1 Актуальность проблемы обеспечения киберустойчивости Цифровой экономики Российской Федерации в условиях роста угроз безопасности

В этой главе показано, что современные цифровые экосистемы и платформы Цифровой экономики Российской Федерации не обладают требуемой *киберустойчивостью* (англ. — *Cyber Resilience*) для целевого функционирования в условиях *разнородно-массовых кибератак* злоумышленников. К основным причинам данного положения вещей относятся высокая *структурная и функциональная сложность* названных киберсистем, потенциальная опасность имеющихся *уязвимостей и «спящих» аппаратно-программных закладок*, а также недостаточная эффективность современных моделей, методов и средств *обеспечения кибербезопасности* (англ. *Cyber Security*), *надежности* (англ. *Reliability*) и *отказоустойчивости* (англ. *Response and Recovery*). Предложена новая постановка задачи по *обеспечению киберустойчивости* (*Cyber Resilience*) Цифровой экономики Российской Федерации в условиях *разнородно-массовых кибератак*, в которой организация восстановления функционирования киберсистем в ходе деструктивных программных воздействий *упреждает* приведение к существенным или катастрофическим последствиям. Замысел обеспечения киберустойчивости здесь заключается *в придании* киберсистемам способности вырабатывать *иммунитет к возмущениям* процессов вычислений в условиях деструктивных воздействий по аналогии с *иммунной системой* живого организма.

1.1. Ландшафт угроз кибербезопасности

В современном ландшафте угроз кибербезопасности сложные целевые атаки (*Advanced Persistent Threat*, *APT*) специальных технических служб (и киберкомандования) ряда развитых стран мира сочетаются с другими известными кибератаками. Термин «APT-атака» получил широкое внимание

общественности после публикации в газете «Нью-Йорк Таймс» сообщения о проведенной против нее кибератаке китаеязычной группой *APT1* (*https://threatpost.com/inside-targeted-attack-new-york-times-013113/77477/*). Как правило, APT-атаки реализуются в течение продолжительного времени. При этом наряду с фишинговыми сообщениями и вредоносным ПО используются разнообразные методы социальной инженерии.

Рассмотрим основные приемы злоумышленников.

1.1.1. ИЗВЕСТНЫЕ ПРИЕМЫ ЗЛОУМЫШЛЕННИКОВ

Следует констатировать, что арсенал средств и приемов злоумышленников (рис. 1.1–1.5) пополнился новыми приемами и способами [304–307, 311–314].

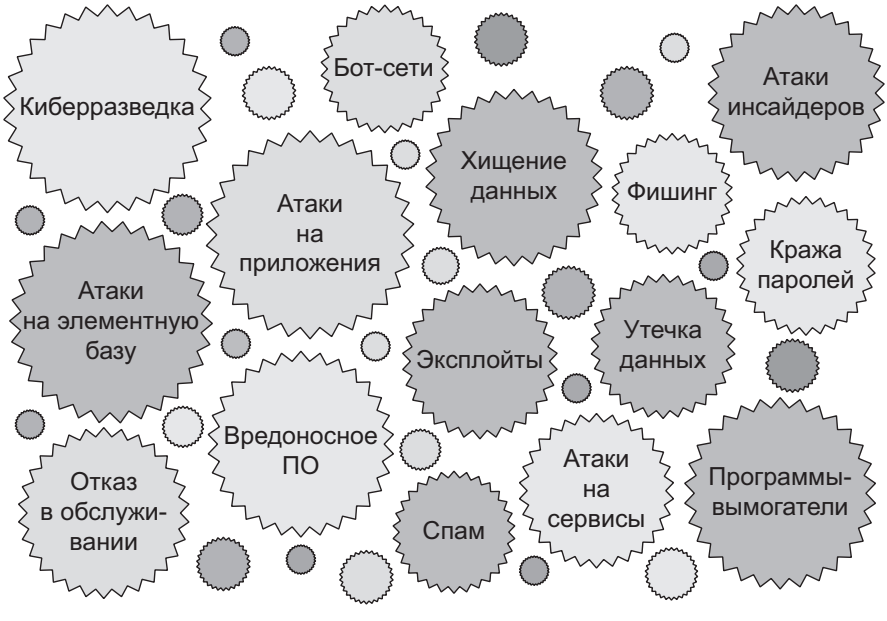

РИС. 1.1. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ ВИДЫ КИБЕРАТАК

Мобильные APT-атаки

В 2018–2020 годах были раскрыты шпионские кампании Zoopark, BusyGasper и Skygofree, главная цель которых заключалась в тотальном шпионаже за жертвами [113, 115, 140, 304, 305]. При этом использовались такие приемы хищения личных данных с мобильных устройств, как перехват звонков и со-

