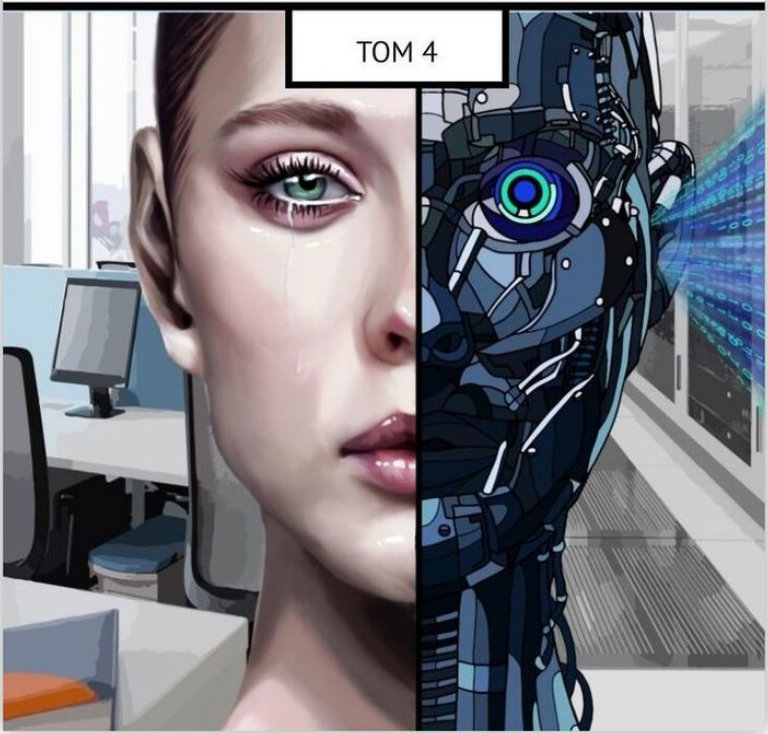
18+

ВЛАДИМИР БЕЗМАЛЫЙ

# Цифровая гигиена



**Владимир Безмалый**

# Цифровая гигиена. Том 4

*http://www.litres.ru/pages/biblio_book/?art=48566164*
*ISBN 9785005075178*

## Аннотация

Мир станет честней и безопасней, когда «цифровая гигиена», то есть набор правил безопасного поведения в цифровом пространстве, войдёт в ежедневную рутину каждого пользователя информационных технологий. Можно было сколько угодно выпускать учёных-эпидемиологов, врачей и гигиенистов, но пока каждый человек на планете не научился мыть руки, человечество не смогло бы победить страшные болезни. То же самое должно произойти и в киберпространстве, тогда «врачам» останется только двигать науку вперёд.

# Содержание

# Цифровая гигиена
# Том 4
# Владимир Безмалый


ISBN 978-5-0050-7517-8 (т. 4)
ISBN 978-5-4493-9108-7
Создано в интеллектуальной издательской системе Ridero

# Введение

Вроде совсем недавно мы открыли первый том «Сказок о безопасности», а уже подоспел четвёртый. Удивляет не только упорство и настойчивость автора, продолжающего следовать своему Пути – в простой и доступной форме знакомить читателей с важными принципами цифровой безопасности, но и саму современную жизнь, в которой с ужасающей скоростью реализуются самые мрачные предсказания и прогнозы. Практически все облечённые в форму сказок случаи нарушения безопасности и приватности пользователей – не плод фантазии автора, а буквально случаи из жизни автора или его реальных и виртуальных друзей. И даже когда автор делает невероятные прогнозы – они сбываются в самом скором времени, заставляя читателей снова и снова задумываться: как стоит изменить своё поведение для того, чтобы этого не случилось с нами? Автор собрал для вас все риски сегодняшнего цифрового мира и даже немного рисков ближайшего завтра, изложил в занятном и понятном виде, а также исподволь даёт вам рекомендации – не назидательно, а в виде доброго совета или заставляя вас придумать такие рекомендации для себя, отвечая на добрые вопросы автора.

Уже сложился круг поклонников серии, которые не только ждут новых сказок, но и посылают автору идеи для новых, рассказывают ему реальные случаи из цифровой жизни

и просят совета. Так что можно сказать, что через трудолюбивый гений автора эти сказки пишет сама жизнь и широкий круг благодарных читателей. Присоединяйтесь и вы: читайте, осознавайте, придумывайте, давайте обратную связь – ведь мы уже необратимо вросли в цифровой мир с его электронными каналами связи и социальными сетями. Наслаждайтесь.

Рустем Хайретдинов – друг и поклонник автора

# Сказки о безопасности: Газовая атака

– Доброе утро, Иоганн!

– Доброе утро, Рита!

– Шеф, вы не забыли, что сегодня пятница и, как обычно, мы обсуждаем увиденное и прочитанное?

– Это я помню. А будет что-то интересное?

– Думаю, очень! Более того, как мне кажется, мы сможем это использовать при проведении спецопераций.

Вечером, в конце рабочего дня.

– Добрый день, друзья! У Риты сегодня важное сообщение. Прошу!

– Спасибо, Иоганн! Как вы знаете, моя мама болеет. И ей периодически нужно проходить сеанс магнитно-резонансной терапии. Спасибо императору (и вам, Иоганн, в первую очередь, за заботу), это делается бесплатно в имперском госпитале. Ну так вот. Я повезла на этой неделе маму на эту процедуру. Но как раз перед тем, как она должна была зайти, в кабинете, в котором установлен аппарат, произошла утечка гелия, который используется для его охлаждения. Всего 120 литров. В принципе немного, персонал и пациенты не пострадали. Мама тоже.

– Погодите, хорошо, что мама не пострадала, а мы тут причем.?

– Майкл, я, безусловно, ценю твою заботу обо мне и моей маме, но ты торопишься. Возьми лучше еще кофе и помолчи, хорошо?

– Так вот, продолжаю. Вся техника, произведенная компанией А, которая оказалась рядом, вышла из строя. Сначала это происшествие было списано на идущее от аппарата электромагнитное излучение. Но как показало расследование, находившиеся поблизости гаджеты иных производителей не пострадали. Виновником оказался гелий.

– И в чем была проблема?

– Проблема, скорее всего, в новейших микро электромеханических системах (MEMS). Их сейчас использует А вместо прежних кварцевых компонентов. Для проверки своего предположения мы поставили эксперимент: уложили в гер-

метичный пакет смартфон этой компании и добавили туда газ в значительной концентрации. Восемь минут спустя гаджет завис и потерял работоспособность.

«Умные» часы и смартфоны той же компании либо серьёзно сбоили, либо совсем выходили из строя. Я попробовала зарядить пострадавшие гаджеты. Однако большая их часть так и не начала работать. У некоторых смартфонов появились проблемы с подключением к мобильной сети, в то время как Wi-Fi-соединение было по-прежнему стабильным.

– Вы обратились в компанию производитель?

– Конечно. В компании нам дали совет по «лечению» пострадавшего устройства. В ней сказано, что гаджет нужно отсоединить от кабеля зарядки и оставить в покое приблизительно на неделю. Этого времени ему должно хватить, чтобы полностью проветриться и вернуть работоспособность.

– Рита, вы говорили, что это может нам помочь в некоторых спецоперациях?

– Да! У бандитов использование техники от А считается модным и престижным. Перед началом операции нам достаточно закачать небольшой объем гелия, и вся техника просто перестанет работать. В результате – никто никуда не сможет позвонить и написать. И удалить информацию тоже. А мы потом получим все в исправном состоянии. Я не права?

– Умница! Нужно попробовать!

***Вот так закончилась эта история. А техника Apple***

***действительно уязвима к «газовой» атаке. Помните об этом!***

# Сказки о безопасности: Нападение на следователя

– Доброе утро, господин комиссар! У нас чрезвычайное

происшествие! На квартиру следователя К совершено нападение. Нападавший убит. Первое впечатление – попытка ограбления, но, с другой стороны, грабить-то там нечего!

– Личность грабителя установлена?

– Да. Это некий Микки Р. Следователь увидел его, когда он проник в квартиру, и заметив в руке грабителя предмет, похожий на оружие, выстрелил. Конечно, жаль, что он так хорошо стреляет, но прокурор уже оправдал его.

– Что было найдено при нападавшем?

– Пистолет калибра 9 мм, он проходил по делу об ограблении ювелирного магазина год назад. Из этого пистолета был убит полицейский.

– Что еще?

– Одноразовый телефон, на который трижды звонили с одного и того же номера. Последний звонок был за 10 минут до убийства.

– Вы отследили номер звонившего?

– Да. Но, увы, это такой же одноразовый телефон.

– Отследите его маршруты передвижения за последнюю неделю. Особо интересно, где он находился в ночное время.

– Уже сделано! При этом отличился стажер из Академии. Телефон в ночное время находился в районе 21-й улицы. Там мотель «У дороги». Кроме того, каждый день с 9—00 до 10—00 он находился в кафе «Три поросенка», видимо хозяин там завтракал.

– Вы звонили по этому номеру?

– Нет! Боялись что-то не так сделать.

– Попробуйте и доложите.

Прошло полчаса.

– Господин комиссар, после нашего звонка телефон был выключен. Увы. Но зато сразу же по тем же координатам включился еще один. Мы уже установили за ним наблюдение. Кроме того, мы выяснили что в мотеле «У дороги» установлены потайные видеокамеры, которые передают изображения и номерные знаки всех автомобилей, на которых приезжают постояльцы. Мы обратили внимание, что вместе с появлением известного номера телефона в мотель регулярно приезжал черный седан с номером NN9980. Этот автомобиль принадлежит мелкому наркоторговцу, который уже привлекался полицией. Я выслал за ним наряд. Его уже привезли.

