ПРЕДИСЛОВИЕ

В 90-х годах я ходил в краевую станцию юных техников (КСЮТ) во Владивостоке, которая доживала свой век после былого величия времен Советского Союза. Кружок судомоделирования, как и многие другие, финансировался государством очень плохо, частные спонсоры того времени («братки» и олигархи) не особо хотели вкладываться в будущее российских технологий, предпочитая спонсировать спортивные мероприятия и команды. Мы выкручивались как могли, первой моделью для всех была подводная лодка с корпусом из эпоксидной смолы и винтом, приводимым в движение закрученной резинкой (не удивлюсь, если ее доставали из трусов). Если ты достигал определенного уровня, то мог собрать модель с настоящим двигателем, вот только он был один на кружок.

В ходе наших первых конструкторских шагов мне и моим друзьям по инженерному делу приходилось постоянно выкручиваться, собирать модели буквально из «говна и палок» и даже рыться в мусорках, чтобы найти нужные компоненты и материалы. Когда мне задают вопрос действительно ли русские хакеры — одни из сильнейших в мире, я отвечаю без сомнения, что для этого есть предпосылки. Люди, которые так тянутся к технике, которые легко находят нестандартные решения при ограниченных ресурсах, несомненно, являются хакерами по духу.

Основным побудительным мотивом написания данной книги является нескончаемый поток искаженной информации о рисках и негативных последствиях цифровизации нашей жизни. Представители ИТ-компаний, руководствуясь желанием наживы, умалчивают,

что человек, используя некоторые инновации, подвергает опасности свою приватность, финансовое положение, а иногда жизнь и здоровье. Они показывают вовне только позитивные аспекты использования своих разработок, оставляя без внимания то, чем мы жертвуем при их использовании. Компании тратят деньги на маркетинг своих продуктов, а не на их устойчивость к взломам и кибербезопасность. Для компаний любой пользователь всего лишь источник дохода. Ради получения приватных данных и денег за свои продукты ИТ-индустрия способна не только на маленькую ложь, но и на откровенный обман.

Государства также вводят нас в заблуждение. Их интерес в том, чтобы ускорить темпы цифровизации. Во многом успехи на данном поприще определяют престиж, инвестиционную привлекательность и поддержку обществом государства. Кроме того, успехи на цифровом поприще повышают престиж страны на мировой арене, обеспечивают приток людских ресурсов и помогают решить многие задачи национальной безопасности. Поэтому государства также способны на умалчивание некоторых негативных эффектов внедрения информационных технологий, а иногда и на откровенный обман. В чем они правы, так это в том, что цифровизация действительно может сделать жизнь граждан лучше и удобней, повысить прозрачность предоставления государственных услуг, обеспечить безопасность улиц наших городов и многое другое. Вот только, как и ИТ-компании, государства пока не могут гарантировать нам адекватный уровень защиты нас и наших данных от посягательств киберзлоумышленников.

Сложно ответить на вопрос, для кого эта книга. Можно лишь предположить, кому она была бы интересна. Это на данный момент практически любой человек, так как вопросы кибербезопасности, взломов и мошеннических действий касаются практически каждого. Новости кибербеза льются буквально из «каждого утюга». Если вы зачитываетесь постами про новые взломы или останавливаете свой взгляд на заметках о хакерах, то эта книга для вас. Она может быть воспринята

как «бульварное чтиво» специалистами в области кибербезопасности или профессиональными взломщиками компьютерных систем, но и тем и другим будет интересно то, как киберпреступность и кибербезопасность влияют на общество и современную жизнь.

Внимания к ИТ последнее десятилетие всегда хватало, но с февраля 2022 года компьютерная сфера стала интересовать не только специалистов, но и обычных людей, власть и бизнес. Если у вас есть компьютер или смартфон, то на страницах книги вы найдете подсказки, на какие особенности ИТ-продукта вам стоит обратить внимание, чтобы не стать жертвой прослушки или сбора данных. Читатель узнает, на что стоит обратить внимание при прочтении пользовательского соглашения и как следует настраивать политики безопасности и приватности цифрового приложения. Для тех, кто интересуется ИТ-бизнесом, сей опус будет занимателен, поскольку подскажет основные риски в сфере кибербезопасности. Если кто-либо интересуется цифровизацией государственной сферы, то он также найдет многие ответы на свои вопросы на страницах данной книги.

Книга рассказывает, что под влиянием киберпреступности происходит в экономике, современном обществе и государстве в России и мире. Дается ответ, почему киберпреступность только набирает обороты, и как она влияет на процесс внедрения технологий в нашу повседневную жизнь. По мнению автора, фактор киберпреступности в скором времени должен стать ключевым, когда речь идет о новом модном гаджете или ИТ-приложении.

В книге кратко рассматривается история киберпреступности. Компьютерный антисоциальный андеграунд влиял на развитие ИТ-индустрии и глобального киберпространства на протяжении десятилетий. Преступники играли ключевую роль в происходящих процессах компьютеризации всех сфер человеческой жизни, начиная с создания Интернета. Крупные хакерские атаки меняли общественное мнение по поводу развития информационных технологий. Они заставляли государства реагировать и менять политику управления киберпространством. Через исторический экскурс автор доказывает,

что киберпреступность еще больше будет влиять на жизнь полностью «оцифрованного общества» в будущем.