общений, несанкционированное подключение и съем данных геолокации абонентов и пр. В том числе была реализована функция прослушивания через микрофон: смартфон жертвы использовался в качестве «жучка» для записи конфиденциальных переговоров. Особое внимание было уделено бескомпроматному доступу и краже сообщений из большинства известных мессенджеров. В ряде случаев злоумышленники использовали эксплойты, повышающие локальные привилегии троянов (вредоносного ПО) на устройствах жертвы и открывающие доступ к удаленному наблюдению, а зачастую и управлению устройством. Кроме того, была реализована функция кейлоггера: злоумышленники записывали действия жертвы с клавиатурой устройства. Шпионская кампания Skygofree была реализована в Италии, BusyGasper — в России, Zoopark — в странах Среднего Востока. Явно прослеживается тенденция предпочтения преступниками, занимающимися шпионажем, мобильных платформ для планирования, организации и проведения кибератак [113, 114, 115, 304].

Эксплойты

Эксплуатация уязвимостей в аппаратно-программном обеспечении критической инфраструктуры остается важным средством компрометации устройств и ключевых компонент инфраструктуры [140, 305, 306, 307]. В 2018 году были обнаружены две серьезные уязвимости процессоров Intel — *Meltdown и Spectre*, которые предоставляют атакующему доступ к чтению памяти любого процесса и эксплуатируемого процесса соответственно. Они существуют как минимум с 2011 года.

Meltdown (CVE-2017-5754) затрагивает центральные процессоры Intel и позволяет атакующему читать данные в памяти любого процесса системы. Для эксплуатации требуется выполнение кода; его можно обеспечить разными способами, например путем эксплуатации ошибки в ПО или через посещение вредоносного веб-сайта, который загружает *JavaScript*-код, осуществляющий кибератаку. При успешной эксплуатации уязвимости могут быть считаны данные, находящиеся в памяти: пароли, ключи шифрования, PIN-коды и т. д. Производители оперативно опубликовали патчи для наиболее популярных ОС. Однако обновление Microsoft от 3 января 2018 года оказалось несовместимо с большинством известных антивирусов и на некоторых системах потенциально могло привести к BSoD. Обновление устанавливалось лишь в том случае, если был выставлен особый ключ в реестре, указывающий на отсутствие проблем с совместимостью.

В отличие от *Meltdown*, уязвимость *Spectre* (CVE-2017-5753 и CVE-2017-5715) эксплуатируется и на других архитектурах (AMD и ARM). Кроме того, *Spectre* может читать данные в памяти только эксплуатируемого процесса.

Большинство выпущенных патчей привели к сокращению поверхности кибератаки, уменьшив риск эксплуатации уязвимостей, но устранить угрозу полностью не удалось. Компания Intel выплатила премиальные $100 000 за обнаруженные новые процессорные уязвимости *Spectre* (CVE-2017-5753). Так, *Spectre 1.1* (CVE-2018-3693) может приводить к переполнению буфера, а *Spectre 1.2* позволяет перезаписать данные, доступные только для чтения, а также вызвать нарушения изолированных сред на процессорах, которые не применяют защиту памяти при чтении и записи. Эти новые уязвимости обнаружили Владимир Кирианский (МТИ) и независимый исследователь Карл Вальдспургер [113, 117].

18 апреля 2018 года на *VirusTotal* был инкогнито загружен эксплойт — новая уязвимость нулевого дня в *Internet Explorer* (CVE-2018-8174). В ходе исследования выяснилось, что он эксплуатирует полностью пропатченную версию *Microsoft Word*. При этом цепочка заражения выглядела так. Жертва получала вредоносный документ *Microsoft Word*, при открытии которого загружалась HTML-страница, содержащая *VBScript-код*. Далее инициировалась уязвимость *UAF* (*Use After Free*) и запускался шелл-код. Это первый случай, когда *URL Moniker* использовался для загрузки эксплойта *Internet Explorer в Word* [140, 161, 164, 170].

В августе 2018 года обнаружили новую кибератаку на основе эксплуатации уязвимости нулевого дня в *win32k.sys* — файле драйвера *Windows*, которая позволяла злоумышленникам получить контроль над скомпрометированным компьютером. Уязвимость применили при организации точечных целевых атак на организации в странах Ближнего Востока. Было обнаружено не менее десятка жертв, а цифровые следы привели к группе *FruityArmor*.