– Ты возил пассажира в мотель «У дороги»?

– Я, а что, это нарушение?

– Кто приказал? Ну!

– Приказал Муса, он мой поставщик. Я должен ему денег. Он сказал: сделаешь, и ты мне ничего не должен.

– Сможешь описать пассажира?

– Конечно. Я готов.

– Где сейчас телефон?

– В забегаловке «У моста». Уже минут 30.

– Там есть камера?

– Там нет. Но есть в отделении банка. А она как раз за-

хватывает вход в забегаловку.

– Посмотри, кто входил туда в момент, когда там появился нужный телефон и сравни с нарисованным портретом.

– Вот он!

– Распространи и опергруппу на выезд.

– Уже.

Через полчаса преступник был арестован. Это оказался находящийся в розыске Джонни Д. Именно он должен был убить следователя, но нанял вместо себя другого исполнителя. А сам задержался, чтобы закончить начатое.

Так закончилось еще одно дело в комиссариате.

# Сказки о безопасности: Угон грузовика

– Иоганн, нам нужна помощь ваших специалистов.

– Что случилось на этот раз?

– Полиция жалуется, что на трассе, соединяющей порт со столицей, резко выросло число угонов грузовиков с товаром.

– Ну, вы смеетесь? Мы-то тут причем?

– Думаю, что как раз вы-то причем! Ведь угоняют грузовики выборочно. В первую очередь с дорогой электроникой и элитным алкоголем. Угоняют то, что дорого стоит и легко продать. Вам не кажется это подозрительным? А нам кажется.

– А где точка, в которой сходятся все сведения?

– Логистический центр. там все данные обрабатываются на сервере. И, насколько нам известно, там весьма слабая ИТ-служба.

– Тогда вы правы. Это к нам. Но нам нужны официальные полномочия для проверки компьютерной сети.

– С этим как раз проблемы нет. Выделяйте оперативную группу.

– Марк, ваша группа выделяется в помощь транспортной полиции. Вы должны проверить состояние компьютерной сети компании Sea and Logistic. Мне кажется, у них утечка данных по грузам и грузовикам. И заодно попробуйте разобраться, как все же угоняют грузовики, ведь они используют цифровые ключи.

– Задачу понял. Выезжаем.

Прошло два дня.

– Иоганн, а тут все весьма грустно! Серверное программное обеспечение не обновляли более года. Более того, серверные операционные системы, антивирусное программное обеспечение, да и многое другое просто ворованное! Мне кажется, против директора, ИТ- и ИБ-руководителей нужно открывать уголовные дела за халатность! Или как минимум уволить! Здесь куда не ткни, все друг другу родственники. Ужас какой-то.

– А что с грузовиками? Разобрались?

– Конечно. Практически все они на выезде останавливаются у маленького кафе, где водители покупают себе воду и сигареты. Там ежедневно стоят два неприметных автомобиля, пассажиры которых занимаются перехватом ключей. А на следующей стоянке грузовики и угоняют.

– Что посоветуете водителям?

– Ключи держать в фольге. Впрочем, Мэри предложила и другой вариант: укладывать их в пустую банку из-под пива или колы. Говорит, что так проще, фольга порвется, а банка целая. И перехватить ничего нельзя.

– Молодец! Объявите ей благодарность от меня!

Вот так и закончилась история с угонами.

# Сказки о безопасности: Пропавшее электричество

– Доброе утро, шеф!

– Доброе утро, Софи! Что-то у вас встревоженный вид. Что случилось? Проблемы?

– Действительно проблемы. У мамы в доме отключили электричество. Вернее даже не только у мамы, а по всему их микрорайону. Говорят, за неуплату. Но мама клянется, что в их доме платят все. Поможете разобраться?

– Софи, вы странный человек! Когда мы отказывали своим? Разве вы такое видели?

– Нет конечно! Но мало ли что…

– Не морочьте голову. Все наши персональные дела у меня на контроле. Передайте оперативникам мою просьбу лично разобраться и сразу же доложить!

Прошло два дня.

– Иоганн, свет восстановили. Как оказалось, в одном из домов была найдена майнинговая криптовалютная ферма, хозяева которой не платили за электричество, а воровали его!

– Лихо! И что, никто не слышал шум вентиляторов? Никто не обратил внимание, что там работают кондиционеры?

– Нет, думали, что там просто идет ремонт!

– Ваша мама подала в суд на владельцев оборудования? Если нужно, мы поможем с адвокатами.

– Думаю, что придется так и сделать. Что вы вообще посоветуете на будущее?

– Увы, спасение утопающих дело рук самих утопающих! Нужно смотреть за тем, кто завозит оборудование, и вообще,

внимательнее поглядывать вокруг. А пока жильцам нужно подать заявление в прокуратуру. Это поможет избежать обращения в суд со стороны энергоснабжающей компании.

– Спасибо! Так и сделаем!

***Увы, это не сказка. Подобные ситуации уже были в России. Так что будьте внимательнее!***

# Сказки о безопасности: Прочесть почту

– Доброе утро, шеф!

– Доброе утро, Рита! Я как раз собирался вас вызвать. Есть работа, но я пока не представляю, как ее выполнить. Нам нужно прочесть письма из почтового ящика Виктора Рэя. Но он использует двухэтапную аутентификацию на почтовом сервере компании М.

– Задание принято, а уж как – мы разберемся сами. Разрешите применить средства негласного съема информации?

– У вас разрешение императора на применение любых методов. Но все же желательно выполнить это максимально тихо, не привлекая внимания.

Прошла неделя.

– Шеф, вот вам искомая почта. Так как мы не знали за ка-

кой период, то выкачали все, что есть на сегодня.

– Молодцы, но как???

– Для выполнения задания мы решили клонировать сим-карту подозреваемого, на которую приходит СМС в виде второго фактора. Но не тут-то было. Оказалось, что СМС приходит не на основной его номер, а на предоплаченную карточку, которая не зарегистрирована на него. Тогда, уточнив, что в доме он проживает один, мы использовали фальшивую базовую станцию и воспользовались ею в один из дней, когда в доме он был один. В результате мы получили номер его второй сим-карты. И клонировали ее.

– И что вам это дало?

– Компания М позволяет воспользоваться не только двухэтапной аутентификацией, но и организовать нечто типа структуры одноразовых паролей (One Time Password – OTP).

– Поясните.

– Для входа на почту можно запросить только «второй фактор», без ввода пароля. Именно этим мы и воспользовались. В результате мы получили СМС на клон сим-карты и вошли в аккаунт. Ну а затем просто выкачали все письма. Если потребуется, это можно повторить в любое время.

– Молодцы. А знаете, как от этого защититься?

– Конечно. Использовать в качестве второго фактора аппаратный ключ. Тогда бы мы ничего не смогли сделать без физического доступа к этому ключу.

***Такая атака на почтовый сервис компании Microsoft***

***уже реальность. Впрочем, начиная с версии 1809 уже существует и средство защиты!***

# Сказки о безопасности: Когда лучше не двигаться

Утро солнечного выходного дня началось с резкого телефонного звонка.

– Питер, срочно подъем. На 19-й улице разбойное нападение на ювелирный магазин. Взяты заложники. Короче, машина уже у подъезда. Подъем, солдат!

– Ну вы окончательно обалдели! Единственный выходной и тот испоганили. Комиссар, можно я не буду их арестовывать, а просто убью? Сволочи, такой сон испортили!

– Питер, хватит возмущаться! Подъем!

– Ладно! Уже встал! Умываюсь и спускаюсь. Но все же они сволочи!

– Да кто б спорил! Вперед, солдат! Служба не ждет! Заложники на тебя надеются!

Второй специалист по освобождению заложников был в отпуске, и Питер остался один. Потому, несмотря на формальный выходной, вариантов у Питера не было.

Прошло 10 минут. Вот и магазин. На окнах висели глухие шторы. Сколько внутри преступников, никому не известно. Как работать?

– Кто командир?

– Я!

– Доброе утро, Майкл! Что известно?

– Да в том и дело, что почти ничего. На связь они пока не выходили, требований не предъявляли. Мы даже не знаем, сколько их внутри.

– Ваши предложения?

– С нами тут стажер из Академии. У него есть предложение.

– Говорите, стажер!

– В магазине работают две точки Wi-Fi.

– И чем нам это поможет?

– Исследователи нашей Академии разработали новую систему, использующую для слежки окружающие сигналы Wi-Fi и обычный смартфон. С помощью смартфона мы можем локализовать местонахождение человека в доме сквозь стены, используя отражение сигналов Wi-Fi. Ведь для радиосигналов не существует дверей или стен. Они смешиваются, отражаясь от различных поверхностей, и с точки зрения Wi-Fi картина мира выглядит весьма смазанной. Движущи-

еся люди также отражают сигналы, однако, в отличие от статичных предметов, они не выглядят смазанными. Поэтому можно легко рассмотреть человека за стеной и определить его движения.

– Н-да… Я не успеваю следить за всеми разработками. Пора на учебу. Вы сами сможете помочь?

– Да. Я участвовал в этой работе, а все программное обеспечение для работы мы получили еще на прошлой неделе.

– Так почему вы еще здесь? Бегом в отделение! Занимайтесь! Если вам нужна помощь людьми или транспортом, скажите. В вашем распоряжении все службы нашего полицейского управления. А на период этой операции вам подчиняются все отделения города.