Также данная книга — это предостережение. Сейчас в моде необдуманный технооптимизм, когда люди безоговорочно верят гуру ИТ-сферы, которые обещают нам счастливое будущее в результате внедрения новых технологий. Чего никогда не говорят гуру, так это то, что у технологических инноваций всегда есть побочный эффект. Любое решение по поводу внедрения технологии, независимо от того, принимает ли его государство или частная компания, должно сопровождаться оценкой будущих рисков в сфере кибербеза.

Любая новая информационная технология, скорее всего, — это огромная дыра безопасности. В книге дается обзор связанных с киберпреступностью проблем применения некоторых популярных технологий. В тексте раскрывается, как преступники используют нашу слепую веру в новинки технологического мира и чем это оборачивается. Автор ни в коем случае не пытается убедить читателя, что технологии плохие и от них необходимо отказаться. Манифест книги в том, что технологии надо использовать осознанно, понимая риски и возможности их нелегального использования.

Ярким примером, среди прочих примеров в книге, являются беспилотные автомобили. Илон Маск и другие ИТ-гуру обещают нам снижение аварийности на дорогах, улучшение экологического состояния городов, снижение стоимости автоперевозок грузов и пассажиров. Но это обман будущего покупателя, поскольку обещанное работает только в идеальных условиях. Если мы добавим в уравнение злоумышленника, который может вмешаться в работу беспилотника, то оценки безопасности и рисков будут не такими радужными. Читатель будет удивлен, насколько легко взломать любой автомобиль и почему этот факт никого не заботит.

В книге будет много примеров серьезных угроз кибербезопасности, о которых многие из нас даже не подозревают. На страницах читатель встретит много кейсов хакерского мастерства и халатности разработчиков программных продуктов и устройств. Сей опус поведает,

какие действия киберпреступников привлекали внимание общества и государства. О взломе киберпреступниками популярной метавселенной также рассказано на страницах этой книги.

Не обойдет книга своим вниманием и кибервойны. Читатель узнает, как хакеры участвовали в крупнейших политических событиях последних десятилетий, в том числе событиях на Украине в 2022 году. В книге можно прочитать о столкновении самых могущественных хакерских группировок на полях политического конфликта между Москвой и Западом. В книге рассказывается о том, чем нам грозят войны в киберпространстве в будущем и почему эти действия могут обернуться катастрофой для всего мира.

Значительная часть книги посвящена прогнозу, а также анализу трендов и направлений будущего развития киберпреступности. На страницах рукописи предпринята попытка приоткрыть завесу в будущее исходя из того, какие тренды развития в сфере ИТ сформировались в наши дни. Автор не претендует на то, что его прогноз на 100% сбудется, лишь представляет читателю возможные пути развития. Во многом прогнозы помогают понять, насколько реалистичны заявления представителей технологических компаний и государственных органов, которые обещают положительные эффекты от внедрения той или иной технологии.

Попытка составить картину будущего интересна не только с точки зрения понимания социальных, экономических и политических трендов будущего. Прогноз позволяет отдельному человеку разобраться, к чему готовиться и на что следует обратить внимание уже сейчас. Из книги вы узнаете, как можно будет ввести в заблуждение искусственный интеллект и в чем опасность миров виртуальной реальности. В рамках повествования будет изложено, каким образом хакеры, используя последние достижения в сфере нейротехнологий, будут взламывать наш мозг. Мы с вами познакомимся с цифровой личностью и с тем, как ее можно будет подделать. А самое главное — разберем, чем угрожает миру будущего цифровая личность в руках хакера.

Автор данной книги изучал все, что связано с киберпреступлениями, взломами и хакерами, на протяжении 20 лет. Начав как программист, который интересуется написанием устойчивого к взлому программного кода и обожает хакеров, он продолжил в качестве исследователя-криминолога, который осознавал всю опасность злоумышленников, использующих возможности информационных технологий. Я написал несколько научных книг и несколько десятков научных статей, но в какой-то момент понял, что хочу поделиться своими мыслями с широкой аудиторией. Несмотря на то что книга носит публицистический характер, все написанное основывается на последних достижениях в сфере изучения киберпреступности, кибербезопасности и информационных технологий.

Читатель на страницах книги может заметить легкую симпатию к хакерам, и это не случайно. Автор данной книги, будучи в 90-х студентом института математики и компьютерных наук, поклонялся культу хакеров и их невероятным возможностям. Несмотря на то что годы преподавания правовых предметов заставляют относиться к киберпреступникам в первую очередь как к преступникам, в книге есть место и для восхищения хакерами и их достижениями. Также на страницах данного научно-популярного издания изучена роль хакеров в современном мире и в ближайшем цифровом будущем.

В последнем параграфе данной книги предпринята попытка дать общие советы, которые, как кажется автору, снизят вероятность стать жертвой киберпреступлений. Это не собственная авторская разработка — это всего лишь обобщение мнений специалистов по компьютерному взлому и кибербезопасности. Советы, данные читателю, вряд ли стопроцентно защитят вас от взлома, но точно снизят вероятность стать жертвой киберпреступления.