В конце октября 2018-го стала очевидна еще одна уязвимость Microsoft — уязвимость нулевого дня в *win32k.sys*, приводившая к эскалации привилегий, которые обеспечивали присутствие зловреда в зараженной системе. Эта уязвимость также эксплуатировалась в ограниченном числе кибератак на объекты и организации на Ближнем Востоке.

Вредоносные браузерные расширения

В 2018–2020 годах внимание специалистов привлекло вредоносное расширение *DesbloquearConteúdo* («Разблокировать содержимое» в переводе с португальского), предназначенное для кражи денег. Оно было нацелено на пользователей бразильских интернет-банков и собирало логины и пароли для получения доступа к банковским счетам жертв.

В сентябре 2018 года хакеры опубликовали личные сообщения минимум из 81 000 учетных записей *Facebook*. При этом они утверждали, что в их руки

попало гораздо больше информации, а именно — данные 120 миллионов учетных записей этой соцсети. В *DarkWeb* появилась реклама, где хакеры предлагали купить личные сообщения по 10 центов за учетную запись. Расследования компании *Digital Shadows* и Русской службы BBC показали, что значительная часть 81 000 учетных записей принадлежала жителям России и Украины, небольшая — жителям Великобритании, США и Бразилии. Представители *Facebook* предположили, что сообщения были украдены с помощью вредоносного браузерного расширения.

Вредоносные расширения встречаются довольно редко, но требуют повышенного внимания из-за потенциального ущерба, к которому могут привести [164, 170, 237, 238].

+35 %	Выросло количество DDoS-атак	**445** **млрд долл.** Ущерб от действий киберпреступников
58 %	От всего корпоративного трафика почты — спам	
+ 3,4 %	Выросло количество утечек конфиденциальной информации	
72 %	Выросло количество программ-вымогателей	

РИС. 1.2. ДИНАМИКА КИБЕРАТАК НА ФИНАНСОВЫЙ СЕКТОР ЭКОНОМИКИ

Методы социальной инженерии

Социальная инженерия — важный инструмент в арсенале киберпреступников. Это подтвердил чемпионат мира по футболу 2018 года в России [140, 248, 254, 257]. Задолго до начала этого важного события киберпреступники стали активно эксплуатировать данную тему в рассылках и создавать под нее фишинговые страницы. Одним из видов мошенничества стали рассылки-уведомления о денежных выигрышах в лотерею, а также сообщения о розыгрыше билетов на матчи. Мошеннические веб-страницы зачастую очень похожи на настоящие: они качественно проработаны и даже имеют *SSL*-сертификаты для большего правдоподобия. Мошенники выманивали у пользователей данные, имитируя официальные уведомления *FIFA*. Жертве

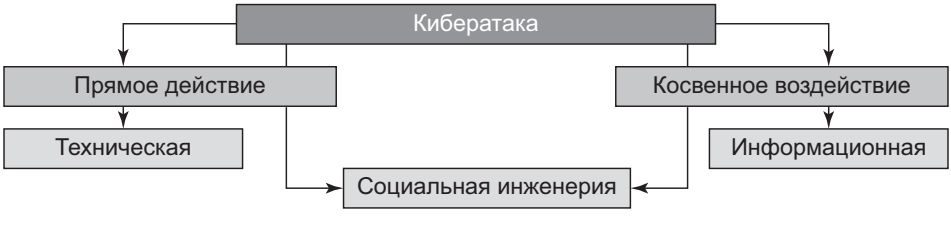

РИС. 1.3. РОСТ СЛОЖНОСТИ КИБЕРАТАК

сообщали, что обновлена система безопасности, поэтому, под угрозой блокировки аккаунта, нужно заново ввести сведения о себе. Ссылка из письма вела в поддельный личный кабинет, а оставленная там информация уходила к мошенникам (https://securelist.ru/2018-fraud-world-cup/90108/).