Прошло еще полчаса.

– Комиссар, мы смогли определить, что в магазине шестеро преступников, они находятся в основном зале, постоянно перемещаются и чего-то ждут. Сколько заложников, мы точно сказать не можем, так как они неподвижны. Точность распознавания около 99%.

– Стажер, вы уже получили высшую оценку вашей практики. Ребята, а теперь работа за вами. Вперед!

Через 10 минут все было закончено. В зале оказалось семеро злоумышленников. Один из них стоял на месте, и потому его невозможно было определить.

# Сказки о безопасности: Где взять деньги

Несмотря на солнечное утро за окном, все присутствовавшие в конференц-зале на совещании руководителей автомобильной компании N ощущали непонятную тревогу. Казалось, в зале вот-вот разразится гроза. Атмосфера накалялась буквально на глазах.

– Господин вице-президент, что у нас с выпуском автомобилей?

– Уже третий квартал подряд их производство растет. Не так быстро, как хотелось бы, но все же понемногу. Главное – не падает.

– Хорошо, а что с продажами?

– Думаю, на этот вопрос лучше ответит руководитель департамента продаж!

– Так пусть отвечает!

– У нас продажи остаются на том же уровне.

– Так на кой черт у нас растет производство? Вам не кажется, что такими темпами мы скоро будем производить все больше автомобилей «на склад»? Нам нужна прибыль, а она неуклонно падает! Нам нужны деньги! Или вам они не нужны?

– Господин президент, позвольте?

– Майкл, что вы можете сказать? Ваш ИТ-департамент не приносит прибыли, а сокращать там уже некого.

– Вот и я о том же. Самое ценное в мире, господин президент, это информация, которой мы владеем. И мне, кажется, пора перестать сидеть на мешках с золотом и жаловаться, что нам никто не платит!

– Погодите, Майкл, я не понимаю. Неужели ваши подчиненные научились видеть деньги там, где даже я их не вижу.

– Именно так, господин президент! В нашем распоряжении есть информация об образе жизни владельцев так называемых подключенных автомобилей, собранная с мобильных приложений и информационно-развлекательных

систем. Однако ценным активом также являются данные клиентов, собранные финансовыми отделами нашей компании.

Ведь на сегодня уже есть 100 млн. владельцев наших автомобилей. А значит, мы владеем их данными!

– Откуда?

– Они берут у нас взаймы деньги, когда покупают автомобили в кредит. Мы знаем, кем они работают. Мы знаем, женаты ли они. Как долго живут в своих домах, потому что все это указано в заявлениях на получение кредита. И это все мы знаем благодаря тому, что люди нам доверяют!

– Вы это серьезно?

– Вполне! Ведь несмотря на то, что мы пока не торгуем такими данными, они у нас есть! А значит рано или поздно до этого додумаются и наши конкуренты, и больше всего прибыли получит тот, кто первым это сделает! Главное не опоздать!

# Сказки о безопасности: Обманчивый поиск

– Потапыч! Можно к тебе зайти?

– Что снова произошло, Хрюша? Какие проблемы в это раз?

– У меня никаких, хочу, наоборот, тебя поблагодарить за науку. Я серьезно!

– Ты серьезно? Что случилось?

– В этот раз не у меня. Слава Богу и благодаря тебе, у меня

все хорошо! Неприятности случились у Хрюнделя.

– Да что ж случилось-то?

– Да все нормально, он придурок! Но все ж внимательный придурок!

– Да ты можешь пояснить?

– Решил он позвонить к себе в банк и нет чтобы посмотреть на номер на своей банковской карте, нет, полез в Интернет искать номер телефона. Позвонил он в банк, а на той стороне приятный женский голос ответил, мол, да, это банк, но прежде, чем мы сможем вам помочь, нам нужно идентифицировать вас. Назовите пожалуйста имя владельца карты, срок ее действия и кодовое слово. Он назвал. Тогда у него попросили полный номер карты, не последние 4 цифры, а полный номер. Он сделал и это. А уж когда попросили назвать CVV-код, используемый для подтверждения онлайн-транзакций, до него, кажется, дошло, и он просто положил трубку. Говорила я ему говорила, что нужно быть внимательнее, а он все такой же. Спасибо тебе, что ты меня научил!

– Да уж! Давай я постараюсь понять, почему он дозвонился не на тот номер.

Прошла неделя.

– Хрюша, оказалось, что так «попал» не только твой Хрюндель, а и еще много народу. Проблема оказалась в сервисе Google Maps. Мошенники научились использовать его для собственного обогащения, выдавая с его помощью себя за сотрудников службы поддержки банковских организаций.

– Но как?

– Схема мошенничества настолько простая, что потенциальные жертвы сами связывались с мошенниками. Как оказалось, любой пользователь может назваться собственником того или иного предприятия, включая банковские организации, и изменить контактный телефон, который приводится в Google Maps, на свой. А поскольку сервис уделяет недостаточно внимания контролю за достоверностью сведений, возможность отредактировать информацию есть практически у любого.

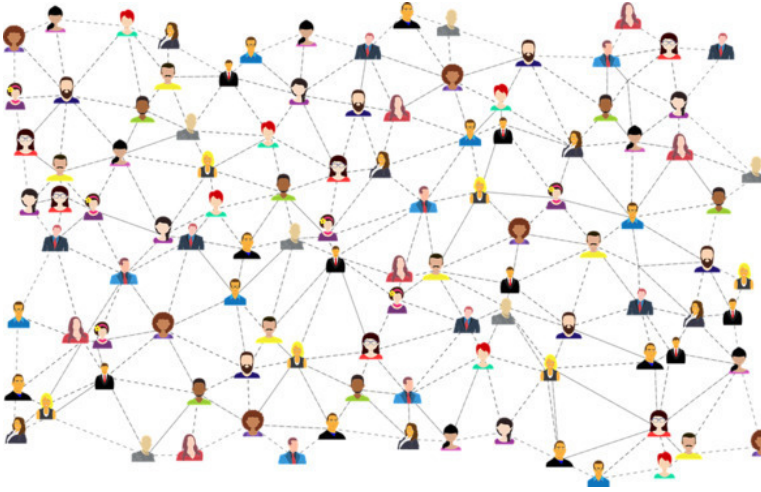
– О Боже! И что ж делать?

– На самом деле не все так страшно. Такая схема с подлогом телефонных номеров рассчитана на наименее осведомленных пользователей, которые ищут контактные данные своего банка в поисковой системе. Однако стоит учесть, что сегодня таких пользователей гораздо больше, чем тех, кто связывается со службой поддержки банка через чат в приложении или сразу заходят на официальный сайт в поисках телефонного номера или адреса электронной почты.

Потому запомни, если тебе нужна помощь, сразу запиши телефон службы поддержки своего банка или их веб-сайт. И не нужно искать его через разные поисковые системы. Короче, надо быть умнее и внимательнее. И не паниковать.

А сейчас пойдем спокойно попьем чаю с медом. Липовым! И не волнуйся!

# Сказки о безопасности: Дело о педофилах



– Иоганн, нам поставлена интересная и очень важная проблема. Как вы знаете, в последнее время участились случаи шантажа и даже похищений детей с помощью публикаций в детской социальной сети Safe Kids Net.

– Погодите, но ведь эта сеть исключительно для детей от 6 до 15 лет.

– Вы правы. Однако не так давно мы заметили в ней подозрительных посетителей. И, насколько я понял, совсем не де-

тей.

– ???

– Да все просто. Наши сотрудники с факультета психологии по нашей просьбе зарегистрировались там. И заметили, что через некоторое время к ним проявили нездоровый интерес два посетителя. Наши сотрудники говорят, что им кажется, что оба эти члена социальной сети совсем не дети. Но как это проверить? Не станешь же задавать вопросы.

– Конечно. А что говорят ваши психологи?

– Кто-то из них слышал о том, что когда-то в нашей Академии разрабатывалась интеллектуальная компьютерная модель, предназначенная для анализа текстов, публикуемых в соцсетях. Она вроде бы позволяла определять возраст написавших их лиц. Вы не могли бы узнать о судьбе этой разработки? Для нас, сами понимаете, это чрезвычайно важно!

– Безусловно!

Прошло два часа.

– Добрый день, Паула! Ты по-прежнему возглавляешь научный отдел Академии? Ты не против приехать к нам в гости? Есть вопросы.

– Да, конечно, только такси поймаю.

– Паула, какое такси? Я уже выслал к тебе оперативную машину.

– Даже так?

– Именно так! Все подробности при встрече. Да, ты по-прежнему любишь кофе со сливками и миндальное печенье?

– Иоганн, ты все помнишь!

– Мало того, печенье уже принесли! Жду!

– Иоганн, к вам Паула из Академии.

– Привет, Паула! У нас есть проблема. Кажется, вы занимались разработкой компьютерной модели, предназначенной для анализа текстов, публикуемых в соцсетях?

– Да. Это мой проект. Но тебе-то это зачем?

– Есть проблема. Похоже в детской соцсети завелись педофилы. Проблема серьезная. Мы сможем проанализировать тексты, написанные интересующими нас персонажами?

– Конечно. А в перспективе, я так понимаю, эта работа станет регулярной?

– Думаю да, а что?

– Здорово, потому как у нас на очереди новый проект. Он сейчас на завершающей стадии.

– И что на этот раз?

