также необходимо научиться ставить краткосрочные цели, служащие вехами на пути. Если для достижения вашей главной цели требуется 7, 10 или более лет, то вы очень легко можете начать обесценивать то, что уже сделали. Чуть позже мы поговорим о том, как ставить достижимые цели, которые позволят поддерживать мотивацию по мере продвижения вперед.

8.3.3. Обращайтесь к коллегам

Нет, не нужно ставить цели, основываясь на том, что другие думают о вас, или на том, насколько впечатляющими они считают ваши достижения. Однако это не означает, что коллеги не способны поддержать вас в борьбе с синдромом самозванца.

Один из его неприятных симптомов — то, что профессионалы, как правило, с трудом принимают комплименты. Подумайте об этом. Как вы реагируете, когда другой человек говорит вам, какую отличную работу вы проделали или как он впечатлен вашим достижением? Вы благодарите его и радуетесь, что кто-то разделил с вами радость от вашего успеха? Или считаете это лестью и начинаете отрицать ценность своего достижения?

Нас с детства учат не хвастаться. Однако иногда мы можем зайти слишком далеко и проявлять из-за этой привычки чрезмерную скромность, когда дело доходит до признания собственной ценности. Из-за страха прослыть тщеславным человеком или хвастуном он преуменьшает значение комплиментов. Кроме того, людям обычно гораздо проще поверить, что тот, кто делает комплимент, просто предвзят или старается «быть милым», вместо того чтобы признать искренность его чувства. Столкнувшись с проявлением синдрома самозванца, вы можете перевернуть сценарий с ног на голову и использовать его для подтверждения собственной значимости.

В следующий раз, когда вы почувствуете себя самозванцем, поделитесь этим ощущением с человеком, которого уважаете. Вероятно, вы обнаружите, что он чувствует то же самое. Вас может даже шокировать, что многие люди больше всего недовольны как раз тем, что вас в них восхищает. Не уклоняйтесь от таких разговоров. Вполне вероятно, что другие тоже больше всего восхищаются теми аспектами вашего карьерного пути, которые вызывают у вас наибольшие опасения. Будьте открыты и готовы признать, что они говорят искренне. Тот факт, что разговор на эту тему инициировали вы, не означает, что ваши собеседники предвзяты.

Ваши наставники также могут сыграть здесь важную роль. Учитывая, что они, скорее всего, тоже испытывали подобные чувства, они способны поделиться с вами приемами, которые помогли им самим. Благодаря этому вы сумеете найти подходящие для себя решения и применять их в своем карьерном путешествии. Это еще раз подчеркивает важность взаимодействия с наставником, о чем подробно говорилось в главе 7. Поставьте эти отношения себе на службу, и они помогут вам убедиться, что вы не мошенник, что вы достаточно квалифицированны и вполне достойны той похвалы, которую получаете.

8.3.4. Приносите пользу другим людям

Я прекрасно понимаю, что ваша карьера только начинается. Вероятно, вы не чувствуете, что можете помогать другим в их карьерном продвижении. Но это неправда. Даже делая первые шаги, вы уже можете служить источником вдохновения для других людей, которые только присматриваются к работе в этой области. Продолжая делиться опытом в процессе развития карьеры, вы будете помогать людям расти и двигаться вперед вместе с вами.

Замечательный побочный эффект этих действий заключается в том, что благодаря им вы справитесь с синдромом самозванца: помощь другим позволяет сразу несколькими способами получить подтверждение собственной значимости. Для начала подумайте о разговорах с теми, кого вы вдохновляете. В ваших достижениях есть нечто такое, что люди могут перенести на себя. Поделившись опытом и увидев реакцию собеседника, вы поймете, что этапы вашего пути, казавшиеся вам незначительными, на самом деле весьма ценны. Это послужит подтверждением вашего успеха и поможет справиться с чувством, будто вы еще ничего не добились, обусловленное тем, что вы пока не достигли своей конечной цели. Кроме того, когда вы разговариваете с человеком, которого вдохновляете, вам легче поверить в его искренность. Слушайте, что вам говорят, делитесь знаниями, и вы поймете, как далеко уже продвинулись.

Принося пользу другим, вы также можете продемонстрировать свои знания в различных технических аспектах кибербезопасности. Вы внезапно обнаружите, что навыки и приемы, которые вы воспринимали как должное, способны кому-то принести пользу. Делясь знаниями с другими людьми, вы начнете понимать, как сильно выросли. Это может служить напоминанием о том, с чего вы начинали свой путь, а также показателем вашего развития в навыках и знаниях. Пусть опыт обучения других членов сообщества станет дополнительным средством самопознания.

Наконец, когда вы помогаете другим расти вне зависимости от того, на каком этапе находитесь сами, вы приближаетесь к собственным целям. Если вы стремитесь занять руководящую должность, то этот опыт вооружит вас действенными лидерскими навыками. Если вы больше хотите развить техническую смекалку, представьте, какую пользу можете извлечь из собственного исследования, которое проведете, чтобы помочь решить чью-то проблему.

В этом и заключается смысл поговорки о том, что прилив поднимает все лодки. Чем больше вы будете способствовать росту других людей, тем больше будете расти сами. Благодаря этому вы быстрее достигнете своих целей, что, в свою очередь, поможет вам избавиться от синдрома самозванца.

8.3.5. Признавайте и празднуйте свои достижения

Один из самых сложных аспектов борьбы с синдромом самозванца — научиться объективно воспринимать свои прошлые достижения. Как я уже говорила, мне оказалось трудно признать масштаб того, чего я достигла на ранних этапах карьеры. Мне было 19 лет, и я еще даже не окончила колледж, когда устроилась программистом на свою первую работу. Многим это может показаться впечатляющим, однако я считала, что мне просто повезло, потому что все это произошло в эпоху доткомов, когда программисты пользовались большим спросом.

Мы уже обсудили, почему трудно признать собственные успехи и понять, что получение помощи и везение — не просто нормальные, а необходимые условия для успеха в любой области. По мере продвижения вперед важно признавать свои достижения, праздновать их и позволять себе гордиться ими.

Возможно, вы задаетесь вопросом: что значит признавать достижения? Позвольте мне поделиться с вами простым упражнением, которое поможет вам осознать ценность того, что вы сделали. То, что ваша карьера в кибербезопасности еще не началась, не проблема. Мы рассмотрим тот опыт, что уже у вас есть. Вы можете вспомнить свои академические достижения, работу в других областях или даже в хобби. Чтобы выполнить это упражнение, подойдет любое из этих направлений. Выберите одно или даже два, возьмите лист бумаги, и давайте начнем.

1. Вспомните о своем опыте. Как вы научились делать эти вещи? Перечислите все образовательные шаги, которые вы предприняли, всех людей, которые помогали вам учиться или делились с вами знаниями, а также все счастливые случайности, с которыми вы столкнулись на этом пути.

2. Отдельно перечислите наиболее приятные аспекты этого опыта. Например, какие-то особенности работы, которые вам нравились (даже если работу в целом вы ненавидели), или достигнутый успех, веху на пути к нему, или даже просто определенный уровень удовлетворения.

3. Посмотрите на эти два списка и установите связи между ними. Опишите, как предпринятые вами образовательные шаги, помогавшие вам люди и счастливые случайности повлияли на приятные аспекты вашего опыта.

4. Опишите, как вы использовали внешние факторы, чтобы в вашем опыте появились эти приятные аспекты. Сосредоточьтесь на своих действиях. Как именно вы воспользовались полученной информацией или возможностью, чтобы получить внутреннее удовлетворение?

5. Переформулируйте описания своих действий так, как если бы собирались включить их в резюме. Неважно, связаны они с работой или нет. Подумайте, как вы рассказали бы о них другим, если бы хотели их впечатлить. Не преувеличивайте и не лгите; просто расскажите историю так, чтобы другие оценили ваши достижения.

6. Взгляните на то, что вы написали, со стороны. На мгновение постарайтесь забыть, что речь идет о вас, и представьте, что бы вы почувствовали, прочитав все это в чужом резюме или биографии. А затем напомните себе, что все это сделали вы. В этом описании нет ни лжи, ни преувеличений — только достижения, которыми вы можете гордиться.

Сохраните эти описания. Они послужат хорошим напоминанием об этом упражнении, которое вы можете выполнять снова, продвигаясь по карьерной лестнице. Используйте его, чтобы более объективно оценивать свои карьерные достижения в сфере кибербезопасности. Это поможет вам справиться с монстром под названием «синдром самозванца», который постоянно пытается доказать вам, что вы не на своем месте или недостаточно компетентны.

