

ОГЛАВЛЕНИЕ

Вместо предисловия. Киберпреступность
и киберполиция не имеют национальных границ 9

Введение 16

Глава I ИННОВАЦИИ В ПОЛИЦИИ

§ 1. Общие положения 19

 Прогнозирование
 и стратегическое планирование 22

 Технологии 22

 Партнерство и сотрудничество 23

 Законодательная работа 23

 Методы и подходы к инновациям 24

§ 2. Дроны: угрозы, инструмент, средства
доказательства. 26

 Дроны в руках преступников и полиции 27

 Дроны как инструмент полиции 30

 Развитие дронов 33

§ 3. Искусственный Интеллект (ИИ) 35

 Угрозы ИИ. 37

 Потенциал использования ИИ правоохранительными
 органами 42

§ 4. Робототехника и киберполиция 43

 Промышленные роботы 45

 Сервисные роботы 46

 Социальные роботы 47

Военные роботы.	47
Беспилотные автомобили.	48
Потенциальные возможности робототехники.	49
Осмотр подозрительных предметов.	52
Автоматизация анализа доказательств.	53
Роботы для уличных патрулей.	53
Преступники тоже используют роботов.	54
§ 5. Печать — 3D и 4D.	56
3D-печатное огнестрельное оружие.	59
Правовые подходы к напечатанному огнестрельному оружию.	62
3D-печать и интеллектуальная собственность.	64
Потенциальные возможности для полиции.	64
3D-печать. Доказательства.	64
3D-печать для копирования отпечатков.	65
3D-печать для уголовных расследований.	65
3D-печать для повышения безопасности полицейских.	66
Направления прогресса для полицейских органов.	67

Глава II КИБЕРПОЛИЦИЯ И КИБЕРПРЕСТУПНОСТЬ

§ 1. Международно-правовое определение киберпреступности.	69
§ 2. Киберпреступность.	85
Специализированное вирусное программное обеспечение.	90
Атаки на критическую инфраструктуру.	91
Кражи данных и сетевые атаки.	92
Крупнейшие в истории хищения данных.	93
Масштабы DDoS-атак увеличиваются.	95
Инструменты DDOS-атак легко доступны.	97
Взлом сайтов. Низкая эффективность и разнообразная мотивированность.	97
§ 3. Смычка киберпреступности и кибертерроризма.	97
Террористические группы в цифровом подполье.	98
Неэффективность террористических кибератак.	99

Джихадистские сети экспериментируют с криптовалютами	100
§ 4. Онлайн сексуальная эксплуатация детей	102

Глава III
АНОНИМНЫЕ СЕТИ, ТЕНЕВОЙ ИНТЕРНЕТ
И КРИМИНАЛЬНАЯ ОНЛАЙН-ТОРГОВЛЯ

§ 1. Анонимные сети и теневой интернет	114
Интернет	116
Темный «интернет»	119
Сеть Tor	120
§ 2. Типы преступлений в Darknet	122
Криминальная торговля	122
Преступление как услуга (СаaS)	122
Жестокое обращение с детьми	123
Экстремизм	123
Нелегальные финансовые системы	124
§ 3. Криминальная онлайн-торговля	125
Darknet-рынки	126
Активизация вторичных рынков	128
Наркоторговля продолжает доминировать в Darknet	128
Рынки Darknet утрачивают значимость для киберпреступников	129
Торговля контрафактными товарами	130
Торговля оружием процветает в Darknet	131
Украденные данные — главный товар в сети Darknet	132

Глава IV
КИБЕРПРЕСТУПЛЕНИЯ И ТЕЛЕКОММУНИКАЦИИ

§ 1. Понятие и история развития телекоммуникаций	133
Типы современных сетей связи	136
5G порождает ряд новых острых проблем для правоохранительных органов	139
Ряд понятий, используемых в современных телекоммуникациях	139
Законодательные ограничения	142

§ 2. Сущности современного мира телекоммуникаций	143
Умные города	143
Умные предприятия	145
Умный дом.	146
Робот (устройство)	146
Смарткар, или автономный автомобиль	146
Смартфон (персональное устройство)	147
Технологии проникновения коммуникаций:	
Фемто- и пиктосоты	147
§ 3. Виды мошенничества в сфере телекоммуникаций	148
Мошенничества с использованием доступа к абонентским терминалам	149
Доступ мошенников к личному кабинету клиента	153
Доступ к инфраструктуре телекоммуникационных операторов	153
Новые виды мошенничеств в телекоммуникационной сфере	154
Новое поколение сетей — новые угрозы	157
Физические атаки на телекоммуникационную инфраструктуру	160
Платежные мошенничества с использованием телекоммуникационной инфраструктуры и социального инжиниринга.	161
§ 4. Мошенничество в сфере финансовых технологий	167