– Это метод определения профессии и образования. К работе над системой привлекли лингвистов, психологов и специалистов по анализу данных. На основе их заключений строится специальная математическая модель, которая опирается на корреляцию между численными значениями различных параметров текста и характеристик автора. Для создания этой модели потребовался машинный анализ огромного количества текстов, взятых в Сети, причем необходимым условием было наличие открытого профиля автора текста.

– А если он пытается это скрыть?

– Эта модель поможет вычислить демографические характеристики автора текста даже в том случае, если он намеренно пытается скрыть свой возраст.

– Ого! Таким образом фактически мы идем к полной деанонимизации в сети.

– Иоганн, ну ты же взрослый вроде мужчина. Ну какая, к черту, анонимность в сети?

Прошло две недели.

– Господин комиссар, на основании проведенного анализа мы можем сказать, что за перечисленными детскими профилями скрываются вполне взрослые люди. Более того, нашими подразделениями установлены их личности. Мы хоть сейчас можем провести аресты.

***Подобный анализ уже сегодня проводится на базе Курчатовского института. Так что анонимность в сети все чаще становится мифом. Помните об этом.***

# Сказки о безопасности: Дактилоскопический развод

– Привет, Потапыч!

– Привет, Хрюша. Что случилось? Опять проблемы?

– Ага, да вот только не у меня, а у Хрюнделя. Ты ж знаешь, мы купили ему смартфон. С тех пор он целыми днями играет на нем, я уже говорила тетушке, что так нельзя делать, но он нас не слушает.

– И что произошло на этот раз?

– В этот раз он непонятно куда просадил свои деньги. Клянется, что ничего не делал, но на счету денег нет. Думаю, что его элементарно обманули. Но вот доказать я не могу ничего.

– У него Android на смартфоне?

– Нет, мы специально купили ему iPhone, чтобы не думать о вирусах. Тетушка была этим сильно напугана и даже специально решила, что заплатит дороже, но, чтобы у Хрюнделя было все лучшее.

– Тем более странно. А какие приложения он устанавливал в последнее время?

– Я не знаю, какие-то игрушки, впрочем, если это важно, я пришлю к тебе Хрюнделя завтра с утра вместе со смартфоном.

– Договорились. Жду его с утра. Я позову своего знакомого, он специалист по смартфонам.

Настало утро.

– Хрюндель, что ты устанавливал на свой смартфон перед тем, как у тебя пропали деньги?

– Игрушку.

– Какую? Мне из тебя клещами тянуть все?

– Вот эту. А что?

– Что необычного было во время установки?

– Меня попросили все время держать пальцем по домашней кнопке своего iPhone, чтобы отсканировать мой отпечаток пальца для использования в игре.

– А ты, естественно, так и сделал?

– Да!

– Что скажешь, Ворон?

– Да что сказать? Его просто и элементарно обманули. Пока происходит сканирование, приложение запускает покупку в приложении, которая затем аутентифицируется с помощью Touch ID и завершается до того, как пользователь даже поймет, что происходит.

– Лихо! То есть он сам за все заплатил?

– Ну да. Причем ни один банк никогда не вернет ему деньги, ведь он сам все сделал. Нужно писать в компанию, чтобы удаляли приложение.

– А что ему посоветовать?

– Да что! Поменьше играть и быть умнее. Хотя, поможет ли? Не уверен!

***Согласно данным аналитической фирмы Sensor Tower, «дактилоскопическая» тактика злоумышленников оказалась чрезвычайно успешной. Приложение Calories Tracker в ноябре привлекло 60 тыс. долл., а Fitness***

*Balance – 10 тыс. Они уже удалены из App Store.*

# Сказки о безопасности: Слежка за автомобилями


– Иоганн, нам нужна ваша консультация. Что вы думаете по поводу электромобилей?

– Думаю, что при наличии определенной воли со стороны императора мы можем получить дополнительно новое средство наблюдения за гражданами страны. Да, у нас сегодня есть системы распознавания лиц, множество камер на дорогах, авторизация в мессенджерах и веб-сервисах – все это

позволяет полиции знать, что делает гражданин в конкретный момент времени. А теперь к числу этих инструментов мы можем добавить еще и электромобили.

– Да, но как мы это поясним гражданам?

– А зачем им что-то пояснять? Единственные, кому придется что-то пояснять, это производители электромобилей. Но им-то как раз пояснить все достаточно просто.

– Как?

– Заботой о покупателе, естественно. Ведь если все производители такого рода транспортных средств будут встраивать системы, которые каждые 30 с отправляют властям информацию о местонахождении машины, ее скорости и направления движения, то они всегда смогут оказать помощь покупателю за минимальное время. Ведь лучше производителя эту помощь никто не окажет. Ну а покупателю достаточно знать, что его координаты в случае чего будут передаваться на ближайшую станцию техобслуживания.

– Но тогда нужно будет договариваться не только с нашими, но и зарубежными производителями электромобилей.

– А куда они денутся, иначе не будем импортировать. И все.

– Отлично. Так и сделаем.

Прошло несколько лет. Чиновники говорили, что они используют данные для того, чтобы усилить безопасность пешеходов и автомобилистов, оптимизировать промышленное производство и инфраструктурное планирование, избежать

возможности обмана со стороны автопроизводителей, которые получают льготы со стороны государства.

И все было хорошо. Правда никто не знал, что вся эта информация с легкостью может использоваться и для других целей – например, установления местонахождения конкретного человека. А в перспективе электромобили следующего поколения будут отсылать властям и более персонализированные данные – например, что человек искал в навигационной системе, с кем он встречается, какие локации посещает.

Разумеется, был построен центр сбора и анализа информации. Он разместился в неприметном здании. Незачем привлекать лишнее внимание. Основной же офис располагается в подвале.

В офисе есть огромный экран, на котором отображается местоположение электромобилей – и картинка не статичная, все это постоянно изменяется, в соответствии с изменением местоположения машин. Если кликнуть на одну из точек-автомобилей, то можно получить все необходимые данные о транспортном средстве, включая модель, скорость, пробег и остаток заряда батареи.

– Иоганн, нам нужно отследить машину господина Д. Он использует электромобиль. Вот его госномер, марка, номер двигателя и кузова.

– Да, это все что нам нужно. Можем найти его прямо сейчас. Нам нужно буквально минуту. Господин комиссар, он едет по 5-й улице. Продолжить наблюдение?

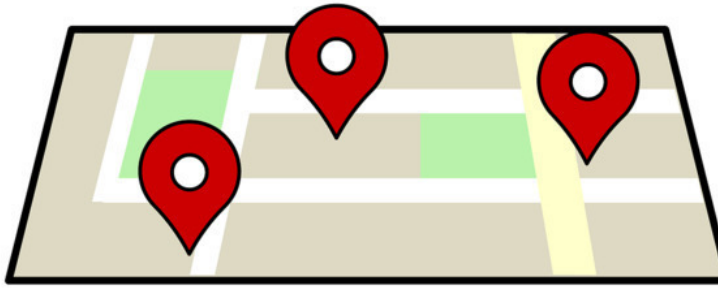
– Наша машина будет там через 5 минут. А мы можем его остановить?

– Безусловно.

Через 5 минут господин Д. был задержан полицией.

***Вы думаете это сказка? Совсем нет. Сегодня электромобили уже отслеживаются в Китае.***

# Сказки о безопасности: Загадочное уведомление



– Привет, Потапыч!

– Привет, Заяц! Что хотел?

– Да ерунда какая-то. Не могу понять. Поможешь?

– Не знаю, но попробую. А что случилось?

– Да вчера сидели с соседкой, вдруг ей приходит push-уведомление от Google Maps «Вы получили бесплатный приз от Google» и ссылка.

– Странно, конечно. Зачем Google рассылать какие-то

призы? Им и так хорошо. И что дальше?

– Когда она нажала на ссылку, оказалось, что оно от пользователя по имени You Have Received a Free Prize, и Карты предложили обменяться с ним местоположением. Я предложил заблокировать, и все на этом закончилось. Ты не сталкивался с таким? Интересно, а что произойдет, если доверчивый пользователь все же продолжит?

– Хороший вопрос. Не знаю. Думаю, что большинство пользователей отказываются предоставлять свои данные. Тем не менее, найдутся и те, кто согласятся указать местоположение. В основном, видимо, те, кто решат, что уведомления рассылают близлежащие магазины в рекламных целях. Я пока не понимаю, кто и зачем это рассылает, однако думаю, что ты дал правильный совет.

– Спасибо, Потапыч! Я помню, как ты нам рассказывал, что ничего не бывает бесплатным. Уж лучше и я моя подружка обойдемся.

– Ты прав. Лучше обойтись!

# Сказки о безопасности: Опасные куклы для взрослых

– Иоганн! Срочно приезжайте! За вами и вашими сотрудниками уже выслан транспорт! За Марком и Ритой, как наиболее далеко живущими сотрудниками, я выслал вертолет транспортной полиции.

– Да что случилось?

– Приедете, расскажу. Уж больно неприятная история. Прямо скажем, с душком.

– Еду.

– Итак, господин комиссар, что произошло?

– Вчера нашему секретарю имперской канцелярии пришло письмо от неизвестного злоумышленника. Он угрожает опубликовать некоторые компрометирующие фотографии и видеозаписи и требует предоставить ему копии секретных документов.

– А можно понять, где сделаны эти фотографии и видео.

– Можно. Сделаны они в новом салоне интимных услуг Robo-Dolls. Там вместо обычного персонала – роботы. Последнее поколение секс-кукол связывается с управляющим сервером, запоминает данные своего «пользователя», чтобы обеспечить более «индивидуальный подход». Ведь пользователи всегда хотят чего-то большего от своих гаджетов.