ПОДВЕДЕНИЕ ИТОГОВ

— Синдром самозванца связан с тем, что человек недооценивает собственные достижения и ощущает, будто находится не на своем месте.
— Синдром самозванца иногда мешает продвигаться по карьерной лестнице, и с ним может столкнуться любой человек на любом этапе своего пути.
— Синдром самозванца могут вызывать перфекционизм, завышенные ожидания, сравнение себя с другими, отсутствие примеров для подражания, с которыми человек себя идентифицировал бы, и обесценивание собственных достижений.
— Вы способны справиться с синдромом самозванца, если будете избегать соперничества, ставить перед собой важные лично для вас цели, получать поддержку от коллег, а также объективно признавать и отмечать свои достижения.

Глава 9
Достижение успеха

В этой главе

- Распознавание и преодоление трудностей на пути к карьерному успеху
- Постановка долгосрочных целей и разработка стратегии для их достижения
- Смена направления в сфере кибербезопасности
- Применение знаний на практике

В главе 8 мы перешли от обсуждения поиска первой работы в сфере кибербезопасности к разговору о долгосрочном карьерном успехе. Мы сосредоточились на синдроме самозванца — одной из ключевых проблем, с которой специалисты по кибербезопасности могут столкнуться на любом этапе карьеры. Однако это лишь одна из угроз для вашего карьерного успеха. А поскольку я хочу, чтобы это руководство помогало вам на протяжении всего пути, очень важно подробно обсудить остальные проблемы и то, как с ними справляться.

Запуск карьеры, будь то поиск первой работы сразу после окончания учебы или смена направления, предприятие рискованное. При правильной стратегии вы будете понимать, к чему стремиться и что для этого предпринимать, а также видеть прогресс и фокусироваться на главном. Стратегия, сформулированная в начале пути, несомненно, будет

меняться со временем. В главе 2 мы рассмотрели, какие есть направления в сфере кибербезопасности. Вполне вероятно, что в процессе работы вы хотя бы раз смените специальность. Тем не менее план, составленный в самом начале, будет долгие годы служить вам ориентиром.

Если вас привлекает динамичность и изменчивость карьерного пути, то сфера кибербезопасности — особенно хороший вариант для вас. Здесь много различных, но связанных между собой дисциплин, а потому сменить направление относительно легко. Впрочем, решиться на это может быть непросто.

В этой главе мы подробно поговорим о смене направления, чтобы вооружить вас требуемыми для этого инструментами. Итак, вы почти дочитали руководство. Пришло время применить знания на практике.

9.1. Преодоление карьерных трудностей в сфере кибербезопасности

В главе 8 мы подробно обсудили синдром самозванца — распространенную проблему, с которой, вероятно, придется столкнуться и вам на разных этапах профессионального пути. Однако это не единственная трудность, способная разрушить ваши надежды на длительную и успешную карьеру.

Чтобы реализовать такой долгосрочный план, необходимо научиться предвидеть потенциальные проблемы и разбираться в них. Хотя обсуждаемые далее трудности не уникальны для сферы кибербезопасности, они проявляются особенным образом. Эти проблемы часто обсуждаются в отраслевых СМИ, на различных конференциях и, конечно же, в социальных сетях. Хорошая новость заключается в том, что с ростом осведомленности о них начали появляться и стратегии борьбы с ними.

9.1.1. Эмоциональное выгорание

Если вы спросите любого карьерного консультанта или специалиста по подбору кадров, какие проблемы беспокоят его больше всего, то одним из первых пунктов списка наверняка будет *эмоциональное выгорание* — состояние истощения и разочарования в своей работе, как правило, вызванное длительным эмоциональным и/или физическим стрессом. Человек в этом состоянии обычно чувствует себя эмоционально истощенным и перегруженным трудовыми обязанностями, а также ощущает повышенную тревожность. Выгорание — не уникальное для сферы кибербезопасности явление. Оно встречается во всех отраслях, и это ключевой бизнес-риск для любого работодателя.

Однако в последние годы в кругах специалистов по кибербезопасности выгорание обсуждается все чаще. В главе 1 мы говорили о том, что многие организации жалуются на недостаточную квалификацию сотрудников. Затем в главе 3 была приведена статистика, демонстрирующая, что нехватка навыков во многом обусловлена практиками найма. При подборе персонала организации так или иначе испытывают сложности, а к уже нанятым специалистам предъявляются огромные требования. Из-за растущих требований, в свою очередь, профессионалы испытывают больше стресса.

Однако сложность с поиском квалифицированных специалистов — не единственный фактор, который оказывает давление на уже нанятых сотрудников. Для многих организаций кибербезопасность — не основной вид деятельности. Из-за этого работа служб по кибербезопасности рассматривается как статья расходов или центр издержек, то есть как источник необходимых затрат на ведение бизнеса, который сам по себе не приносит дохода. Таким образом, когда руководство решает повысить прибыльность за счет сокращения или устранения расходов, отдел кибербезопасности часто попадает в число подразделений, испытывающих наибольшее напряжение. Хотя осведомленность о важности кибербезопасности в целом растет, бюджеты, выделяемые на работу соответствующих служб и на средства защиты, увеличиваются довольно медленно. В результате рост способностей персонала не поспевает за ростом бизнеса в целом. Это создает дополнительное давление, но и здесь проблемы не заканчиваются.

Бизнес по большей части растет за счет внедрения новых технологий и инноваций. Роль кибербезопасности в контексте быстро развивающихся технологий обсуждалась в главе 1. Когда появляется новая технология, перед специалистами по кибербезопасности встает задача по обеспечению ее защиты. С каждым днем таких систем становится все больше. Специалисты по кибербезопасности должны постоянно следить за свежими тенденциями и новшествами, а также неустанно учиться, расширяя свои базы знаний и сохраняя способность защищать наш цифровой образ жизни. Добавьте к этому факторы стресса, связанные с подбором кадров и ограниченными бюджетами, и вы получите нечто, напоминающее бесконечный цикл попыток сделать как можно больше с минимальными затратами.

Наконец, не стоит забывать о критической важности самой роли профессионалов в области кибербезопасности. В конце концов, наша работа — защищать организацию, и в случае нашей неудачи может пострадать вся компания. Например, украдут данные клиентов или их деньги или случится что-то другое, столь же катастрофическое. Бизнес может потерять прибыль, получить штраф от регулирующих органов

или утратить доверие акционеров. В зависимости от отрасли инцидент рискует затронуть целые рынки или даже всю мировую экономику, как мы видели в последние годы на примере различных утечек данных и атак программ-вымогателей. Все это тоже повышает уровень давления и стресса, которые специалисты по кибербезопасности испытывают на работе.

Начав карьеру в сфере кибербезопасности, вы, вероятно, переживете фазу *медового месяца*. В этот период все рабочие моменты наполнены волнением, связанным с новыми вызовами. Вы чувствуете себя максимально энергичным, поскольку каждый день дарит возможности для обучения и роста. Вероятно, в это время вы будете испытывать максимальное удовлетворение от работы.

К сожалению, эта фаза не длится вечно. Освоившись с ролью, вы постепенно начнете подвергаться стрессу. Повседневные переживания станут более приземленными и однотипными. Определенные задачи или организационные трудности будут вызывать у вас раздражение. Это свойственно любому карьерному пути. Тем не менее, если на этом этапе вы не начнете что-то делать, чтобы сопротивляться влиянию этих факторов, стресс будет накапливаться и рано или поздно произойдет выгорание.

В предотвращении эмоционального выгорания ключевой аспект — регулярная забота о себе. Суть ее может варьироваться от человека к человеку. По факту это должен быть регулярный и запланированный отдых от трудового стресса. В частности, следует избегать переработок. Учитывая критическую важность кибербезопасности для организации и иногда даже для мировых рынков, переработки здесь — обычное дело. Чувствуя определенную долю ответственности за результат в каждом деле, вы можете работать намного дольше, чем от вас ожидается.

Забота о себе предполагает выделение времени, свободного от работы. Выключите компьютер и выйдите из офиса. Можете запланировать на этот период другие занятия. Хобби, физическая нагрузка, общение с семьей и другие не связанные с работой виды деятельности помогут вам переключиться.

Еще один важный элемент заботы о себе — использование отпуска. К сожалению, люди нередко пренебрегают этим свободным временем, о котором так старательно договаривались при приеме на работу. Во многих компаниях неиспользованные дни отпуска сгорают. Помните, что ваш работодатель учитывает это время в расходах, связанных с вашим наймом, поэтому вы никогда не должны чувствовать вину за его использование.

Взяв отпуск, отнеситесь к нему серьезно. Если необходимо, отправьтесь туда, где с вами нельзя будет связаться, или как минимум сообщите

всем, что во время отпуска вы будете недоступны. Не поддавайтесь искушению «ответить только на этот звонок», каким бы важным он ни казался.