Глава V
КИБЕРПОЛИЦИЯ И ИНТЕРНЕТ ВЕЩЕЙ

§ 1. Понятие интернета вещей.	176
§ 2. Интернет вещей — риски и угрозы	178
§ 3. Основные направления преступности с использованием IoT	187
§ 4. Киберполиция на защите интернета вещей	192

Глава VI
КИБЕРПОЛИЦИЯ ДЛЯ УМНОГО ГОРОДА

§ 1. Особенности умного города	205
§ 2. Риски умного города	208

§ 3. Киберполиция против новых рисков	210
Государственно-частное партнерство по обеспечению безопасности умного города.	214

Глава VII
КИБЕРПОЛИЦИЯ И ЦИФРОВАЯ ВАЛЮТА

§ 1. Цифровые валюты: определение, характеристики и пользователи.	218
Ключевые определения	218
Типы криптовалют, их особенности и пользователи	219
Примеры использования криптоактивов криминалом.	226
Централизованные виртуальные деньги	229
§ 2. Бэкграунд усилий по предотвращению отмывания денег и финансирования организованной преступности и терроризма через криптовалюты	231
ФАТФ и новые технологии	234
Реакция ЕС	238
Оценка рисков использования террористами и киберкриминалом виртуальных валют	243
Риски за пределами терроризма и организованной преступности	249
Конвергенция киберкриминала и терроризма	261
§ 3. Юридические и регуляторные механизмы борьбы с блокчейн-преступностью.	264
Саморегулирование	276
Рекомендации правоохранительным и законодательным органам	278
Закключение	283



*Заместитель Председателя правления
ПАО Сбербанк России,
кандидат юридических наук С.К. Кузнецов*

Вместо предисловия

КИБЕРПРЕСТУПНОСТЬ И КИБЕРПОЛИЦИЯ НЕ ИМЕЮТ НАЦИОНАЛЬНЫХ ГРАНИЦ

Рад представить вниманию читателей очень актуальную книгу двух генералов — докторов юридических наук *Юрия Жданова и Владимира Овчинского «Киберполиция XXI века»*.

Работа содержит самые современные оценки использования технологий новой промышленной революции как в преступных целях, так и в антикриминальной деятельности. Это касается технологий искусственного интеллекта, робототехники, дронов и целого ряда других инноваций. Но «красной нитью» по книге проходят проблемы киберпреступности.

По оценкам международных экспертов, сейчас в мире около 40 млн киберпреступников, а потери мировой экономики от их действий только в 2018 г. оценивались в 1,5 трлн долларов.

Новый файл с вредоносным кодом появляется в сети каждые 4 секунды, а одним из главных вызовов стали *утечки данных корпораций* в результате целевых атак на их сотрудников. Во второй четверти 2019 г. доля умышленных инцидентов с утечками данных выросла с 50 до почти 60 %, внешних атак — с 34,5 до 40,6 %.

С увеличением числа кибератак возрастает и причиняемый ими ущерб. В 2019 г., по прогнозу Сбербанка, общемировой ущерб уже достигнет 2,5 трлн долларов. К 2022 г.,

по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак может вырасти до 8 трлн долларов.

Одной из причин ускоренного роста киберпреступности, по мнению международных специалистов, является стремительное развитие технологий. К 2022 г. к интернету будет подключен один триллион устройств. К 2023 г. у 80 % людей появится аватар в цифровом мире. При этом более 50 % интернет-трафика домохозяйств в 2024 г. будут потреблять «умные» устройства и бытовая техника.

Проблема борьбы с киберпреступностью перешла за рамки узких форматов или отдельных стран и вышла на международный уровень. Киберпреступники уже давно не имеют национальных границ — в отличие от нас, тех, кто борется с ними. Поэтому эффективно противостоять киберпреступности можно, лишь объединившись, организовав эффективное, действенное сотрудничество государств друг с другом.

Кибератаки становятся все более разнообразными и все чаще направлены на новые технологии. Дополнительные риски создают различные облачные сервисы, а также популярный сегодня тренд BYOD (bring your own device), когда сотрудникам компании разрешается работать с личного компьютера или ноутбука, подключаемого к внутренней сети компании.

2019 год можно назвать *годом утечек*, которых происходит все больше как в России, так и в мире в целом.

Стабильно высоким остается количество DDoS-атак (distributed denial of service), когда систему намеренно перегружают огромным количеством запросов с разных адресов.