– Та-а-к, кажется, кто-то взломал эти куклы. Вы правы, это действительно дело нашего департамента. Посмотрим, что там такое.

– Макс, езжайте туда вы. Думаю, что Рите там будет не со-

всем приятно.

– Шеф, да какая разница? Куклы они и есть куклы, тем более мы туда работать едем.

– Хорошо, берите ее с собой. Сам понимаешь, дело строго секретное.

– Еще бы.

Прошел день

– Шеф, а ведь действительно, кукол взломали. Вернее даже не кукол, а канал связи между ними и сервером. Вообще, разработчикам хочется сломать руки и запихать их вместо ног. Идиоты! Как можно было сделать шифрованный канал и назначить вместо ключа шифрования серийный номер куклы, который пишется прямо на ее коробке. Я даже не знаю, как это назвать!

– Спасибо, Макс! Куклы нужно отозвать, пока не исправят программное обеспечение. И в дальнейшем разрешать их продажу только после того, как они пройдут сертификацию в нашем департаменте!

– Ну да, мы секс-роботов еще не сертифицировали.

– А что ты предлагаешь, Макс? Оставить как есть?

– Нет, конечно.

– А что со злоумышленником? Мы что-то знаем о нем?

– Да. Ребята уже связались с его провайдером, установили его место жительства. Вы не представляете, шеф! Этот идиот работал прямо из дома. Туда уже уехал наряд полиции, думаю они его уже привезли.

– Отлично! Давайте его сюда! Нам интересно, откуда он узнал о дефекте шифрования.

– Что вы можете сказать? Ведь вы же не программист. Откуда вы это знаете?

– Мой брат работает в компании-производителе кукол. Он говорил об этом дефекте, но руководство компании сочло, что вносить изменения слишком дорого. А через месяц моего брата просто уволили по сокращению. Он рассказал мне обо всем, и я просто украл у него это программное обеспечение. Он даже не знает об этом.

– Понятно, вы просто подставили его.

– Да! Но мне нужны были деньги.

– Ну а теперь вместо денег вы получите тюремный срок.

Вот так закончилась эта история. Думаю, что очень скоро подобное станет реальностью.

# Сказки о безопасности: Цифровой апокалипсис

– Иоганн! Срочно приезжайте! За вами и вашими сотрудниками уже выслан транспорт! В столице и вообще по империи – коллапс. В первую очередь транспортный. Все подробности по приезду.

– Да что случилось?

– Приедете, расскажу. Операция строго секретна. Всем

перейти на использование шифрованной связи.

Прошло полчаса.

– Все в сборе?

– Да, шеф!

– Пригласите комиссара полиции. Он доложит, что произошло.

Сегодня утром, а точнее 1 час и 45 минут назад более 30 млн. граждан империи, использующих мобильный Интернет, сообщили что они остались без доступа к Интернету. Мало того, о подобном сообщили наши посольства еще из трех стран. Мы не знаем, что это. Возможна массовая террористическая атака. Вам предстоит разобраться, что случилось.

– Н-да, еще три-пять лет назад это было бы просто небольшим раздражением, а тут чуть ли не угроза терроризма.

– Рита, ты, безусловно, права. Однако ты забываешь, что за это время среднемесячное использование мобильных данных в нашей стране выросло в двадцать раз, и владельцы телефонов используют их для всего – от потоковой передачи музыки до заказа такси и навигации.

– Согласна. Сегодня это цифровой апокалипсис.

– Именно так! Курьеры не могут доставить вовремя грузы. Заказать элементарную пиццу проблема. Таксисты не могут работать, ведь они опираются на навигационную систему, а она тоже не работает! Информационная система на столичных автобусных остановках вышла из строя. Мало то-

го, остановлена работа многих небольших компаний, работавших через Интернет. Это катастрофа! Люди блокированы от жизни, социальных сетей, банков, данных. В некоторых торговых центрах невозможно расплатиться карточками, а так как мы уже привыкли не иметь в руках наличных, то люди просто не понимают, что им делать!

– А что говорят операторы мобильного Интернета?

– А что они могут сказать? Обвиняют неназванного стороннего поставщика программного обеспечения.

– Иоганн, нам нужно получить доступ к сетям операторов мобильного интернета и связаться с этим «неназванным» поставщиком.

– Все уже готово, документы выписаны. Работайте!

Прошло четыре часа.

– Шеф, мы нашли причину. Она проста до банальности.

– А можно подробнее?

– Этим «неназванным» поставщиком оказалась фирма Е. Она уже принесла свои извинения и дала поразительное признание, что проблемой стал истекший сертификат клиентского ПО. А ведь чего проще было бы просто следить за сроком окончания сертификата!

– Проблема решена?

– Да. Они сейчас распространяют новый сертификат. Но, боюсь, на решение уйдет порядка 24 часов.

– Ну что ж, это лишнее свидетельство того, насколько мы зависим сегодня от Интернета.

# Сказки о безопасности: Рекламный путеводитель

– Иоганн, у нас проблема.

– Что, опять? Так надеялся хоть под Новый Год отдохнуть. Что случилось?

– Нам нужно отследить место встречи наркокурьера с покупателем.

– А что там такого сверхъестественного? Неужели ваши люди справиться не могут? Вы меня удивляете!

– Проблема в том, что явно мы не можем его вести, слишком велика вероятность обнаружения слежки. А не явно у нас не получается. Он ныряет в метро и все.

– Он не пользуется навигаторами?

– Нет!

– А что вы о нем знаете?

– Он договаривается о месте встречи через социальную сеть, приходит и ему там дают следующие координаты. И так несколько раз.

– Отследите его через сотовую связь.

– Ха! Мы так и хотели. Не получается. Он для связи использует мессенджеры и только общедоступные точки Wi-Fi, а по городу их полно. Не знаю, что и делать. Потому и пришли к вам на поклон. Думаете, нам так легко расписаться в собственном бессилии?

– Не думаю. Ладно. Что у нас на него есть?

– Есть MAC-адрес его смартфона.

– Ну, это уже кое-что. А какой социальной сетью он поль-

зуется?

– Сетью F.

– Так это ж в корне меняет дело. Все гораздо проще, чем я думал. Помните, мы организовали рекламную компанию T? Вы еще говорили, что это глупая трата денег. Помните?

– Я и сейчас так думаю.

– А зря! Совершенно зря! Социальная сеть F уже умеет прогнозировать «траекторию местоположения» пользователя, другими словами, определять место, куда он, вероятно, движется. Чтобы подсунуть соответствующую рекламу.

– И что нам это даст?

– Можно, например, сообщить ему, что кафе, куда он, скорее всего, направляется, закрыто на ремонт и предложить альтернативу. Если он примет это предложение, мы будем знать куда он идет, будем там раньше и перехватим его общение по Wi-Fi. Таким образом мы сможем его перехватить и в конечной точке.

– А кто ему даст эту рекламу?

– Комиссар, вы меня удивляете! Конечно, компания T. Собственно, для этого мы ее и создавали!

– Иоганн, вы и ваши сотрудники настоящие маги! Я, кажется, всерьез понял, почему вашего департамента боятся в полиции. Вы умеете найти выход, причем таким образом, который нам даже в голову не приходит. Поздравляю! И спасибо огромное, что вы играете на нашей стороне. Я беру свои слова обратно о компании T. И вообще, если вам нужна лю-

бая, я подчеркиваю, любая помощь от нас – обращайтесь! И вам и вашим сотрудникам!

– Спасибо! Ловлю на слове!

# Сказки о безопасности: Распознать лицо


– Иоганн, у нас проблема.

– Что, опять? Так надеялся хоть под Новый год отдохнуть. Что случилось?

– Вы уже слышали о стрельбе на 21-й улице? В баре «Под липой».

– Да, я прочел об этом утром, а что?

– Да там банда каких-то отморозков пристрелила мужчи-

ну. Но самое интересное не это. При нем найден смартфон. Мы вели этого курьера от самой границы и так бездарно потеряли. Проблема в том, что смартфон использует аутентификацию по Face ID. У нас нет времени ждать, пока вскроют этот смартфон, да и гарантии, что его вскроют, нет. Сможете помочь?

– Думаю да. Ирина, пригласите сюда Марка.

– Марк, нужно вскрыть телефон. Проблема в том, что мы ничего о нем не знаем. Он требует Face ID. А у хозяина выстрелом снесло полголовы. Сможем помочь?

– Думаю, да. У нас есть фотографии этого человека? Причем чем больше, тем лучше.

– Комиссар?

– Есть, конечно, причем сделаны разными камерами и с разных сторон. Я распоряжусь, и их вам немедленно доставят.

Прошло полчаса.

– Марк, вам пришло электронное письмо. Направлено на секретариат с пометкой «Марку, срочно!». От комиссара.

– Отлично, я его жду.

– Александра, будьте добры. Вы сможете сделать мне 3D-снимок головы по этим фото? В цвете.

– Безусловно. Пять минут.

– Марк, вот ваш снимок. Что сделать дальше?

– Распечатайте в натуральную величину на нашем 3D-принтере. Только в цвете.

– Понятно! А зачем, если не секрет?

– Будем подставлять эту голову смартфону. Попробуем его открыть.

Прошел еще час.

– Иоганн, с комиссара хороший кофе. С коньяком. И печенье, миндальное! Мы все сделали. Открыли смартфон, данные скачали. И знаем, куда направлялся курьер.

– Комиссар, примите мои поздравления. Мы вскрыли смартфон. Порядок!