В преддверии чемпионата мира проанализировали почти 32 000 точек *Wi-Fi*-доступа в 11 городах, где проходили матчи [309, 316, 326, 330]. Оценив алгоритмы шифрования и проверки подлинности, подсчитали количество открытых сетей и сетей, защищенных по стандарту *WPA2*, а также их доли в общем количестве точек доступа. Выяснилось, что более 20 % точек доступа используют ненадежные подключения: преступникам достаточно оказаться рядом, чтобы перехватить трафик, а вместе с ним — пользовательские данные. Около $^{3}/_{4}$ всех точек доступа используют шифрование по стандарту *WPA/WPA2*, который считается одним из самых безопасных. Уровень защиты зависит в основном от настроек *WPA*, выбранных владельцем сети, в частности, от сложности установленного пароля. На подбор сложного ключа шифрования могут уйти годы. При этом даже сети, использующие надежные протоколы, такие как *WPA2*, нельзя автоматически считать полностью безопасными. Упомянутые сети уязвимы к кибератакам типа подбора пароля, переустановки ключей и пр. Перехватить трафик из общедоступной точки Wi-Fi с шифрованием WPA реально, если поймать «рукопожатие» между точкой доступа и устройством в начале сеанса (https://securelist.ru/fifa-public-wi-fi-guide/90142/).

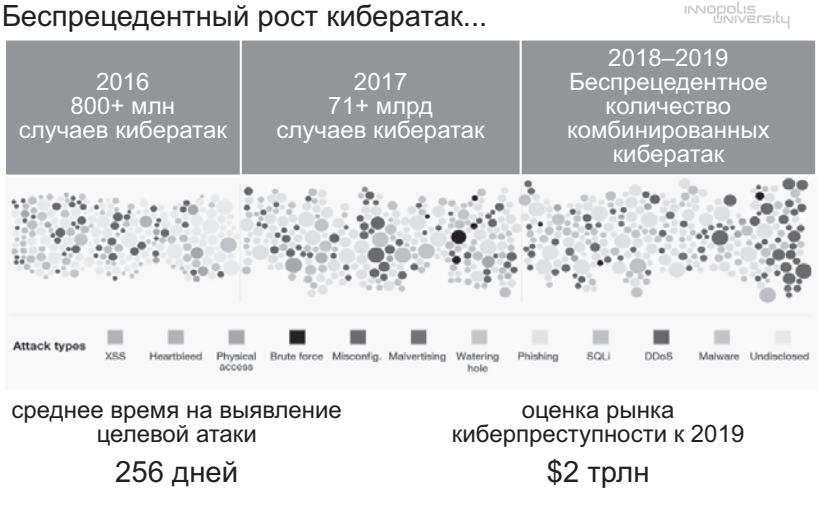

РИС. 1.4. ОЦЕНКА РЫНКА КИБЕРПРЕСТУПНОСТИ

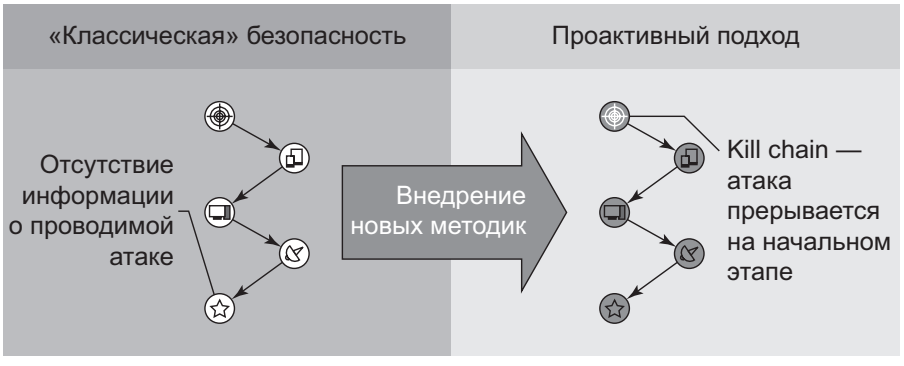

РИС. 1.5. ЭВОЛЮЦИЯ ПАРАДИГМЫ КИБЕРБЕЗОПАСНОСТИ

До 2000 года	Середина 2000-х годов	Начало 2010-х годов	Сейчас
Вся информация внутри периметра компании: • строительство «стен» вокруг компании • вся информация под тотальным контролем	Кибер-безопасность выходит за периметр компании: • аутсорсинг • информация остается под тотальным контролем	Понятие периметра исчезает с развитием облаков, BYOD, социальных сетей: • защита информации выходит за периметр компании • от обнаружения к предупреж-дению	Переход на новую парадигму «цифровая устойчивость»: • риск-ориентированный подход • гибкий подход к обеспечению информационной безопасности

РИС. 1.6. ОСНОВНЫЕ ПРИЧИНЫ ЭВОЛЮЦИИ КИБЕРБЕЗОПАСНОСТИ

Финансовое мошенничество

В 2018–2020 годах проявилась APT-атака (фишинговая кампания с октября 2017 года), направленная на кражу денег, преимущественно у промышленных компаний [332, 333, 334, 335, 336]. Злоумышленники использовали стандартные методы фишинга, обманом заставляли пользователей открывать зараженные почтовые вложения. Для этого письма маскировали под коммерческие предложения и другие финансовые документы. Киберпре-

ступники использовали легитимное ПО для удаленного администрирования — *TeamViewer* или *Remote Manipulator System (RMS)*. В результате было поражено более 800 компьютеров в 400 промышленных компаниях разной сферы деятельности: производство, добыча и переработка полезных ископаемых, энергетика и т. п. (https://securelist.ru/threats-posed-by-using-rats-in-ics/91624/).