Если вы, чтобы предотвратить выгорание, не установите личные границы на ранних этапах, это может не только повлиять на вашу текущую работу, но и подорвать всю вашу карьеру. Специалисты по кибербезопасности часто говорят, что почти решились уйти или ушли из этой сферы из-за того, что выгорели. Сегодня у вас есть активы: ваши сила и страсть. Однако, чтобы сохранять курс, этот уровень энергии необходимо поддерживать.

9.1.2. Гейткипинг

На каком-то этапе карьеры (вероятно, даже на нескольких) вы неизбежно столкнетесь с таким явлением, как *гейткипинг* (от англ. gatekeeping, концепция «привратника»); это установление или попытка установления неуместных или ложных требований, связанных с некоторой ролью или функцией. Например, в разговорах с другими профессионалами вы можете услышать, что человек, чтобы стать эффективным специалистом по кибербезопасности, должен какое-то время проработать в службе поддержки. Однако, хотя эта роль действительно способна вооружить вас полезными навыками, это ни в коем случае не обязательное требование.

В сфере кибербезопасности гейткипинг — неприятная реальность. Складывается впечатление, что в нашем сообществе эта практика встречается чаще, чем в других. Возможно, что это объясняется, по крайней мере частично, отсутствием четкой траектории карьерного роста. Взглядов на то, какой она должна быть, множество, а некоторые люди к тому же выдают свое мнение за факт. Кроме того, как говорилось в главе 8, для сообщества специалистов по кибербезопасности характерен токсичный уровень конкуренции. Соперничество побуждает некоторых людей изобретать препятствия, чтобы сдерживать рост остальных.

Гейткипинг не только усугубляет проблемы, связанные с синдромом самозванца, но иногда даже заставляет людей чувствовать, что сообщество в целом недостаточно дружелюбно. Трудно представить, скольких потенциальных специалистов отпугнуло мнение ряда более опытных профессионалов, что для входа в отрасль надо обладать опытом, не связанным с обеспечением безопасности. Слышать эти истории временами очень обидно, учитывая, насколько неоправданны некоторые искусственные барьеры.

При определенном уровне осведомленности решить проблему гейткипинга не так сложно. Иногда достаточно лишь знать о ее существовании, чтобы отличить обоснованное требование от предвзятого мнения. И, столкнувшись с последним, просто проигнорировать указание такого «привратника», ведь вы знаете, что добиться желаемого можно разными путями.

Впрочем, если «привратник» способен влиять на ваш карьерный рост, проблема усугубляется. Указания человека, от которого зависит достижение вашей следующей цели, игнорировать сложнее. Столкнувшись с «привратником», каким-либо образом ограничивающим ваше продвижение, важно сохранять спокойствие и не переходить в наступление. Прав он или нет, в случае конфронтации между вами его мнение, учитывая его положение и влияние, будет обладать большим весом, чем ваше.

Однако спокойствие не означает покорность. Важно сохранять уверенность в себе и при общении с этим человеком и другими людьми проявлять ее в дружеской манере. Будьте прямолинейны, делясь своим мнением и знаниями, и не идите на уступки, если не верите, что они помогут.

Иногда для победы над «привратником» достаточно превратить его в союзника. Вместо того чтобы пытаться убедить человека в том, что он ошибается, просто начните с ним работать. Развейте некоторые из его тревог (которые, вероятно, и вызывают проблемное поведение), показав ему, что вы не представляете угрозы. К каждому «привратнику» нужно будет искать свой подход, однако если вы умеете распознавать гейткипинг и у вас есть план решения проблемы, это поможет ускорить ваш карьерный рост.

9.1.3. Стагнация

Хотите верьте, хотите нет, но, несмотря на то что карьера в сфере кибербезопасности требует непрерывного обучения и роста, многие профессионалы через некоторое время обнаруживают себя в *стагнации*. Это значит, что они застревают в какой-то колее, рост уровня навыков или знаний прекращается.

В некоторых случаях стагнация наступает из-за личностных факторов, чье влияние приводит к тому, что человек теряет мотивацию к самосовершенствованию. Некоторые специалисты по кибербезопасности останавливаются на достигнутом или чувствуют себя настолько комфортно в своей роли, что перестают заставлять себя делать и изучать что-то новое. Это может быть побочным эффектом эмоционального

выгорания: утрата страсти к работе приводит к тому, что она превращается в простую формальность. Другая причина — синдром самозванца или просто боязнь риска. Новые вызовы могут казаться пугающими. Некоторым людям так страшно потерпеть неудачу, что они даже не пытаются что-то предпринимать.

Иногда стагнация обусловлена рабочей атмосферой. Организации тоже рискуют попасть в болото удовлетворенности и перестать вкладываться в свои трудовые ресурсы. В частности, плохое руководство может сдерживать развитие персонала. Кроме того, некоторые компании, где служба кибербезопасности не генерирует прибыль, не видят необходимости расширять способности и знания ее сотрудников. Они считают текущее положение вещей достаточным для поддержания бизнеса, поэтому не делают никаких дополнительных инвестиций. Наконец, в некоторых организациях пути для развития просто отсутствуют. Это может быть потому, что вакансии на должности более высокого уровня подолгу не открываются, или потому, что вы уже достигли вершины в своей организации.

Чтобы выйти из стагнации или предотвратить ее, надо для начала определить ее причину. Той стагнации, в какую вы загнали себя сами, можно избежать, если не допускать выгорания, а также культивировать в себе страсть к работе и готовность к риску. Ищите внутри организации или за ее пределами проекты, которые позволят вам продолжать развиваться и расширять набор навыков. Беритесь за вдохновляющие вас задачи. Рискуйте, однако на случай, если что-то пойдет не так, помните, что у вас есть запас прочности. В конце концов, специалисты по кибербезопасности очень востребованы, так что прыжок веры вряд ли положит конец вашей карьере.

Если причина стагнации кроется в ограничениях, связанных с работой, справиться с ней может оказаться сложнее. Тем не менее поищите способы расширить свое влияние в организации. Попросите разрешения возглавить программу по внедрению нового процесса, инструмента или чего-то подобного, чтобы продемонстрировать свои новаторские качества и прозорливость. Благодаря этому вы освоите новые навыки и, вероятно, изучите новые интересные технологии. Поищите возможности для взаимодействия с руководителями более высокого уровня. Например, поговорите со своим менеджером о том, как вам повысить свою видимость внутри организации. Наконец, подумайте о составлении карьерного плана. Опишите желаемые варианты обучения и узнайте, может ли его профинансировать ваш работодатель.

Если эти шаги не увенчаются успехом или организация окажется не в силах предоставить вам пути для продвижения, вероятно, придется задуматься о смене работы — и это абсолютно нормальная часть

карьерного роста. Очень важно распознать признаки стагнации вовремя — чем раньше, тем лучше — и начать искать новые возможности до того, как она станет фактором, осложняющим трудоустройство.

Лично я придерживаюсь правила: если кто-то предлагает мне работу, в которой я вижу для себя перспективы, я всегда выслушаю предложение и изучу его. Даже если вы не ищете работу, такое событие может стать вашим счастливым билетом в следующий важный проект. В том, чтобы исследовать новые возможности по мере их появления, нет ничего плохого. Убедитесь, что вам есть куда расти. На рис. 9.1 представлены три проблемы, описанные в этом разделе, а также советы о том, как с ними справиться или избежать их.

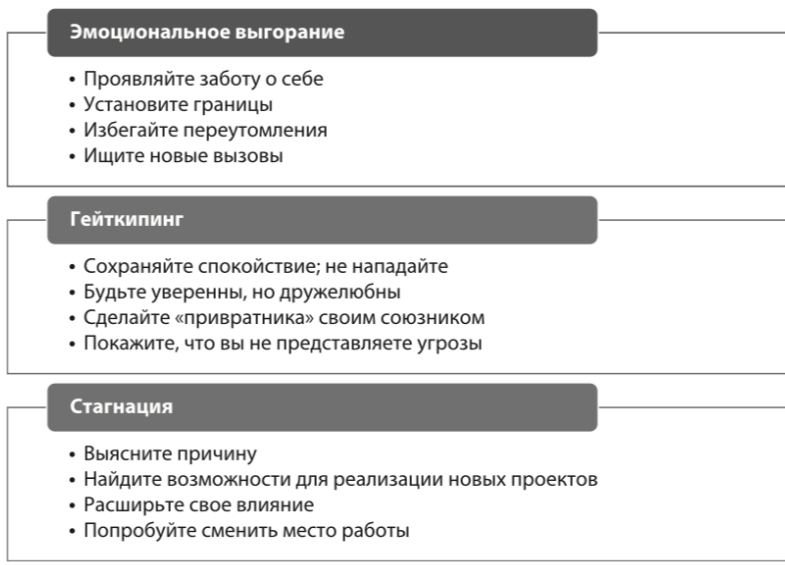

Рис. 9.1. Распространенные проблемы на пути к карьерному успеху и способы их решить или избежать

9.2. Разработка карьерной стратегии

Разработка карьерной стратегии — важнейший шаг, который позволит вам определиться с желаемыми профессиональными успехами, а также понять и достичь их. Нередко люди отправляются в новое карьерное путешествие, не обдумав, куда именно они идут. К сожалению, в результате некоторым приходится по несколько раз сменить направление, что способно замедлить их продвижение к конечной цели.