Отдельно следует сказать об интернете вещей (IoT) и 5G. С одной стороны, замечательно, когда ваш холодильник сам заказывает продукты, а чайник можно дистанционно попросить подогреть воду. Но надо понимать, что в таком случае и холодильник, и чайник, и любое другое устройство, имеющее доступ в интернет, **может быть использовано** для DDoS-атак. Причем вы как пользователь об этом даже не узнаете, да и вряд ли будете сильно задумываться о ки-

бербезопасности таких устройств, ведь в них не хранятся ваши деньги. В мире уже 8 млрд IoT-устройств, с каждым годом их количество будет расти, и, соответственно, мощность DDoS-атак также будет только нарастать.

Следует назвать еще два тренда. *Первый* — преступные группировки все чаще используют сложные сценарии атак, придуманные специально под конкретную отрасль или даже компанию. *Второй* — киберпреступники все активнее ищут не прямые пути доступа в инфраструктуру организации. Для этого они атакуют «цепочку поставок»: вместо того чтобы подбираться к хорошо защищенной компании, находят ее уязвимых партнеров и подрядчиков, заражают их сети, а через них — и основную цель атаки. Число таких атак в мире в 2018 г. выросло на 78 %.

К сожалению, чтобы проникнуть в инфраструктуру компании, не всегда нужно взламывать софт. Гораздо проще «взломать» сотрудника, который, сам того не зная, приведет преступника к нужным данным. Это касается, например, *фишинга*, на который сегодня приходится более 60 % атак на банковский сектор России и ряда европейских стран. **Фишинг** — это массовые рассылки о том, что вы, например, выиграли приз или можете пройти опрос и получить за это деньги. В таких письмах содержится ссылка на вредоносный сайт, внешне неотличимый от сайта известного бренда. Переходя по ссылке и вводя свои данные, пользователь заражает свое устройство вирусом.

Ежегодно Центр киберзащиты Сбербанка предотвращает более полумиллиона попыток отправить сотрудникам банка письма, содержащие вредоносные вложения или фишинговые ссылки. С начала 2019 г. специалисты Службы кибербезопасности Сбербанка выявили и отправили на блокировку более 4000 фишинговых ресурсов, схожих с сайтом Сбербанка.

Защиту клиентов Сбербанка от хищения денег обеспечивает *система фрод-мониторинга, основанная на искусственном интеллекте*. Она выявляет подавляющее большинство всех попыток мошенничества. 88 % от общего объема мошенничества в отношении наших клиентов составила так называемая «соци-

альная инженерия». Это опять-таки про то, что проще «взломать» человека, чем систему. Существуют десятки мошеннических схем, которые чаще всего сводятся к тому, чтобы под благовидным предлогом (разблокировка карты, компенсация за санаторно-курортное лечение и прочее) узнать у человека конфиденциальную информацию: данные его банковской карты, логин и пароль для входа, например, в Сбербанк-Онлайн.

Необходимо постоянно вести разъяснительную работу, рассказывать клиентам о том, что никому, даже сотруднику банка, ни при каких обстоятельствах нельзя сообщать любые данные карты, кроме ее номера. **Говорить о том, что пин-код от банковской карты или пароль от интернет-банка нельзя хранить на бумажке.**

В большинстве случаев система антифрода способна остановить киберпреступника — она анализирует все транзакции клиента и в режиме реального времени выявляет подозрительные операции, которые не соответствуют финансовым привычкам клиента. Например, когда пенсионерка Мария Ивановна, которая живет в Саратове и никогда никуда не выезжала, вдруг совершает финансовую операцию во Владивостоке, банк делает ей контрольный звонок, и выясняется, что это мошенники пытаются снять деньги с ее счета.

Но, к сожалению, основную часть мошенничества с использованием социальной инженерии составляют так называемые *«самопереводы»*, когда клиент самостоятельно совершает и подтверждает операцию под воздействием мошенника (например, перевод аванса за покупку с сайтов объявлений или из соцсетей), а в дальнейшем обращается в банк с жалобой на то, что его обманули.

Вывод очевиден: только технические средства, даже самые современные и эффективные, полностью защитит клиентов от «социальных инженеров» не могут. Поэтому нужно продолжать работу по повышению киберграмотности клиентов, усиливать это направление на уровне государства.