– Мои поздравления вашим ребятам. А курьер с кофе, коньяком и печеньем уже в пути! Я сам приеду чуть позже.

***Это уже совсем не фантастика. С помощью гипсового слепка головы такие смартфоны уже вскрывали.***

# Сказки о безопасности: Дырявая оборона

– Иоганн, император приказал провести аудит наших систем противоракетной обороны.

– Хм, господин канцлер, я понимаю, что это необходимо. Однако, простите, мы-то тут причем? Это дело департамента обороны!

– Согласен, однако возникли проблемы. Нужен именно ИТ-аудит, причем независимый. Но сами понимаете, кого попало мы не можем пустить, это ведь совершенно секрет-

ные объекты. Так что придется поработать вашим сотрудникам.

– Согласен, но работать им придется в военной форме. Никто не должен знать, что это не специальное подразделение департамента обороны.

– Понимаю. Проверке подлежат как технические, так и организационные аспекты.

– А почему вообще встал этот вопрос?

– После запроса из канцелярии императора. Адмирал С., курирующий направление противоракетной обороны, выразил обеспокоенность состоянием критической инфраструктуры, обрабатывающей данные систем ПРО. А ведь эта информация включает, помимо прочего, результаты военно-космических исследований, инженерно-техническую документацию, спецификации и исходный код различных программ на службе вооруженных сил империи.

– Понятно.

Прошел месяц.

– Господин канцлер, аудиторы изучили ситуацию на пяти случайно выбранных объектах ПРО и выпустили два доклада с выводами.

– Ваши впечатления?

– Откровенно? Сказать бардак – это просто ничего не сказать! Серьезнейшие проблемы! Подрядчики не справились с контролем доступа, учетом и устранением уязвимостей. Армия не смогла защитить сети и системы, хранящие,

обрабатывающие и передающие технические данные систем ПРО.

– А можно подробнее?

– Легко, я пригласил сюда руководителей аудиторских команд. Прошу, Франц!

– Господин канцлер, Франц Игл! Руководитель аудиторской команды ВМС империи. Проверкой, проведенной на базе в Штромм, выяснено следующее. Персонал не использует многофакторную аутентификацию. Политика безопасности предписывает сотрудникам использовать для доступа к ИТ-инфраструктуре не только пароль, но и ключ, который нужно активировать в течение определенного срока после приема на работу. На практике этот период растягивается до бесконечности. Нам удалось найти сотрудника, который авторизуется только по паролю на протяжении последних семи лет. На одном объекте многофакторная аутентификация в сети оказалась вообще не предусмотрена. Таким образом, система уязвима перед фишинговыми атаками и хищением пароля.

– А может это только одна такая база?

– Увы, господин канцлер. Мы обнаружили незакрытые уязвимости ПО на трех из пяти объектов. Причем это уязвимости, патчи к которым выпущены от пяти до двадцати (!) лет назад! Как минимум на одной базе ИТ-служба не установила антивирус.

– Господин канцлер, позвольте и мне? Эдвард Трауб,

аудиторская команда ВВС. При проверке выявлено, что сотрудники трех баз ПРО не шифровали данные при копировании на съемные носители. По их словам, выполнить требование безопасности было невозможно из-за технической отсталости используемых систем – они не обладали необходимыми мощностями для шифрования, а на новое ПО у летчиков не было денег. Кроме того, руководители технически не могли контролировать соблюдение установленных правил.

И последнее, но самое удивительное. В дополнение к проблемам ПО на многих объектах обнаружились проблемы физической безопасности. В двух случаях посторонние лица могли проникнуть в серверные комнаты, где стояли открытые стойки с оборудованием, что позволяло потенциальным злоумышленникам подключить к нему вредоносные устройства. Руководитель одной из этих баз не знал о необходимости закрывать стойки. В свое оправдание он заявил, что у них не бывает случайных посетителей. На втором объекте требование запирать серверы было размещено прямо на оборудовании, однако персонал игнорировал указание.

– А что говорят руководители?

– Они никак не прокомментировали наши выводы. Просто отказались!

– Да-а-а-а! Теперь я понимаю, что адмирал обрисовал положение еще в розовых красках. Прошу всех руководителей аудиторских команд быть на императорском совете. Докла-

дывать будете лично!

***А ведь это не совсем сказка. Проверка показала огромное количество недостатков в информационной безопасности баз ПРО США. И что с этим делать, пока никто не знает!***

# Сказки о безопасности: Взлом новогоднего праздника

По сообщению собственного корреспондента «Эльф Таймс» из штаб-квартиры «Мастерской Санты», корпорация

перенесла взлом и фишинговую атаку. В данный момент все последствия атаки устраняются.

«Мастерская Санты», мировой производитель игрушек со штаб-квартирой на Северном полюсе, насчитывает более 80 000 эльфов-сотрудников. Большая часть производства приходится на декабрь, но практически все работники заняты 364 дня в году, чтобы спроектировать, создать и упаковать более двух миллиардов игр и игрушек, которые потребуются для рождественского утра и Нового года.

# Первый признак беды

Отдел жалоб «Мастерской» гордится своим положительным рейтингом удовлетворенности клиентов. Очень редко звонки в департамент поступают вне напряженного декабрьского периода. Поэтому, когда в ноябре эльф Грамблс из службы поддержки клиентов получил звонок от обеспокоенного родителя, это вызвало у него крайнее удивление.

«В тот момент, когда эльф Грамблс сообщил мне о звонке одного из родителей, я понял, что это срочный вопрос и решать его нужно очень быстро. Маленький Джонни плакал и не мог спать, но после долгих уговоров он признался своему отцу, что Санта требует с него выкуп! Малыш получил электронное письмо с сообщением о том, что Санта заметил, что он плохо себя ведет, и поэтому решил его переместить из списка „хороших“ в список „непослушных“, если Джонни не заплатит ему 1400 долл. в биткоинах, – рассказал Эльф Бернар, руководитель „Мастерской“. – Отец Джонни был возмущен, но, подавив гнев стаканом чего-то достаточно крепкого, понял, что что-то тут не так! Поэтому он позвонил в службу поддержки, чтобы узнать, сможет ли он заставить Санту пересмотреть приговор Джонни или договориться о более разумной плате».

# Поиск компромисса

Эльф Бернар был очень взволнован. Как это могло произойти? Неужели кто-то получил доступ к базе данных «Хорошие и плохие» и выдает себя за Санту? Он понял, что нужно срочно звонить в эльфийское агентство безопасности, его главе, чтобы срочно сообщить о развитии событий и своем страхе перед взломом базы данных. К его удивлению, эльфийский агент Х ответил, что подозревает возможный источник нарушения.

«Эльфийский агент Х сказал мне, что в начале года эльф Глиттерпантс подал жалобу в службу поддержки, когда внезапно перестал работать его десктоп», – рассказал эльф Бернар. При осмотре эльф Гик из ИТ-отдела определил, что эльф Глиттерпантс получил электронное письмо, пересланное эльфом Уэлли из отдела упаковки. В электронном письме была ссылка, предлагающая 75% скидочный код на блестящие банты, поэтому эльф Глиттерпантс нажал на нее. После того, как он заполнил свою личную информацию на вебсайте, он получил всплывающее окно с просьбой ввести свое имя пользователя и пароль, чтобы обновить флэш и распечатать ваучер. Он так и сделал, и запустил скачанный файл. Через несколько секунд его экран погас, и он позвонил в службу поддержки.

Эльф Гик восстановил десктоп, провел антивирусное ска-

нирование и решил, что все хорошо. В соответствии с процедурой он уведомил эльфийского агента X об инциденте. Агент X принял заверения эльфа Гика в том, что машина была чистой. В то время он рекомендовал эльфам Глиттерпантс и Уэлли посетить тренинг по безопасности. Но, оглядываясь назад, эльфийский агент X признал, что должен был понять опасность веб-сайта, запрашивающего имя пользователя и пароль.

# Сканирование и защита системы

Эльф Бернар и агент X приступили к работе. Они рассмотрели все роли и полномочия пользователей и провели полную проверку своих систем. Сканирование выявило 100 867 незащищенных уязвимостей, сгруппированных и расставленных по приоритетам.

«Мы очень благодарны агенту X и его команде безопасности. Они не только помогли нам защитить нашу критически важную базу данных клиентов, но и предотвратили крупный инцидент. Мы защитили все ключевые системы и внедрили программу управления исправлениями. Я знаю, что многие люди говорят, что Санта – волшебник, но в этом году агент X проделал тяжелую работу, следя за тем, чтобы все милые девочки и мальчики получили подарки в это Рождество», – резюмировал эльф Бернар.

# Сказки о безопасности: Атака под Новый год

– Светлана Ивановна, мы получили из прокуратуры e-mail. В нем написано: «Вам необходимо провести аудит соответствия вашей компании требованиям по защите КИИ

в соответствии с Федеральным законом… В случае отказа к вам могут применяться статьи…» Куда его?

– Перешлите мне, распечатайте, учтите во входящих. И да, перешлите безопасникам, юристам и… Что такое КИИ?

– Судя по ФЗ это критическая инфраструктура

– О! Тогда разошлите членам Совета.

– Хорошо!

Все получившие письмо открыли его. Ну а как же, письмо-то из прокуратуры! Перешли по ссылке. А в это время где-то отославший его злоумышленник улыбался, потирая руки. Атака удалась! Злонамеренное программное обеспечение получил не только секретарь директора. На такую удачу никто и не рассчитывал. Запустить? Нет, не стоит, запустим позже, а пока… пока пусть спит зловред. Запустим на выходных или после Нового года, когда у всех голова будет болеть после праздников.