Я вовсе не имею в виду, что исследовать разные пути бесполезно или что нужно отмахиваться от возможностей, нежданно возникших

на горизонте. Тем не менее в такие моменты важно иметь четкое видение своего карьерного пути: так вы лучше поймете, как эти возможности вписываются в ваш общий план. Благодаря этому вы решите, стоит ли вам скорректировать план или отказаться от них, сочтя отвлекающим фактором.

Разработка стратегии начинается с постановки долгосрочных целей, то есть с формирования общего *видения*. Это отправная точка любой карьерной стратегии. И все же — это лишь точка старта. Как только вы определитесь с тем, куда направляетесь, вам нужно будет проанализировать свое текущее положение и выявить пробелы в навыках или знаниях, которые вам предстоит восполнить, чтобы свое видение реализовать. Список того, что вам требуется для роста, поможет наметить путь к конечной цели.

После этого вам нужно будет расписать этот путь в подробностях. Ставьте краткосрочные и реалистичные цели, достижение которых вы сможете отмечать по мере продвижения вперед. Это будет укреплять вашу уверенность и служить подтверждением того, что ваша карьера развивается, а не стагнирует. Кроме того, это поможет избежать пагубного влияния синдрома самозванца, который мы обсудили в главе 8.

9.2.1. Сформулируйте долгосрочное видение

Перед тем как отправиться в новое карьерное путешествие, крайне важно сформулировать видение долгосрочной цели: оно будет служить вам ориентиром при принятии решений на протяжении всего пути. Видение способно меняться со временем, но это в любом случае та линия горизонта, к которой вы постоянно движетесь. Можете даже называть его своей полярной звездой. Ключ в том, чтобы цели получились достижимыми и реалистичными, но не настолько специфическими, чтобы их видение приходилось то и дело перестраивать.

Думайте об этом как о путешествии. До того как отправиться в путь, вы, вероятно, определяете место, в котором хотите оказаться. Прежде чем выбирать автомагистрали и живописные маршруты для исследования, вы обычно отмечаете для себя пункт назначения. Ваше видение — как раз этот пункт назначения. Его реализация вовсе не означает конец путешествия. Разумеется, вы можете отправиться дальше, однако то, какую цель вы выберете изначально, будет влиять на каждое решение, принимаемое на этом пути вплоть до ее достижения. Вы должны понимать, что, сделав крюк, следует вернуться на прежний маршрут. Вы, безусловно, можете сходить с него, чтобы исследовать живописные тропы, но пункт назначения будет оставаться неизменным.

Карьерная цель в видении должна быть достижимой, но не слишком простой и быстрой в реализации. Как правило, я рекомендую подумать, где человек хотел бы оказаться через 7–10 лет. Такой временной отрезок обычно позволяет представить себе некоторые аспекты будущего, допуская при этом изменение общего ландшафта или цели. В рамках более длительного периода обязательно произойдут какие-то изменения в личной жизни и в отрасли в целом, так что поддерживать выбранное направление окажется проблематично. Более краткосрочное видение не позволит проложить маршрут к достаточно масштабной цели и заставит ограничиваться тактическими решениями, которым не свойственно вести человека в одном общем направлении.

Вспомните упражнения по самоанализу из главы 4. Вспомните, какие направления кибербезопасности вы посчитали для себя наиболее интересными и выбрали в качестве желаемого карьерного пути. Теперь самое сложное. Представьте, что вы отправляетесь в этот путь сегодня. Как думаете, где вы окажетесь через 7 или даже 10 лет? Где вы хотите быть через 10 лет? Эти вопросы кажутся слишком туманными, учитывая, что в сфере кибербезопасности нет четкой последовательности шагов для выстраивания карьеры, которой можно было бы придерживаться. Итак, давайте рассмотрим, как поставить реалистичную цель на 10 лет вперед.

Лучше всего начать с вашего определения успеха или того, что для вас наиболее важно. Вы стремитесь занять определенную должность? Или вас больше всего волнует рост зарплаты? Может, вы хотите развиваться в какой-то определенной отрасли или даже работать в конкретной организации?

У разных людей показатели успеха бывают разными и имеют разный вес. Чтобы определить наиболее важные именно для себя, возьмите лист бумаги и выполните небольшое упражнение.

1. Перечислите факторы, которые считаете показателями успеха. Например, заработная плата, должность, отрасль, лидерство, активизм или участие в развитии сообщества. Проявите креативность.
2. Определите, чего бы вы хотели достичь через 10 лет по каждому из пунктов. Постарайтесь быть реалистом, но если не получается отвечать уверенно, не переживайте. На этом этапе точность и достижимость цели не критичны.
3. Проанализируйте все факторы и цели и расположите их в порядке убывания важности. Если их 10, присвойте им оценки от 1 до 10, где 1 — самый важный фактор.
4. Двигаясь с конца, анализируйте каждый фактор: спрашивайте себя, если бы вы достигли всех остальных целей, кроме этой, смогли бы вы

чувствовать себя успешным? Если да, вычеркните эту цель. Продолжайте двигаться вверх по списку, пока ответ на вопрос не станет отрицательным.

5. Оставшиеся факторы будут наиболее важными для вас на следующие 10 лет; это сферы, на которых вам следует сосредоточиться. Теперь на их основе можно сформулировать свое видение долгосрочных целей.

При отсутствии четкого видения карьерного пути попробуйте обратиться за помощью к участникам сети профессиональных контактов и к наставникам. Если в вашей сети есть люди, занимающиеся тем, что вас интересует, обратитесь к ним и узнайте, как именно развивалась их карьера. Если они не сумеют вам помочь, то, возможно, свяжут вас с кем-то, кто находится на том же этапе карьеры. Поговорите с наставниками, если они у вас есть. Даже если они работают в других направлениях кибербезопасности, попросите их поделиться своими идеями или оценить ваши. Благодаря этим людям вы сможете убедиться, что ваше видение адекватное и реализуемое в десятилетней перспективе.

9.2.2. Определите, что вам нужно для роста

Теперь, когда у вас есть четкое видение того, куда вы направляетесь, пришло время выяснить, что вам нужно для того, чтобы там оказаться. Сначала лучше всего понять, какие знания, навыки и опыт, по вашему мнению, вам в этом помогут. Тем, кто только входит в отрасль, иногда трудно с этим определиться.

Здесь снова можно обратиться к участникам вашей сети личных и профессиональных контактов. Обсудите тему со своим наставником и спросите, в силах ли он дать какие-то рекомендации или связать с кем-то, кто может это сделать. Если ваша цель — занять конкретную должность, просмотрите соответствующие объявления о вакансиях в интернете.

В своих размышлениях старайтесь не зацикливаться на технических навыках. Подумайте, владения какими лидерскими, деловыми и коммуникативными навыками ожидают от человека, достигшего такой же цели. Думайте в абсолютных терминах. Рассмотрите все грани своего видения — и те, что у вас уже развиты, и те, что вам предстоит развить.

Когда вы четко осознаете, что вам нужно, чтобы реализовать свое видение, вернитесь к перечню способностей, составленному в главе 4. Определите разрыв между вашим текущим положением и тем, где вы хотите оказаться через 10 лет. Самое главное при этом быть честным с самим собой и максимально объективным в отношении своего

нынешнего положения и величины разрыва. Составьте список ключевых областей, на которых вам нужно сосредоточиться.

9.2.3. Составьте план на 1 год, 3 года, 5 лет

План на 1 год, 3 года, 5 лет часто используют в корпоративном мире, чтобы контролировать производительность и развитие сотрудников. Однако вовсе не обязательно ждать, пока от вас потребует составить его ваш работодатель. Теперь, когда у вас есть видение и вы понимаете, какие пробелы необходимо устранить, постановка целей на ближайшие 1 год, 3 года и 5 лет поможет вам наметить маршрут.