Суть кибербезопасности заключается в том, что это постоянная, ежесекундная работа на опережение, непрерывная «гонка вооружений», которая происходит по обе стороны

закона. И одна из ключевых составляющих этой работы — *обмен информацией*. С этим всегда непросто: кому захочется поделиться даже с узким кругом экспертов тем, что его «хакнули», да еще во всех подробностях описать процесс? Это тяжело, но если молчать — всем будет только хуже. Как говорится, все компании делятся на тех, кого взломали, и тех, кто еще об этом не знает. Необходимо, чтобы экспертное сообщество узнавало о таких взломах как можно раньше, чтобы в будущем их предотвращать.

Следует внимательно следить за всем, что происходит в мире кибербезопасности, обмениваться информацией с российскими и международными партнерами, совершенствовать средства мониторинга, развивать свои защитные технологии. В частности, Сбербанк разработал и использует собственную *Threat Intelligence Platform*, которая позволяет собирать и анализировать информацию о различных киберугрозах.

Надо бороться за то, чтобы *информационное сотрудничество стало отлаженным как часы механизмом для всех участников процесса: бизнеса, правоохранительных органов, государства*. И это сотрудничество должно быть *международным*, должно быть выше любой геополитики и любой бюрократии. Иначе в нем не будет никакого смысла, потому что киберпреступники могут атаковать любую компанию и гражданина любой страны из любой точки мира.

Ведущие преступные кибергруппировки транснациональны, и без международной кооперации их не вывести на чистую воду.

В России уже удалось сформировать основные контуры такого сотрудничества в финансовой сфере. К примеру, платформа обмена данными о киберугрозах, реализованная под эгидой *Ассоциации банков России*, сегодня объединяет порядка 70 финансовых организаций, включая крупнейшие финансовые институты страны.

В мировом масштабе тоже есть серьезные успехи. Активно действуют *Интерпол*, *Европол*. Ведет работу *Центр по кибербезопасности ВЭФ (Centre for Cybersecurity, C4C)*, официальное открытие которого состоялось во время ежегодной сессии

в Давосе в 2018 г. Это уникальная площадка для сотрудничества представителей крупнейших глобальных корпораций, ведущих игроков международного рынка кибербезопасности, представителей правоохранительных органов с целью выработки совместной стратегии по противодействию глобальной киберпреступности. Сбербанк является одним из партнеров основателей С4С и обладает постоянным местом в Наблюдательном совете центра.

Услуги кибербезопасности для внешних клиентов оказывает дочерняя компания Сбербанка BI. ZONE, один из признанных во всем мире лидеров в сфере обеспечения кибербезопасности. В числе ее услуг — исследование и анализ вредоносного программного обеспечения, расследование инцидентов кибербезопасности и быстрое реагирование на них, сбор информации о потенциальных угрозах, различные виды тестирований: на защищенность от методов социальной инженерии, на проникновение, на защищенность мобильных и веб-приложений.

Следует активно развивать *российский рынок страхования киберрисков*. Дочерняя компания Сбербанка «Сбербанк страхования» первой в России предложила массовые продукты по страхованию киберрисков.

Внедрение искусственного интеллекта (ИИ) кардинально упрощает многие рутинные задачи, стоящие перед подразделениями кибербезопасности. Количество данных экспоненциально растет, и справиться с этим может только ИИ, который берет на себя наиболее трудозатратные операции, включая круглосуточный мониторинг и отражение ежесекундных кибератак. Однако преступники тоже в курсе всех возможностей искусственного интеллекта. И они не только атакуют компании, применяющие ИИ, чтобы проникнуть в их системы, но и сами используют его для поиска уязвимостей, проведения фишинговых атак, обхода биометрической аутентификации и защиты, создания вредоносного программного обеспечения, подбора паролей.

Цифровой мир — это, безусловно, наше будущее, ведь прогресс необратим. Насколько этот мир будет безопасным — зависит от всех нас. И от государства, и от бизнеса, которые

должны выработать адекватное существующим киберугрозам законодательство, в том числе *международное*.

Россия, как и многие другие страны, видит решение в *разработке под эгидой ООН универсальной конвенции о борьбе с киберпреступностью*, которая учитывала бы современные реалии, принципы уважения прав человека, суверенного равенства государств и невмешательства в их внутренние дела.

Россия также рассчитывает, что подготовленный экспертами из РФ проект универсальной конвенции ООН о сотрудничестве в сфере противодействия информационной преступности станет своего рода отправной точкой для обсуждения.

Новая книга *Юрия Жданова и Владимира Овчинского* — хорошее подспорье для тех, кто ведет борьбу с современной киберпреступностью. Она анализирует мировой опыт в этом направлении и будет полезна всем, кто хочет знать о том, как защитить мир от киберугроз — чумы XXI века.

*Станислав Кузнецов,
Заместитель Председателя правления
ПАО Сбербанк России,
кандидат юридических наук*