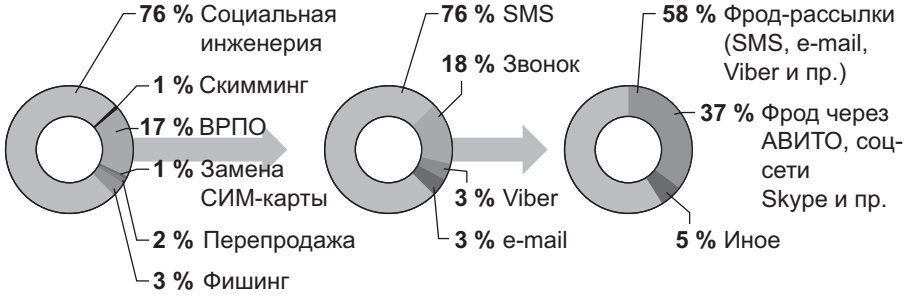

РИС. 1.7. ТИПОВЫЕ ПРИЕМЫ КИБЕРПРЕСТУПНИКОВ В ФИНАНСОВОМ СЕКТОРЕ ЭКОНОМИКИ

Программы-вымогатели

Программы-вымогатели по-прежнему угрожают пользователям. При этом появляются новые виды этого вредоносного ПО с требованиями выкупа [113, 115, 145, 149, 161].

В начале августа 2018 года в более чем 20 странах, включая Бразилию и Вьетнам, был выявлен троянец *KeyPass*, который шифровал большинство доступных файлов (ряд файлов игнорировался) на локальных дисках и в сетевых папках жертв. Для шифрования использовался симметричный алгоритм шифрования AES-256 (в режиме Cipher Feedback (CFB) с нулевым вектором инициализации) с 32-байтным ключом. Шифровалось максимум $0 \times 500\,000$ байтов (~5 МБ) данных в начале каждого файла. Зашифрованные файлы получали расширение **.KEYPASS*, и в директории, где они хранились, добавлялся файл *«!!!KEYPASS_DECRYPTION_INFO!!!.txt»* с требованием выкупа. Отличительной чертой KeyPass является возможность «ручного» управления: троянец позволяет злоумышленникам кастомизировать процесс шифрования, меняя такие параметры, как ключ шифрования, название и содержание требования о выкупе, идентификатор жертвы, расширение зашифрованных файлов и список директорий, которые следует исключить из шифрования [140, 145, 161].