Возможно, вас удивило, что план ограничен пятью годами, а видение рассчитано на десятилетнюю перспективу. На это есть несколько причин. Во-первых, гораздо проще составить подробный карьерный план на 5 лет вперед, чем на 10 лет. Здесь цель — упростить задачу, а не заниматься сложным планированием и прогнозированием будущего.

Во-вторых, пятилетний план позволяет оценить успехи после преодоления половины пути. Несмотря на то что каждый из интервалов (1 год, 3 года и 5 лет) предусматривает собственные измеримые цели, после выполнения пятилетней программы у вас будет возможность проверить, по-прежнему ли ваш план нацелен на реализацию долгосрочного видения. Кроме того, у вас будет достаточно времени, чтобы понять, насколько вам понравится это путешествие. Например, вы можете обнаружить, что сформулированное видение потеряло для вас актуальность. Таким образом, горизонт планирования, ограниченный пятью годами, предоставляет больше свободы, чем подробный десятилетний карьерный план.

Составление пятилетнего плана не должно показаться слишком сложной задачей, если вы нашли время сформулировать свое видение и перечислить потребности в росте. Все, что требуется, — это поставить реалистичные и измеримые цели, связанные с удовлетворением выявленных потребностей. Как следует из названия, в этом плане вам нужно указать те цели, которых вы планируете достичь в рамках каждого из временных интервалов.

Также важно убедиться, что ваши цели достижимы и реалистичны. Для этого можно снова обратиться к наставникам и участникам сети деловых контактов. Или же обсудить цели со своим руководителем или даже с коллегами. Однако при сборе информации помните, что люди озвучивают свое обоснованное мнение, а не эмпирически подтвержденные факты. Поэтому принимайте только то, что можете использовать, и то, что имеет для вас смысл, а остальное игнорируйте.

Необходимо, чтобы ваш план на 1 год, 3 года, 5 лет был разбит на этапы, как показано на рис. 9.2. Как минимум в нем должно быть перечислено то, чего вы планируете достичь, или то, где вы хотите находиться на каждом из них. Если вы захотите больше деталей, попробуйте составить дорожную карту, показывающую весь путь до цели. Она должна включать конкретные задачи, которые вам необходимо выполнить, чтобы прийти к намеченному результату на каждом этапе. Задачи могут быть связаны с обучением, карьерным продвижением или другими аспектами развития ваших навыков и знаний.

Думаете, тут слишком много расчета? Думаете, большинство людей не осилит такой объем предварительной работы? Что ж, знайте: все это мы уже делаем — такова человеческая природа. Разница в том, что расчета в наших действиях меньше. Вероятно, вы мечтаете о должности директора по информационной безопасности, о собственной компании или о том, чтобы заниматься конкретным типом исследований. Однако для достижения этих целей крайне важно зафиксировать их на бумаге. Мечтать хорошо, но в том, чтобы ставить цели и достигать их, удовольствия гораздо больше. Составить план — это один из способов взять на себя ответственность.

Рис. 9.2. Пример плана на 1 год, 3 года и 5 лет

9.3. Смена направления

Один из самых привлекательных аспектов карьеры в сфере кибербезопасности — возможность с легкостью перейти с одной специализации на другую. Все направления, обсуждавшиеся в главе 2, так или иначе связаны между собой. Степень этой связи отличает кибербезопасность от многих других сфер с несколькими областями специализации. Например, если нейрохирург решит стать акушером, ему придется пройти многолетнюю программу обучения и ординатуры, поскольку в новом

направлении деятельности используются совершенно другие инструменты и методы работы.

А вот если специалист, отвечающий за операции по обеспечению кибербезопасности, захочет стать архитектором безопасности, то на новой должности он сможет применить большую часть знаний, полученных на прежней работе. Сложность с тем, чтобы сменить направление, здесь заключается не в самой смене направления, а в том, чтобы определить момент, когда это следует сделать, наметить путь и рискнуть. Хорошая новость: благодаря всему, что вы узнали с помощью этого руководства, вы сможете совершить этот поворот в карьере, когда посчитаете нужным.

9.3.1. Выявление потребности в изменениях

Хотя сменить направление в сфере кибербезопасности легко, к этому не следует относиться легкомысленно. Речь по-прежнему идет о повороте в карьерном пути, что связано с неопределенностью и риском. Люди решаются на это по разным причинам. Если вы способны понять, когда пришло время что-то менять или когда что-то менять просто необходимо, это может обеспечить дальнейший карьерный рост и предотвратить стагнацию.

Обычно решение о смене направления в сфере кибербезопасности — личный выбор каждого. Если вы сделали все описанное в этой главе, но все еще чувствуете симптомы выгорания, вероятно, вам стоит подумать о смене специализации. Например, если вы работаете в SOC, а трудовые обязанности и темп работы вызывают слишком большой стресс, это может говорить о необходимости изменений. Однако перед этим убедитесь, что вам не нравится именно конкретное направление кибербезопасности, а не то, как оно реализовано в вашей организации.

Для этого можете обратиться к участникам вашей сети контактов, занимающим аналогичные должности, и узнать об их опыте. Разделяют ли они чувство разочарования, заставляющее вас сомневаться в том, что вы правильно выбрали направление? Если да, то, вероятно, действительно пришло время его сменить.

Также можно припомнить все аспекты, которые вас не устраивают; если не хотите, не записывайте их — просто подумайте о них. Действительно ли это та самая неотъемлемая часть вашей работы, которая заставляет вас стремиться к переменам? Если да, то, возможно, смена направления и правда вам необходима. Однако если вас не устраивает политика вашей организации, коллеги, рабочие процессы или предоставляемые вам инструменты или поддержка, то имеет смысл задуматься о переходе в другую компанию.

Еще одна из причин, способных подтолкнуть к смене направления, — это стагнация. На каком-то из этапов карьеры вы рискуете обнаружить, что утратили страсть к тому, чем занимаетесь. В таком случае, быстро переключившись на новую роль, вы можете открыть для себя новые сферы интересов и возродить страсть к своему делу. Например, если при сотрудничестве с разными подразделениями службы безопасности вы познакомились с дисциплинами, которые показались вам особенно интересными, почему бы и не сменить направление — просто чтобы исследовать новые области и расширить свой набор навыков.

Опять же, здесь главное убедиться, что сменой направления вы решаете ваши проблемы. Если вы хотите изучить другие аспекты кибербезопасности, это может стать достаточно веской причиной, чтобы выбрать новую дисциплину, — как и чувство, что добились всего, чего хотели, в текущей области. Если же вы впали в стагнацию из-за отсутствия путей для продвижения или из-за того, что ваш работодатель не инвестирует в ваше развитие, то, возможно, лучше будет перейти в другую организацию.

Так или иначе, важно распознавать эти проблемы по мере их появления и понимать, почему иногда из-за них направление приходится менять. Будьте честны с собой и не бойтесь признаться себе в том, что это именно, что вам нужно. Возможно, вы сделали ошибку, когда перечисляли свои интересы; это совершенно нормально. Однако вам также следует помнить, что для смены направления есть и другие причины. Например, ваши интересы изменились или вы не хотите, чтобы ваша карьера ограничивалась одной специализацией. Относитесь к необходимости сменить сферу деятельности спокойно и не считайте ее признаком того, что ваша карьера развивается в неверном направлении.

9.3.2. Итак, вы хотите сменить направление деятельности, что дальше?

Помните упражнение для поиска своей страсти, которое вы выполняли в разделе 4.2.2? Самое время к нему вернуться. Взгляните на первоначальный список своих интересов. Оцените, сколько из них охватывает ваша нынешняя карьера. Также подумайте, какие из них до сих пор актуальны для вас. Так вы определите, действительно ли ваши увлечения изменились, или вы просто сделали все, что могли, в изначальном направлении и готовы сменить его.

Если вы обнаружите, что интересы в списке утратили для вас актуальность, наверное, настало время снова выполнить это упражнение, чтобы определиться с новым направлением. Вы уже знаете, чем хотите

заниматься? Взгляните на те увлечения, что вы перечислили ранее, и решите, насколько они вам подходят. Вы можете многократно выполнять это упражнение на протяжении всей карьеры. Обновляйте список по мере необходимости и анализируйте, насколько хорошо ваш путь соответствует вашим склонностям.

При выборе новой области интересов нелишним будет обновить свой перечень способностей. Хотя сменить направление в кибербезопасности гораздо проще, чем в других областях, осваивать новые навыки все равно придется. Хорошо понимая свои нынешние способности, вы точнее определите, насколько сложно будет переключиться на новую роль. Если вы обнаружите, что для смены направления вам требуется развить навыки, которые у вас уже есть, значит, вы находитесь в более сильной позиции, чем тогда, когда искали первую работу.