В типичной переписке между подразделениями начали появляться сотрудники и руководители компании, и всем стало казаться, что работа уже ведется… Сотрудники стали выдавать всякие перечни, отчеты и данные в «прокуратуру». Атака удалась!

***А вы проверяете получаемые письма? И даже под праздники? Неужели?***

# Сказки о безопасности: Как дети чуть не остались без новогодних подарков

Перед наступлением Нового года в резиденции Деда Мороза царила предновогодняя суета. Нужно было окончательно расфасовать подарки, определить, что кому, разобрать все новогодние письма. Все бегали как на иголках. В такое время канцелярия Деда Мороза всегда нанимала временных сотрудников, молоденьких неопытных эльфов. Самое сложное было обучить молодежь не путаться в переписке. С недавнего времени канцелярия перешла на электронную почту. Так было куда удобнее.

Однако до сих пор никто не уделял серьезное внимание паролям. Как-то работали и ладно.

Этим решили воспользоваться давние враги эльфов – злобные орки. Они решили, что если уж не могут помешать Деду Морозу доставить подарки, то хотя бы постараются перепутать их назначение. Но как это сделать?

– Рэй, что ты задумал?

– Да есть у меня гадкая идея. Там на приеме писем и сортировке сидит невнимательный эльф. Жутко невнимательный и ленивый.

– И что?

– На домашнем компьютере, который недавно взломали мои подчиненные, он использует пароль «123456». Уверен, что и на рабочем то же самое.

– Он что, совсем бестолковый?

– Ага!

– Это хорошая идея!

Решили и сделали. Пароль почты оказался действительно таким.

– Ура, давайте поменяем подарки и на этого придурка спишем.

Так бы все и получилось, но старый Снеговик, долго работавший в службе безопасности Деда Мороза, заподозрил неладное. Он запустил программу проверки паролей и выяснил, что пароль молодого эльфа не отвечал требованиям безопасности. Проверив письма, Снеговик обнаружил несоответствие и исправил все с помощью резервной копии.

Долго благодарил Снеговика Дед Мороз. А эльфа просто с позором выгнали с работы и заявили, что теперь перед началом работы пользователям будут разъяснять требования безопасности.

Так закончилась эта история.

***А вы используете сложные пароли? Точно?***

# Сказки о безопасности: Проверка мобильных устройств

– Иоганн, у меня к вам просьба! Личная. Ваши ребята смогут помочь?

– Ну что вы, Густав! Мы всегда помогаем тем, кто помогает нам. Что вы хотели?

– Мы вводим у себя мобильные устройства. Пользовательские, для менеджеров, работающих «в полях».

– И что тут плохого?

– Боюсь, чтобы не утекли персональные данные наших клиентов.

– Хорошо! К вам на работу будут отправлены два моих сотрудника, Таня и Пауль. Они попробуют разобраться. Их поддерживать будет подразделение Риты. Естественно, у вас никто ничего не будет знать. Хорошо?

– Спасибо огромное, Иоганн! Я ваш должник!

Прошло две недели.

– Иоганн, вы были правы, у них серьезные проблемы.

– Что вам удалось найти?

– Не мне, Тане.

– Докладывайте!

– Шеф, несмотря на то, что инциденты с нарушением сохранности данных могут показаться незначительными по сравнению с теми, в которые вовлечены настольные компьютеры, все же они могут представлять серьезный риск по другой причине: чем чаще не хватает памяти у таких устройств, тем больше пользователей хранят некоторые свои

приложения и файлы с данными в публичном облаке, а оно чаще всего не подконтрольно компании.

– Все верно, а если учесть, что в прошлом публичные облака, используемые пользователями мобильных устройств, уже пострадали от многочисленных атак, то такой сценарий вполне может иметь место.

– Мы также смоделировали атаку, использовав для этого поддельную точку Wi-Fi. Так как мобильные устройства компании находятся в постоянном движении, то взаимодействуют со многими сетями, не контролируемыми компанией. Самый распространенный случай – это открытые небезопасные Wi-Fi соединения в общественных местах. Кибер-преступники могут использовать такие сети для кражи с устройства конфиденциальной информации или даже для получения контроля над ним. Мы установили поддельную точку Wi-Fi с таким же значением SSID, как и подлинная точка доступа, в результате чего пользователь ошибочно подключался к поддельной сети, что позволило нам похитить конфиденциальную информацию.

– Что вы можете посоветовать для минимизации ущерба?

– Прежде всего сведение к минимуму рисков работы с данными на мобильных устройствах – это, как всегда, профилактика и, конечно же, уверенность в том, что сотрудники осторожны при обработке информации. Ну и использование специальных решений, отслеживающих все конечные устройства для того, чтобы обнаруживать аномальное пове-

дение при управлении файлами, содержащим данные.

– А что вы посоветуете в случае поддельных Wi-Fi сетей?

– Да в принципе то же самое. Повышение осведомленности сотрудников о рисках информационной безопасности для мобильных устройств – это, опять же, запрет подключаться к подозрительным Wi-Fi сетям и передавать конфиденциальную информацию и финансовые данные в общественных Wi-Fi. Но также нужно иметь решения безопасности, которые незамедлительно будут предупреждать пользователей в том случае, если сеть является подозрительной, еще до того, как они подключатся к ней. Ну а конкретные решения им должны посоветовать их специалисты по информационной безопасности. Мы ж не можем за них работать!

***Насколько серьезно вы относитесь к безопасности мобильных устройств? Или решили, что пока не до того?***

# Сказки о безопасности: Телевизор-соглядатай

Совещание у президента корпорации NCTV шло второй час. Речь шла о резком снижении прибыли.

– Что вы предлагаете? Мы и так внедрили огромное количество новых технологий, но наши конкуренты делают то же самое. И цены у всех практически одинаковы. Наши телевизоры ничем не отличаются от их. Да и не можем мы каждый квартал выкидывать на рынок что-то новое! Прибыль

составляет менее 5%. Еще немного и заводы придется закрывать! Что делать?

На столе президента пискнул телефон.

– Господин Джонс, к вам просятся срочно руководитель ИТ и руководитель службы информационной безопасности. Говорят, это очень срочно!

– Что нужно этим дармоедам? У меня совещание по вопросам продаж.

– Сэр, они говорят, что именно по этому вопросу им и нужно к вам, тем более что все ведущие менеджеры у вас. Просят уделить им 10 минут.

– Если снова будут просить деньги, то у меня их нет. Пусть зайдут!

– Добрый день, господа!

– Да какой к чертям добрый! Мы решаем, будет ли завтра существовать корпорация или нам закрывать продажи этих проклятых телевизоров. Где прибыль? А тут еще вы!

– Именно по этому поводу мы и решили вас побеспокоить! Мы подумали, что прибыль от продаж телевизоров может достигнуть 30—35%.

– Как это? У коммерческого директора идей нет, а у вас есть, а?

– Все дело в том, что мы айтишники, а он нет. А если серьезно, то мы готовы озвучить наши идеи и, если они принесут прибыль, а они принесут, вы делаете нас акционерами вашей компании, и мы получаем 10% от прибыли. Озвучи-

вать?

– Вы грабители!

– Увы, да. Но ведь мы решили озвучить идею вам, а не идем к конкурентам. Так как? 10 или 15%?

– Вначале 10, а там посмотрим!

– Хорошо. Ради чего телекомпании транслируют свой контент?

– Идиотский вопрос. Ради рекламы.

– Второй идиотский. А как считается эффективность рекламы?

– Весьма приблизительно.

– Ну а теперь подумайте. Наши телевизоры, в сущности, это компьютеры. Мы можем собрать информацию о том, кто именно смотрит тот или иной канал, какие передачи, какой провайдер это передает, в какое время, сколько времени зритель проводит на том или ином канале, его возраст, пол и т. д. Причем весьма точно.

– Но кто будет собирать эти данные?

– Как кто??? Наш телевизор! Причем весьма точно! Мы сможем собрать эти данные и продавать их как рекламодателям, так и провайдерам. Это огромный рынок! А телевизоры… Да кому нужно это железо? Продавать его можно по демпинговым ценам. Хоть по себестоимости, хоть даже ниже. Ведь основная прибыль у нас будет от продажи данных!

– Коммерческий директор, а вы куда смотрите?

– Но, сэр, я ж не айтишник!

– А надо! Пора!

***Смарт-телевизоры могут собирать о зрителях такую информацию, как время просмотра, просматриваемые телепередачи, реакция на рекламу и пр. А в период недавних зимних праздников стоимость 65-дюймовых моделей таких телевизоров (например, Vizio и TCL) с тонкими рамками, поддержкой сервисов потокового видео и форматов 4K и HDR составляла в США всего-то порядка 500 долл. Технический директор Vizio Билл Бакстер объяснил столь низкую цену тем, что некоторые производители телевизоров собирают данные о своих пользователях и продают их сторонним компаниям.***

# Сказки о безопасности: Опасный перезвон

– Потапыч, ты дома?

– Хрюша, ну если я трубку взял, то, где я? Конечно, дома! Что ты хотела? Как обычно неприятности? Приходи!

– Иду, Потапыч, бегу!

Прошло полчаса.

– Потапыч, привет! А вот и я! Ставь самовар. Я медку принесла и пирожков с творожком сладким.

– Та-а-ак, значит проблема серьезнее, чем я думал. Жалуйся!