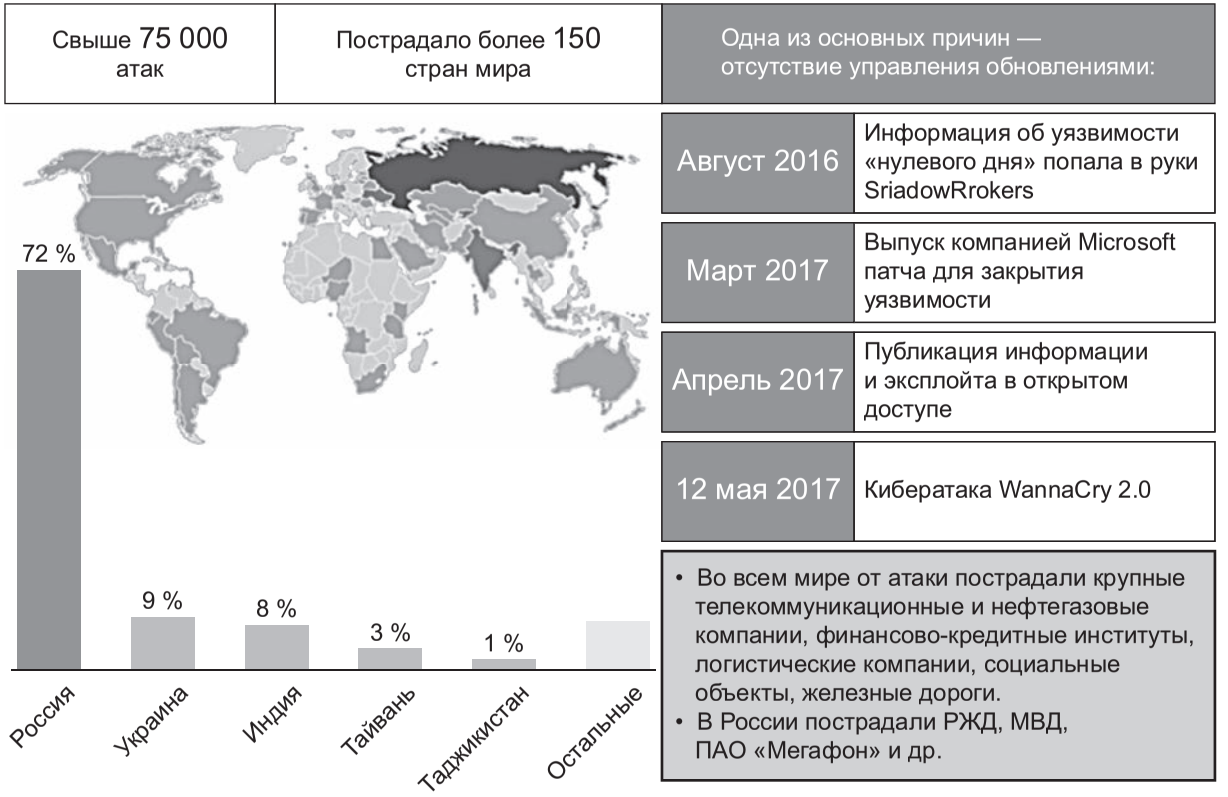

РИС. 1.8. ПОСЛЕДСТВИЯ КИБЕРАТАКИ WANNACRY

Отметим, что после эпидемии *WannaCry* (рис. 1.8) прошло три года, при этом зафиксировано более 75 000 кибератак на объекты и компании в 150 странах мира. Это вредоносное ПО остается в лидерах среди самых опасных шифровальщиков: заражений WannaCry — более 30 % от общего числа и процент неуклонно растет [113–117, 304–307].

Проблемы безопасности «умных» устройств

Сегодня мы окружены «умными» устройствами — бытовой техникой (осветительные приборы, телевизоры, утюги, кофеварки, датчики температуры, детские игрушки), а также счетчиками для сбора и обработки данных ЖКХ, медицинскими устройствами, камерами видеонаблюдения и пр. Появляются «умные» железные дороги, нефтеперерабатывающие заводы, города и даже регионы. У этого многообразия, однако, есть оборотная сторона: чем больше «умных» устройств, тем шире поверхность кибератаки и больше возможностей для злоумышленников [1, 4, 6, 8]. Обеспечить безопасность «умных» киберсистем еще сложнее, когда дело касается Интернета вещей (IoT/IIot), — из-за низкого уровня стандартизации разработчики уделяют мало внимания кибербезопасности. Это легко продемонстрировать на следующих примерах.

В 2018–2020 годах Kaspersky Lab ICS CERT опубликовала ряд исследований о том, насколько уязвимы к кибератакам «умные» **концентраторы** (*SmartHubs*). Концентратор позволяет управлять работой других «умных» устройств в доме, получать с них информацию и передавать им команды. Управление осуществляется с сенсорного экрана, через мобильное приложение или веб-интерфейс. Если в концентраторе есть уязвимость, он потенциально создает единую точку отказа. Изученный концентратор не содержал значительных уязвимостей, но нашлись логические ошибки, которые позволили злоумышленникам получить удаленный доступ (https://securelist.com/iot-hack-how-to-break-a-smart-home-again/84092/).

Также были проверены «умные» **камеры** — на предмет защищенности от хакеров. Такие устройства прочно вошли в повседневную жизнь [12, 21, 25]. Многие из них могут подключаться к «облаку», позволяя наблюдать за тем, что происходит в удаленной точке, — следить за животными, безопасностью жилища и т. д. Исследованная камера обладала значительным функционалом и могла быть использована в качестве видеоняни либо элемента общей системы безопасности жилища. Устройство имело функцию ночного ви́дения и датчик движения, могло передавать видео и звук на смартфон или планшет, а также проигрывать звук через встроенный динамик. При этом в ходе исследования на устройстве было выявлено более 10 уязвимостей — почти столько же, сколько у него функций, — позволяющих удаленно сменить

пароль администратора, выполнить произвольный программный код, собрать ботнет из скомпрометированных камер и вывести камеру из строя [41, 42, 44, 45].