Поскольку вы уже работаете в сфере кибербезопасности, вы вполне можете совершенствовать навыки, пока ищете способы перейти на новую должность. Кроме того, поскольку вы уже зарекомендовали себя в своей организации, вам, вероятно, будет легче определиться с новой ролью и перейти на нее не меняя места работы. В большинстве организаций предусмотрены протоколы перевода сотрудников с одной должности на другую. Изучите эту опцию параллельно с поиском внешних вакансий. Перевод, хотя и может занять больше времени, чем отработка перед увольнением и трудоустройство в новой компании, зачастую вариант более простой, к тому же он позволяет лучше подготовиться к новой роли.

Вернитесь к темам из главы 6, внимательно изучите новую должность и определите, на какую зарплату вы вправе рассчитывать. Одна из проблем со сменой направления внутри компании заключается в том, что руководство зачастую не склонно значительно увеличивать оклад сотруднику, даже если новая должность гарантирует более высокую оплату труда. Изучите, какие обязанности вам предстоит выполнять в новой должности — неважно, в той же компании или другой. Не всегда смена направления предполагает более высокооплачиваемую должность.

Проанализировав перечень своих способностей, вы рискуете обнаружить, что, хотя сейчас занимаете пост руководителя, при смене направления можете претендовать лишь на более низкую должность. В этом случае необходимо определить вероятность снижения заработной платы и то, насколько это для вас приемлемо. Опять же, это еще один способ изучить и оценить новую должность до начала собеседований и переговоров. В конечном счете самые большие проблемы при смене направления связаны не столько с освоением новых навыков, сколько с логистическими аспектами новой роли.

9.3.3. Рискните

Тема риска довольно часто поднималась в последних двух главах. Решая сменить карьерное направление, вы рискуете. Вы покидаете знакомую территорию — неважно, был ваш опыт здесь положительным или отрицательным, — и ступаете на неизведанную землю. Впрочем, специалисты в вашей сфере очень востребованы, и вы всегда можете снова сменить направление или даже вернуться на прежнюю должность, если сочтете нужным.

Риск предполагает проявление некоторой агрессивности. Прежде чем отваживаться на смену карьерного направления, убедитесь, что оно того стоит. Может, вы просто ищете новые пути для обучения и роста. А может, хотите больше зарабатывать или достичь более высоких уровней лидерства. Вам необходимо определиться со своими мотивами и оценить потенциальную выгоду с учетом своих приоритетов.

Риск — неотъемлемая часть роста. Как было сказано в главе 8, если вас затянет в болото безмятежности и вы перестанете рисковать, это, скорее всего, закончится стагнацией, которая сильно повлияет на вашу карьеру. Решив, что настало время сменить обстановку и исследовать новое направление кибербезопасности, не дайте синдрому самозванца или необходимости прокачать какие-то навыки встать у вас пути. Они не помешали вам найти первую работу и поставить перед собой амбициозные цели, так зачем позволять им сейчас сдерживать ваш рост?

9.4. Запуск процесса

Вы это сделали! В главе 1 вы узнали о том, что такое кибербезопасность и как она стала неотъемлемой частью нашего цифрового образа жизни. Вы также осознали, что разнообразие просто необходимо, чтобы наши усилия увенчались успехом. В главе 2 вы познакомились со множеством интересных и разнообразных направлений, существующих в сфере кибербезопасности, и выяснили, какую роль они играют в защите цифровых систем. Вы также узнали, какие характеристики присущи лучшим специалистам в этой сфере и какие практики использовать не стоит.

В главе 3 мы начали говорить о развитии карьеры и о технических навыках, необходимых профессионалам в сфере кибербезопасности. Здесь же мы обсудили гибкие навыки — столь же важные, как и технические. В главе 4 вы ознакомились с проблемами, с которыми вы, вероятнее всего, столкнетесь при поиске первой работы. Вы выполнили несколько упражнений, чтобы провести самоанализ, выбрать желаемый карьерный путь и подготовиться к поиску вакансий. Вы узнали

о базовых навыках и о том, как они помогают продемонстрировать, что вы готовы занять желаемую должность, даже если у вас нет специальных навыков и опыта.

В главе 5 были рассмотрены сертификаты и другие способы развить технические навыки в сфере кибербезопасности. В главе 6 вы узнали, каким стратегиям можете следовать, чтобы составить резюме и успешно пройти собеседование. В главе 7 мы говорили о сети профессиональных контактов и наставнических отношениях.

В главах 8 и 9 мы сфокусировались на будущем и обсудили инструменты, обеспечивающие профессиональный успех в сфере кибербезопасности в долгосрочной перспективе. Теперь вы готовы встать на защиту нашего цифрового мира и принимать вызовы, бросаемые киберзащитникам. Вы можете наслаждаться всеми захватывающими и прибыльными аспектами работы в области, которая славится востребованными профессиями и которая, скорее всего, не потеряет актуальности в ближайшие годы и десятилетия.

Какой еще совет я могу вам дать, помимо всех тех, что были изложены на страницах этого руководства? Пожалуй, я остановлюсь на следующем: сообщество специалистов по кибербезопасности — это удивительный коллектив целеустремленных и высококвалифицированных людей. Отголоски ранней хакерской культуры по-прежнему влияют на то, как строится взаимодействие внутри него. Гордитесь тем, что вы часть этого замечательного сообщества, и постарайтесь сделать его еще сильнее. Активно работайте над повышением инклюзивности, сосредоточивая внимания на том, что для вас наиболее важно, и помогая новым участникам.

Поддерживая друг друга, мы делаем свое сообщество лучше, а мир — безопаснее. Я желаю вам огромных карьерных успехов и надеюсь, что однажды вы расскажете мне о своем опыте.

ПОДВЕДЕНИЕ ИТОГОВ

- Специалисты по кибербезопасности сталкиваются с уникальными проблемами, обретающими форму эмоционального выгорания, гейткипинга и стагнации.
- Постановка долгосрочных целей и разработка пошаговой стратегии для их достижения помогают избежать этих проблем и справиться с синдромом самозванца.
- Смена направления — вполне ожидаемый вариант развития событий, и в сфере кибербезопасности осуществить ее гораздо легче, чем в других отраслях.

Глоссарий

Хотя приведенный далее список не исчерпывающий, в него включены многие распространенные термины кибербезопасности, которые встречаются в этой книге или с которыми вы можете столкнуться в работе. Его цель — познакомить вас с общими концепциями, а изучить их подробнее вы сможете самостоятельно.

ARPANET — экспериментальная сеть сетей, созданная Агентством перспективных исследовательских проектов Министерства обороны США (DARPA); предшественница нынешнего интернета, она соединяла компьютерные сети различных независимых организаций.

DevOps — модель создания программного обеспечения, в рамках которой инженеры-программисты (разработчики, developers) взаимодействуют с командами, занимающимися поддержкой готового ПО (то есть операциями, operations), чтобы сделать процесс разработки максимально эффективным.

DevSecOps — интеграция методов обеспечения безопасности в модель DevOps.

Open Web Application Security Project (OWASP) — основанная в 2001 году некоммерческая организация, реализующая различные проекты и инициативы по повышению безопасности программного обеспечения.

Piggybacking — умышленный пропуск неавторизованного лица вместе с авторизованным лицом через пропускной пункт (например, запертую дверь или турникет).

Tailgating — прохождение неавторизованного лица через контрольный пункт (например, запертую дверь или турникет) без ведома авторизованного лица, идущего впереди него.

Аварийное восстановление (DR, disaster recovery) — вариант реагирования компании на события, отрицательно влияющие на ее системы или способность вести бизнес и восстанавливать работу сервисов.

Авторизация — процесс определения и/или проверки того, что субъекту разрешен доступ к конкретному ресурсу.

Агентство по кибербезопасности и защите инфраструктуры США (CISA, Cybersecurity and Infrastructure Security Agency) — правительственное агентство, подведомственное Министерству внутренней безопасности США. Было создано в 2018 году, чтобы обеспечить кибербезопасность государственных учреждений и критически важных объектов инфраструктуры страны.

Аутентификация — процесс определения того, является ли субъект тем, за кого себя выдает.

База данных управления конфигурациями (CMDB, configuration management database) — каталог с данными об ИТ-активах организации с подробными описаниями их конфигурации.

Безопасность приложений — совокупность методов, с помощью которых организация защищает программное обеспечение, созданное командами разработчиков.

Безопасность программного обеспечения — совокупность методов, разработанных для защиты всего программного обеспечения, развернутого в среде организации, вне зависимости от того, кто его создал — сама организация или сторонний поставщик.