– Да у меня ж есть племянник, Свин. Деньги у него со счета ушли. Позвонил ему кто-то неизвестный. Номер чужой, но его же оператора. Ну, Свин и решил перезвонить. Перезвонил, а деньги со счета ушли.

– Это известное мошенничество. Звонок на платный номер. Номер-то известен?

– Да, а что?

– Давай попробуем позвонить в службу безопасности вашего телефонного провайдера, может помогут чем.

– Давай.

– Алло, у нас проблема. При звонке на вот такой номер у нас ушли деньги со счета. Сможете помочь?

– Нет. Это официально платный номер. Это официальная услуга, вы ж сами перезванивали.

– Да, но почему вы не предупредили, что это платный номер?

– А мы не предупреждаем, извините, это ваши неприятности. Удачного дня.

– Ну что, Хрюша, слышала? Могу только одно сказать. Не знаешь, кто это, не перезванивай. Нужно будет – еще раз позвонят.

– Ой, Потапыч, смотри. Мне SMS пришло. Предлагают посмотреть мои фотографии с корпоратива.

– Не вздумай открывать ссылку. Ты знаешь этот номер?

– Нет, а что?

– Не знаешь – не переходи! И даже если знаешь, перезвони владельцу номера, спроси вначале. Мало ли, вдруг его смартфон взломали. Будь умнее. А то останешься без денег.

– Ой, спасибо, Потапыч! Выручил меня! Буду помнить и Свину расскажу.

***Вот такая история может случиться и с вами. Будьте внимательнее. Эпидемия ссылок в SMS не так давно прошла в Молдове. Хотелось бы, чтобы вы только читали об этом, но не стали сами жертвой такого мошенничества.***

# Сказки о безопасности: Несчастный блогер

Линда считалась самой хорошенькой девушкой их

небольшого городка. Впрочем, и не только городка. Она успешно вела свой блог в инстаграме и зарабатывала на этом деньги путем показа рекламы известных брендов. Ведь у нее было более 40 тыс. подписчиков во всем мире. Однако все шло хорошо до тех пор, пока ее учетную запись не взломали. Хакер получил доступ к странице девушки, ее электронной почте и банковскому счету. Она три дня пыталась добиться помощи от службы поддержки соцсети, но у нее ничего не вышло.

– Джо, я не знаю, что делать? Я написала и позвонила им раз сто, но они мне так и не помогли. Что мне делать??? Ведь это годы работы и единственный мой источник существования.

– Что я могу сказать, Линда, я позвонил своему брату, он работает в крупной компании-разработчике средств информационной безопасности, он попробует помочь. Ты ж читала, что в последнее время хакеры поняли, насколько для популярных блогеров важны их страницы в инстаграме? Тем более для некоторых реклама в этой соцсети – единственный источник дохода. Именно поэтому вас и стали все чаще взламывать.

– Но как?

– Брат говорит, что обычно все происходит так. Хакер присылает блогеру письмо, в котором представляется рекламодателем, предлагает сотрудничество и оставляет ссылку на свой профиль. Ссылка на самом деле фишинговая и ве-

дет на фейковую стартовую страницу инстаграма. Как только жертва фишинга вводит логин и пароль, их сразу видит хакер. Он входит в аккаунт популярного блогера, меняет адрес электронной почты и пароль, закрывая доступ к странице. Затем требует выкуп – обычно около 300 долл. в биткоинах.

– Именно так у меня и было. Только попросили 400 долл. Но я читала, что даже оплата не гарантирует возвращение учетной записи.

– Конечно! Ведь они мошенники. Их задача получить деньги.

– Но что делать?

– Вечером брат сказал, что напишет, подождем. Боюсь, сервис поддержки нам не поможет, ведь они шлют только автоматически сгенерированные ответы.

– Да, несмотря на то что в инстаграме разработана специальная процедура для пользователей, это мало помогает. Непонятно почему.

Настал вечер.

– Линда, приходи в гости. Пришло письмо от брата. Он навел справки и предложил обратиться к какому-то Хосе. Да, там потребуется заплатить, но куда меньше, всего 50 долл., но по словам брата, он знает способы, позволяющие заставить поддержку среагировать на жалобу быстрее. Иногда для этого ему нужен доступ в электронную почту клиента, чтобы переписываться с поддержкой инстаграма от имени клиента. Он обещает вернуть тебе доступ к профилю. По словам бра-

та, это вполне реально, тем более платишь ты после возврата доступа.

– Да, но как?

– Говорят, он взламывает устройства самих хакеров и просто заставляет их отдать пароли. Кто знает. Но тебе ж какая разница? Он тебе дает твой пароль. И все. А как это делает – не наше дело.

***Такая история вполне реальна. Одни занимаются взломом, другие – взламывают взломщика.***

# Сказки о безопасности: Бойтесь красавиц, в сети говорящих

– Иоганн, спасибо за помощь!

– Да ну что вы. Это наша работа!

– Эта ваша работа многое приносит в дело повышения безопасности нашей страны! Передайте вашим сотрудникам мое искреннее восхищение!

– Служу империи!

– И отдельно подготовьте список людей, участвовавших в операции для награждения. Предупредите, что награды носить можно и нужно, а вот рассказывать за что еще долго будет нельзя.

Эта история началась год назад в кабинете Иоганна.

– Шеф, есть идея. Вы ж знаете о наших напряженных отношениях с республикой И?

– Конечно.

– До недавнего времени мы активно использовали для разведки местных жителей. Однако из-за повышенного внимания контрразведки республики И эта деятельность практически прекращена. Увы, наши агенты, впрочем, какие там агенты, так, мелочь, провалились, и нам приходится искать новые методы работы.

– Что вы предлагаете?

– Использовать для вербовки агентов среди военнослужащих республики И социальные сети. Районы, которые нас интересуют – это в основном горная и пустынная местности. Пойти некуда, развлечений практически никаких, вот и проводят время местные военнослужащие в соцсетях. Ну а там, почему бы им не познакомиться с очаровательными одино-

кими женщинами, почему бы не поговорить? Скучно же.

– Ну что ж, Клара. Как вы знаете, у нас в департаменте существует старый армейский закон. «Инициатива наказуема!». Подбираете сегодня себе 2—3 выпускницы Академии и с завтрашнего дня вы с ними прикомандированы к отделу военной разведки департамента обороны. Вы возглавляете это подразделение. Жду еженедельный отчет.

– Что? Вот так сразу?

– А вы как думали. Раз пришли ко мне, значит вы долго над этим думали. А раз так, вам и возглавлять подразделение.

Прошло еще погода.

– Как успехи, Клара?

– Я познакомилась в Интернете под именем Марины с молодым офицером армии республики И. Мы с ним часто разговаривали, подружились. Я представилась медиком из госпиталя города К республики И. Госпиталь тоже находится в удаленном гарнизоне. Постепенно мы становились все большими друзьями, он влюбился. Мне даже пришлось послать ему фото интимного характера. Нет, шеф! Не свое, конечно. Я вообще своих фотографий в сеть не выкладываю.

Короче, его удалось завербовать, и он отправляет мне конфиденциальную информацию об армии, в том числе фотографии танков и бронемашин, данные о вооружениях, координаты воинских подразделений.

Конечно, мы платим ему за передачу стратегически важ-

ной информации. Но по нашим меркам смешные деньги. Они ж там нищие по сравнению с империей.

– А как вы перечисляете деньги?

– С карточки одного из банков республики И, открытой на имя несуществующего гражданина. Эти деньги отправляем на счет брата военного, потом он переводит их на свой электронный кошелек.

– Отлично! Продолжайте работу!

***Ну а вы, уважаемые пользователи, помните, что на той стороне Сети человеком, с которым вы общаетесь, может оказаться не тот, кого вы предполагаете?***

# Сказки о безопасности: Обратная сторона кибербуллинга

– Потапыч! Срочно нужна помощь! Не мне!

– Хрюша, ты чего шла в такую погоду? Дождь, ветер! Нельзя чтобы ты еще и заболела. Ну-ка быстро чаю с малиной, да и ноги попарить еще не мешало бы. Ишь чего вздумала. Позвонить никак нельзя было?

– Да я такое узнала, что о телефоне даже и не вспомнила. Тут такое!!!

– Да что случилось? Рассказывай!

– Короче, в школе, где учится мой племянник, произошло чрезвычайное происшествие. Три великовозрастные дуры из выпускного класса выставили в социальной сети фотографию своего одноклассника, опубликовав его имя, фамилию, класс и школу.

– И что тут криминального?

– Слушай дальше. Они организовали голосование на тему «Кто за то, чтобы его убить?»

– Идиотки!

– Конечно. Причем самое интересное, что все они из благополучных семей, отличницы, прекрасно ведут себя в школе.

– Все равно, дуры!

– Да кто ж спорит? А ты сможешь прийти в школу и рассказать им, почему они дуры? И чем это грозит?

– Когда?

– А в субботу. Ты ж не работаешь?

– Приду. И ребят возьму с собой из отдела.

Вот и настала суббота.

– Добрый день, дети! К нам в гости пришел Потапыч. Он руководитель подразделения информационной безопасности в нашем банке.

– Добрый день. Я не буду долго пояснять, что меня привело к вам. Все и так понятно. То, что сделано, увы, не вернуть. Вы понимаете, что любые наши дела оставляют следы? Так вот. Если вы кому-то в школе сделали гадость, то пройдет год-два и это забудется. Увы, в Интернете это не так. Все что вы сделали, остается в памяти поисковых машин на долгие годы.

# Конец ознакомительного фрагмента.