Потенциальные проблемы касаются не только бытовых устройств. Так, Идо Наор, эксперт GReAT, вместе с Амихаем Нейдерманом из Azimuth Security обнаружили уязвимость в **средстве автоматизации для заправочной станции** (https://securelist.ru/expensive-gas/88566/). Это устройство имеет прямое подключение к Интернету и отвечает за управление всеми компонентами заправочной станции, в том числе топливораздаточной колонкой и платежными терминалами. Дальше — больше: оказалось, что в веб-интерфейс можно получить доступ, используя стандартный логин и пароль. Дальнейшее исследование показало, что злоумышленник может выключить все заправочные системы, вызвать утечку топлива, менять цены на бензин; красть деньги в обход платежного терминала, данные о номерных знаках машин и личные данные водителей, а также выполнить код на блоке контроллера и даже получить доступ к сети заправочной станции [60, 61, 62, 66].

В 2018–2020 годах были исследованы и «умные» **устройства для животных**, а именно — трекеры, устройства для отслеживания их местоположения. Такие гаджеты могут обладать доступом к сети, телефону хозяина и данными о местоположении животного. Целью исследования являлась оценка безопасности подобных устройств. Было проанализировано несколько популярных моделей трекеров на предмет потенциальных уязвимостей (https://securelist.ru/i-know-where-your-pet-is/89828/). Четыре проверенных трекера использовали технологию Bluetooth LE для связи со смартфоном владельца, но только один делал это корректно; остальные могли принимать и исполнять команды от кого угодно. Более того, оказалось, их можно вывести из строя или скрыть от владельца — для этого достаточно просто находиться рядом с трекером. Всего одно из протестированных *Android*-приложений проверяет сертификат сервера, не полагаясь на систему. Как итог — большинство трекеров подвержены атаке «человек посередине»: злоумышленник может перехватить данные, если «уговорит» жертву установить свой сертификат [68, 73, 75].

Также подверглись изучению **носимые устройства для людей**, а именно «умные» часы и фитнес-трекеры. Исследователей интересовал сценарий, в котором установленное на смартфоне шпионское приложение могло отсылать данные со встроенных датчиков движения (акселерометров и гироскопов) на удаленный сервер и из этих данных воссоздавать действия пользователя: ходьбу, сидение, набор текста на клавиатуре и т. д. Сначала для Android-смартфона было создано простое приложение, чтобы обрабатывать и передавать данные, а затем проведен анализ, что можно из них получить.

Выяснилось, что реально не только распознать, сидит человек или идет, но и различить, например, характер ходьбы — прогуливается он или переходит со станции на станцию в метро. Такое возможно, потому что каждому виду движения соответствует свой паттерн данных с акселерометра — благодаря этому фитнес-трекеры отличают ходьбу от езды на велосипеде [76, 78, 96, 97].

Последние годы растет популярность **сервисов краткосрочного проката автомобилей (каршеринга)**, которые сильно повышают мобильность людей в крупных городах. Однако возникает вопрос: насколько защищены личные данные пользователей подобных сервисов? В 2018–2020 годах были протестированы 13 приложений каршеринга на предмет безопасности (https://securelist.ru/a-study-of-car-sharing-apps/90804/). Результаты исследования не обрадовали. Судя по всему, у разработчиков приложений отсутствует понимание текущих угроз для мобильных платформ — как при проектировании приложений, так и при создании инфраструктуры. Для начала неплохо добавить функцию оповещения пользователя о подозрительной активности: на момент исследования лишь один сервис оповещал пользователя, если в его аккаунт пытались зайти с другого устройства. Большинство протестированных приложений оказались плохо продуманными с точки зрения кибербезопасности и нуждаются в доработке [98, 99, 107].

Количество «умных» устройств неуклонно растет: по некоторым прогнозам, к 2025 году их будет в несколько раз больше, чем людей на планете. При этом производители не уделяют достаточно внимания кибербезопасности: отсутствуют напоминания о необходимости сменить стандартный пароль при первой настройке и уведомления о выходе новых версий прошивок, а сам процесс обновления часто сложен для обычного пользователя. Все это делает IoT-устройства привлекательной мишенью для злоумышленников [108, 110, 111, 112]. Их проще атаковать, чем персональные компьютеры, а в домашней инфраструктуре они играют важную роль: одни управляют интернет-трафиком, другие делают видеозаписи, третьи управляют домашними устройствами, например установкой климат-контроля. Растет не только количество, но и качество вредоносного ПО для «умных» устройств. В арсенале злоумышленников появляется все больше эксплойтов, а зараженные устройства используются для организации DDoS-атак, кражи персональных данных и майнинга криптовалют (https://securelist.ru/new-trends-in-the-world-of-iot-threats/91601/).