Ботнет — группа компьютеров, которые скомпрометировал злоумышленник, чтобы проводить дополнительные атаки.

Брандмауэр (межсетевой экран) — сетевое устройство или программное обеспечение, которое контролирует доступ к сети или подключенным к ней ресурсам, анализируя сетевые запросы и применяя правила, определяющие, что разрешено, а что нет.

Брандмауэр веб-приложений (WAF, web application firewall) — особый вид брандмауэра, который анализирует запросы, направляемые веб-приложению, чтобы выявлять потенциальные атаки и обеспечивать защиту от них.

Взлом — событие, при котором злоумышленнику удается обойти средства защиты, чтобы получить несанкционированный доступ к ресурсу.

Вирус — подмножество вредоносных программ. Цель этого вредоносного кода — повлиять на функциональность системы или получить несанкционированный доступ к ней, а также распространиться на другие системы.

Внедрение SQL-кода (SQLi, SQL injection) — тип атаки на приложение, при которой злоумышленник может манипулировать базой данных приложения, отправляя специально созданные данные в его пользовательский интерфейс.

Внутренняя угроза — люди внутри организации, которые могут причинить ей вред, преднамеренно или непреднамеренно скомпрометировав ее системы или данные.

Вредоносная программа — вредоносное программное обеспечение, цель которого — скомпрометировать компьютерную систему, предоставив злоумышленнику несанкционированный доступ к ней.

Входящий трафик — данные, поступающие в систему.

«Горшочек с медом» (honeypot) — система-приманка, призванная привлекать внимание злоумышленников, что дает защитникам время обнаружить их и начать действовать до того, как будут атакованы настоящие системы.

Группа реагирования на инциденты информационной безопасности (CERT, Computer Emergency Response Team) — подразделение Института разработки программного обеспечения Университета Карнеги — Меллона, которое изучает проблемы кибербезопасности и решает их совместно с различными правительственными и отраслевыми организациями.

Директор по информационной безопасности (CISO, chief information security officer) — руководитель, отвечающий за реализацию программы по кибербезопасности на уровне всей организации.

Жизненный цикл разработки программного обеспечения (SDLC, software development life cycle) — набор повторяющихся процессов, с помощью которых в организации группы разработчиков создают, тестируют и развертывают программное обеспечение.

Захват флага (CTF, capture the flag) — мероприятие, где участники должны найти в системе различные индикаторы (флаги), как правило, выполняя атаки той или иной формы. Часто такие мероприятия представляют собой соревнования, в рамках которых хакеры пытаются взломать разные аспекты системы.

Индикаторы компрометации (IOC, indications of compromise) — данные, обнаруженные с помощью методов цифровой криминалистики и указывающие на потенциально вредоносную активность в системе.

Интернет вещей (IoT, Internet of Things) — бытовые устройства, которые не были созданы для вычислений, но предусматривают возможности компьютерной обработки, позволяющие им подключаться к сетям и взаимодействовать с другими цифровыми системами (например, умные холодильники и фитнес-трекеры).

Информационная безопасность (ИБ) — функция бизнеса, связанная с защитой ИТ-активов от угроз.

Информационные технологии (ИТ) — совокупность цифровых систем (включая компьютеры, сети и периферийные устройства), используемых организацией для ведения бизнеса.

Исходящий трафик — данные, покидающие систему.

Командование и управление (C2, command and control) — централизованная система или сеть, контролирующая участников ботнета и позволяющая злоумышленникам реализовывать атаки.

Компрометация — получение неавторизованным злоумышленником доступа к ресурсу.

Контроль — средство защиты или контрмера, применяемая для того, чтобы снизить риск компрометации системы.

Конфиденциальность, целостность и доступность, триада (CIA, confidentiality, integrity, availability) — модель для обсуждения мер по обеспечению безопасности. Под «конфиденциальностью» понимается защита ресурсов от просмотра неавторизованными лицами. «Целостность» подразумевает защиту ресурсов от несанкционированной модификации. А «доступность» — обеспечение бесперебойного доступа к ресурсу для авторизованных пользователей.

«Красная команда» — специалисты по кибербезопасности, которые выявляют уязвимости в системах и программном обеспечении, используя типичные тактики и методы злоумышленников.

Криптография — практика защиты данных от несанкционированного доступа; к данным применяется сложное математическое правило, без знания которого их нельзя расшифровать.

Межсайтовый скриптинг (XSS, cross-site scripting) — тип атаки на веб-приложение, позволяющей злоумышленнику внедрить вредоносный код в браузер жертвы. Входит в десятку ключевых рисков для веб-приложений, согласно OWASP.

Менеджер службы информационной безопасности (BISO, business information security officer) — руководитель программы обеспечения кибербезопасности, реализуемой на уровне подразделения, группы или бизнес-направления внутри организации.

Минимальная привилегия — структура, гарантирующая, что пользователям разрешен доступ к минимальным функциям и ресурсам, которые им необходимы для конкретной цели, задачи или работы.

Многофакторная аутентификация (MFA, multifactor authentication) — использование нескольких форм (факторов) для подтверждения личности пользователя. Пример двухфакторной аутентификации — комбинация того, что пользователь знает (пароль), с тем, что у него есть (код, отправленный на телефон).

Моделирование угроз — анализ системы, проводимый для того, чтобы изучить угрозы, которым она подвержена, и заранее разработать меры противодействия им.

Модель взаимодействия открытых систем (OSI, Open Systems Interconnection) — семиуровневая модель, которая описывает разные функции, позволяющие компьютерам обмениваться данными по сети.

Национальный институт стандартов и технологий (NIST, National Institute of Standards and Technology) — нерегулирующее агентство правительства США, основанное в 1901 году как часть Министерства торговли; оно устанавливает различные стандарты, в том числе в отношении кибербезопасности.

Нулевое доверие — модель реализации защитных мер, где все компоненты системы рассматриваются всеми другими компонентами как ненадежные, так что все взаимодействия требуют прохождения аутентификации и авторизации.

Облако — сервис, который предоставляет отдельным людям и организациям вычислительные ресурсы, освобождая их от необходимости создавать и обслуживать собственные ИТ-системы.

Обратный инжиниринг — деконструкция части программного обеспечения до уровня исходного кода, чтобы проанализировать функциональность без его выполнения.

Общая ответственность — идея о том, что две группы несут некоторую долю ответственности за успешное достижение бизнес-цели. В рамках концепции DevSecOps под этим подразумевается, что все три дисциплины должны обеспечивать эффективную разработку стабильного и безопасного ПО. *Модель общей ответственности за защиту облака* предполагает разделение обязанностей по обеспечению безопасности развернутых в облаке систем между поставщиком облачных сервисов и клиентом.

Оперативная группа по обеспечению кибербезопасности — группа, отвечающая за мониторинг и управление средствами защиты, работающими в ИТ-системах организации.

Отказ в обслуживании (DoS, denial of service) — тип атаки, при которой злоумышленник пытается сделать конкретную систему или ресурс недоступными для использования.

Отказ / невозможность отказа — способность к отрицанию достоверности части данных (отказ) или гарантия того, что сомнения в их достоверности быть не может (невозможность отказа). Примером последнего может быть бесспорная идентификация пользователя, ответственного за выполнение определенного действия в компьютерной системе.

Отрасль кибербезопасности — сообщество людей и организаций, которые заинтересованы в защите цифровых систем, используемых во всех сферах общественной жизни.

Оценка и проверка безопасности — совокупность процессов, направленных на анализ надежности и отказоустойчивости систем и программного обеспечения.

Пентестер (специалист по тестированию на проникновение) — нанятый организацией хакер, который атакует ее системы, пытаясь выявить уязвимости и определить способы их устранения. Также известен как *этичный хакер*.

Переполнение буфера — тип атаки, при которой злоумышленник может перезаписать системную память и тем самым изменить данные или инструкции, выполняемые процессором компьютерной системы.

Перечень активов — каталог всех известных цифровых и физических информационных технологий, используемых в организации.

Постоянная серьезная угроза (APT, advanced persistent threat) — особые субъекты угроз или их группы, которые тайно получают доступ к системе и поддерживают его в течение длительного времени, чтобы скомпрометировать дополнительные системы и расширить свое влияние.

Предотвращение потери данных (DLP, data loss prevention) — методы и средства контроля, которые организация применяет, чтобы не допустить преднамеренную или непреднамеренную передачу пользователями конфиденциальной информации неавторизованным третьим лицам.

Призыв к подаче заявок на выступление с докладом (CFP, call for papers) — предложение участникам сообщества представить свои презентации и другие образовательные материалы на конференции или любом другом мероприятии.