Важно, чтобы вопросы кибербезопасности «умных» устройств (рис. 1.9 и 1.10) учитывались на первых этапах жизненного цикла (анализ требований и проектирование) [118, 120, 131, 134]. Отметим, что в некоторых странах появились соответствующие методические указания и рекомендации. Например, правительство Великобритании утвердило практическое руководство по обеспечению IoT-безопасности (https://www.gov.uk/government/

publications/secure-by-design/code-of-practice-for-consumer-iot-security), а правительство Германии анонсировало создание ряда стандартов https://www.theregister.co.uk/2018/11/20/germany_versus_openwrt_ccc/) по основам кибербезопасности таких устройств.

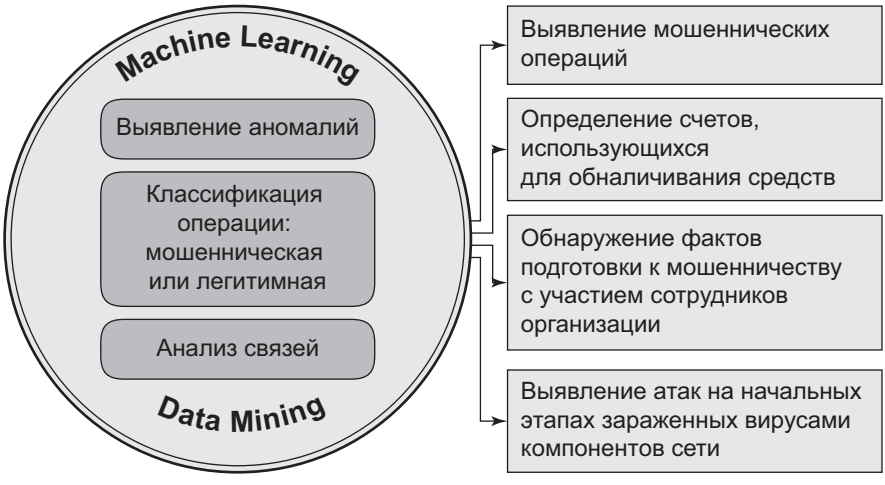

РИС. 1.9. ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ КИБЕРБЕЗОПАСНОСТИ

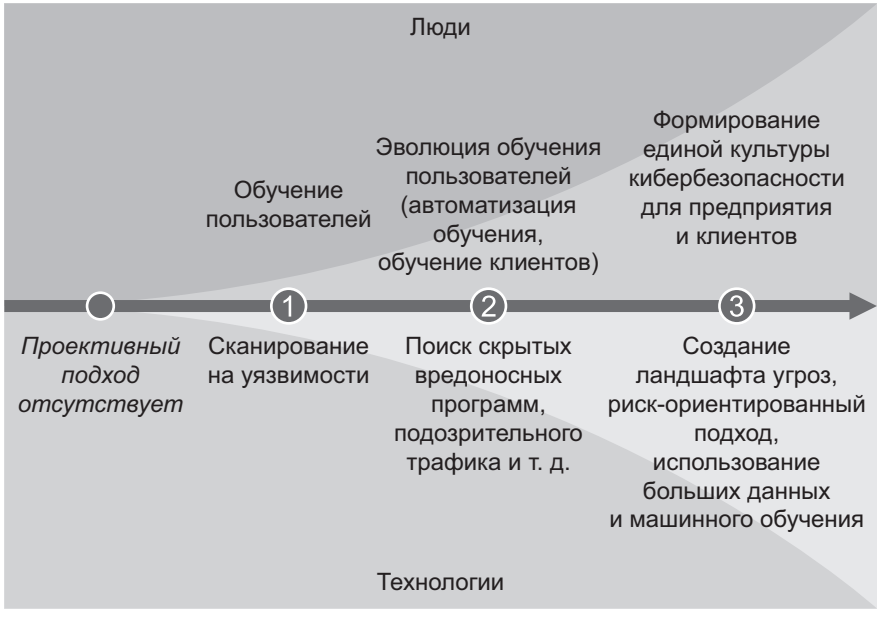

РИС. 1.10. ЦЕЛЕВАЯ МОДЕЛЬ КИБЕРБЕЗОПАСНОСТИ