Программа-вымогатель — особый тип вредоносного ПО, которое после компрометации системы шифрует файлы и данные, делая их недоступными для пользователя или организации, а затем требует выкуп за расшифровку и восстановление доступа.

Промышленные системы управления (ICS, industrial control systems) — ИТ-системы для управления такими физическими системами, как производственные машины, средства управления коммунальными услугами и так далее.

Псевдонимы (handles) — вымышленные имена, которыми люди представляются в социальных сетях и на других платформах. Часто применяются как способ сохранения анонимности.

Распределенный отказ в обслуживании (DDoS, distributed denial of service) — атака, при которой злоумышленник использует большое количество систем, часто в виде ботнета, чтобы провести DoS-атаку системы жертвы. Его цель — перегрузить целевую систему и сделать ее недоступной для использования.

Реагирование на инциденты (IR, incident response) — процесс или дисциплина реагирования на события, которые могут отрицательно повлиять (или уже повлияли) на поддерживаемые ими ИТ-системы и/или бизнес-процессы.

Риск — вероятность того, что из-за конкретной угрозы система окажется скомпрометирована. Как правило, при его определении учитывается вероятность компрометации и потенциального воздействия на систему или на бизнес в случае наступления этого события.

«Синяя команда» — специалисты по кибербезопасности, ответственные за защиту цифровых систем и пользователей от злоумышленников.

Система обнаружения вторжений (IDS, intrusion detection system) — система, которая отслеживает активность в сети или системе, чтобы выявлять потенциальные атаки и отправлять оповещения ее защитникам.

Система предотвращения вторжений (IPS, intrusion prevention system) — система, которая отслеживает активность в сети или системе, чтобы выявлять потенциальные атаки и предотвращать их, а также предупреждать о них защитников.

Сканирование портов — попытка определить службы, которые работают в системе, подключенной к сети; злоумышленник отправляет в систему невредоносный трафик и анализирует реакцию на него.

Смягчение рисков — подход к обеспечению безопасности, направленный не на устранение конкретной угрозы, а на снижение связанных с ней рисков.

Совместимая система разделения времени (CTSS, Compatible Time-Sharing System) — компьютерная система, созданная в Массачусетском технологическом институте в начале 1960-х годов, к которой в одно и то же время могли получить доступ сразу несколько пользователей. Помимо этого, она считается первой известной компьютерной системой, применяющей пароли для аутентификации нескольких пользователей.

Социальная инженерия — дисциплина, изучающая способы обмануть человека, чтобы манипулировать им и в результате получить доступ к защищенному ресурсу.

Список запретов — список известных значений, которые не пропускаются конкретным средством защиты. Также известен как *черный список*, хотя этот термин постепенно выходит из употребления.

Список разрешений — список известных значений, которые пропускаются конкретным средством защиты. Также известен как *белый список*, хотя этот термин постепенно выходит из употребления.

Спуфинг — маскировка источника конкретного запроса или действия, чтобы обойти средства защиты или скрыть, кто за это ответственен.

Тактики, техники и процедуры (TTP, tactics, techniques, and procedures) — совокупность типичных действий, составляющих схему атаки, которые затем можно отнести к определенному типу атаки или даже к конкретной группе злоумышленников.

Угроза — злоумышленник или действие, направленное на компрометацию системы с различными целями.

Удаленное выполнение кода (RCE, remote code execution) — результат использования уязвимости в системе, позволяющий злоумышленнику запускать в ней несанкционированные команды.

Управление идентификацией и доступом (IAM, identity and access management) — структура практик, процессов и технологий для обеспечения аутентификации и авторизации в ИТ-системах.

Управление инцидентами и событиями информационной безопасности (SIEM, security incident and event management) — система, которая собирает информацию из различных ИТ-систем и позволяет анализировать происходящие в них события и реагировать на них, часто в автоматическом режиме.

Управление уязвимостями — практика, применяемая организацией для выявления и устранения уязвимостей в системах и программном обеспечении.

Управление, риск-менеджмент и соблюдение требований (GRC, governance, risk, compliance) — стратегия контроля над различными аспектами подхода, применяемого организацией к информационным технологиям, гарантирующая, что он поддерживает функционирование бизнеса. «Управление» подразумевает использование политик и стандартов, гарантирующих, что процессы способствуют достижению бизнес-целей. Под «риск-менеджментом» понимается выявление факторов, которые могут негативно повлиять на достижение бизнес-целей, и реагирование на них. «Соблюдение требований» означает обеспечение соответствия деловой практики законам и правилам конкретного бизнеса.

Уязвимость — недостаток (или слабость) системы, который может позволить злоумышленнику обойти другие средства ее защиты.

Фаззинг — автоматизированный метод тестирования системы на уязвимости или ошибки кода, когда ей подаются на вход различные формы недопустимых или неожиданных данных.

«Фиолетовая команда» — команда из членов «красной команды» (атакующих сеть или систему), которые работают вместе с членами «синей команды» (защитниками), чтобы улучшить средства защиты и научиться предотвращать типы атак, увенчавшихся успехом.

Фишинг — отправка поддельных электронных писем, чтобы спровоцировать получателя на ответ, который раскрывает его личные данные или позволяет вредоносным программам или программам-вымогателям скомпрометировать его систему.

Хеширование — криптографический метод получения строки символов фиксированной ожидаемой длины, которую нельзя преобразовать обратно в исходные данные.

Целевой фишинг — отправка поддельных электронных писем, чтобы спровоцировать получателя на ответ, который раскрывает его личные данные или позволяет вредоносным программам или программам-вымогателям скомпрометировать его систему. Слово «целевой» здесь говорит о том, что злоумышленник использует конкретные сведения о жертве, чтобы создать более убедительное сообщение.

Центр обработки данных — физический объект, в котором размещены ИТ-системы организации и который обеспечивает необходимое питание, охлаждение и инфраструктуру для их непрерывной работы.

Центр оперативного управления информационной безопасностью (SOC, security operations center) — централизованное подразделение организации, отвечающее за мониторинг и управление средствами защиты, работающими в ИТ-системах данной организации. Этот термин также может обозначать определенное место или места, где работает оперативная группа по обеспечению кибербезопасности.

Цифровая криминалистика и реагирование на инциденты (DFIR, digital forensics and incident response) — сочетание двух связанных направлений, цифровой криминалистики и реагирования на инциденты.

Цифровая криминалистика — одно из направлений кибербезопасности, сосредоточенное на анализе различных аспектов системы для выявления произошедших в ней событий и сборе доказательств.

Цифровой сертификат — электронный ключ, также называемый *открытым ключом*, используемый для шифрования данных перед их отправкой или сохранением в каком-либо месте. Для расшифровки этих данных требуется закрытый ключ.

Червь — подмножество вредоносных программ, где ПО проникает из одной системы в другую через сеть. Она отличается от вируса тем, что далеко не всегда влияет на функциональность системы или получает дополнительный доступ.

Шифрование — применение криптографического алгоритма к данным, чтобы сделать их нечитаемыми для неавторизованных третьих лиц.

Шифротекст — результат применения алгоритма шифрования к некоторым данным.

Эксплойт — использование уязвимости, чтобы получить несанкционированный доступ к системе. Этим термином также описываются применяемые тактики взлома.

Электронные доски объявлений (BBS, bulletin board system) — компьютерное программное обеспечение, позволяющее пользователям подключаться к сети — как правило, с помощью модема — и взаимодействовать друг с другом в текстовой среде. Пользователи могут загружать/скачивать файлы, читать чужие сообщения и публиковать свои. Хакеры использовали BBS для обмена информацией до появления интернета.

Этичный хакер — нанимаемый организацией хакер, который атакует ее системы, пытаясь выявить уязвимости и определить способы их устранения. Также известен как «пентестер», или специалист по тестированию на проникновение.

Предметный указатель

0+

Популярное издание
Серия «Библиотека программиста»

Алисса Миллер

ПУТЕВОДИТЕЛЬ ПО КАРЬЕРЕ В КИБЕРБЕЗОПАСНОСТИ

Ответственный редактор *Екатерина Истомина*
Литературный редактор *Екатерина Никитина*
Художник *Эрик Брегис*
Верстка *Эрик Брегис*
Корректура *Римма Болдинова*

Издатель и изготовитель: ООО «Феникс».
Юр. и факт. адрес: 344011, Россия, Ростовская обл.,
г. Ростов-на-Дону, ул. Варфоломеева, д. 150
Тел/факс: (863) 261-89-65, 261-89-50

Свои пожелания и предложения по качеству и содержанию книг
вы можете сообщить по e-mail: idea@fenixrostov.ru