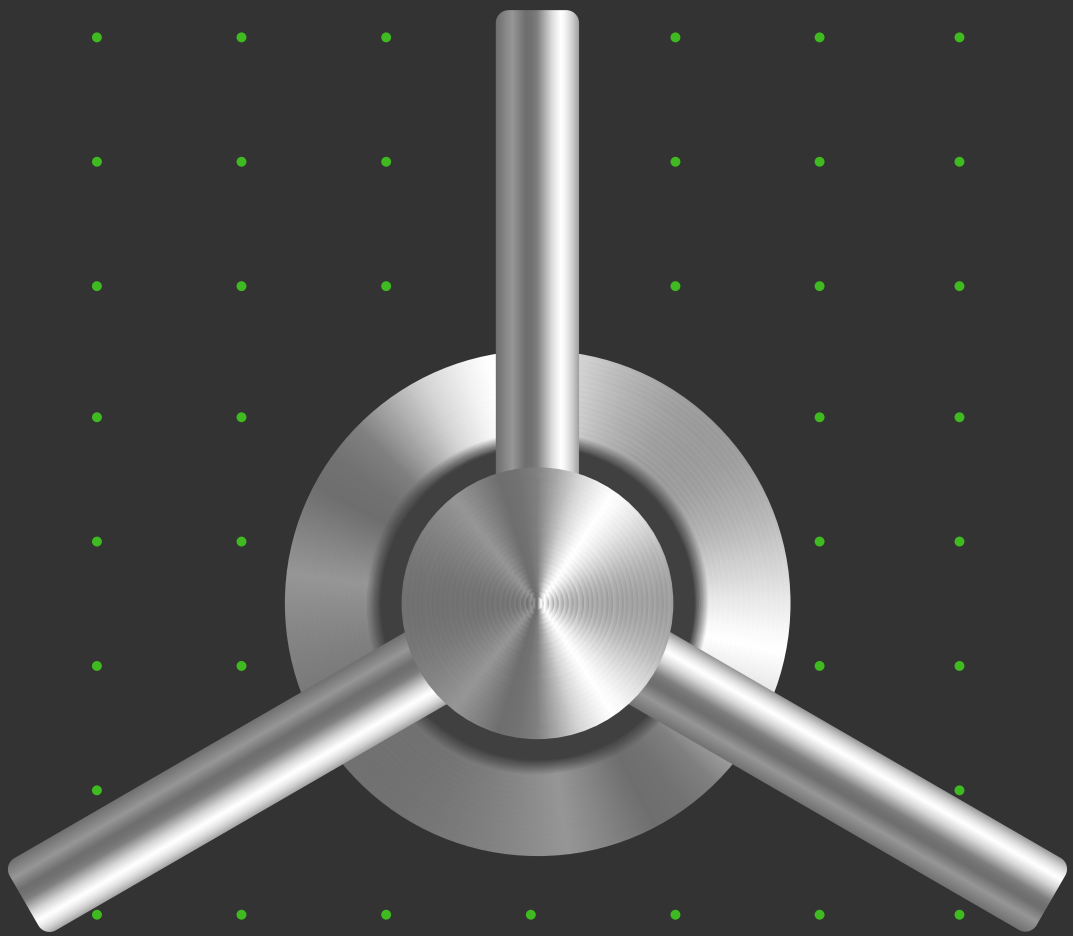
СЕКТОР
АНАЛИТИЧЕСКИХ
ИССЛЕДОВАНИЙ
УНИВЕРСИТЕТА ИННОПОЛИС



ДАННЫЕ БЕЗ ОПАСНОСТИ

Авторский коллектив:
Евсеев Константин, Исаев Михаил, Мурзина Алена,
Муфлиханова Анастасия, Шакирзянова Диляра

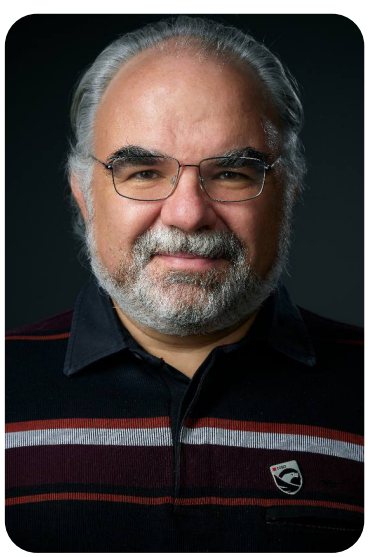
Научное руководство:
Бариев Искандер, Образцова Мария

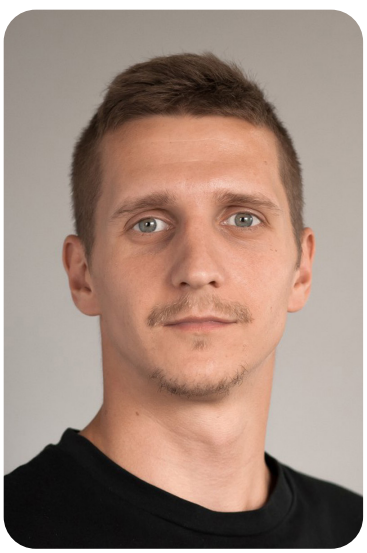
Редакторы:
Авинова Александра, Бородулина Елена

Корректоры:
Бурганова Лейсан, Ушакова Наталья

Дизайн, верстка и иллюстрации:
Тюльпанова Наталья

В номере:





ОТКРЫТАЯ УГРОЗА

Уже не первое десятилетие человечество упорно и настойчиво создает мир-дублер: у нас есть друзья в реальности и друзья в цифровой вселенной, мы занимаемся спортом, а электронные часы отслеживают и дублируют эти данные в цифровой мир, строительные компании, производственные предприятия создают цифровые двойники своих объектов, — и это лишь малая часть объектов, событий и явлений, которые можно обнаружить за пределами реальности, заглянув во вселенную двоичного кода. Нас вдохновляет возможность поделиться с друзьями своими мыслями и фотографиями в соцсетях, сделать заказ и отправить письмо на другой конец света за секунды, позволить роботу собрать машину или налить кофе, но мы, рядовые граждане этой вселенной, редко задумываемся о серебряной подкладке цифровизации. Мы щедро сыплем данными и информацией, оставляя электронные следы, которые не заметет ветер, и на которые, как оказывается, есть спрос, причем не всегда добродетельный. Поскольку данные создали свою экономику, торгуются на свободном и теневом рынке, не могли не найтись люди, желающие на этом заработать или воспользоваться в других целях. Так что теперь нам чаще угрожают не преступники с пистолетами, а преступники за мониторами компьютеров, планшетов и телефонов, которые совершают набеги на компании, обманывают и шантажируют людей, а иногда и целые государства.

Год за годом в мире становится все больше угроз, происходит все больше утечек данных. Статистика шокирует: согласно отчету InfoWatch, в 2022 году утекло 20,12 млрд записей персональных данных и платежной информации, что в 2,31 раза больше, чем в 2021 году. Очевидно, что масштаб киберугроз будет расширяться, следовательно, глобальные расходы на решения по кибербезопасности будут увеличиваться. По прогнозам Statista, в целом расходы на кибербезопасность в мире достигнут 249,9 млрд долларов в 2023 году, а к 2030 году превысят 657 млрд долларов. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности.

Таким образом, возникает своеобразная «гонка»: кто первый выявит уязвимость — исследователь или преступник, что первое будет опубликовано — эксплойт или патч, что выберут компании — как можно быстрее установить патч или быть взломанными и платить выкуп. Ведь пока за уязвимости в дарквебе будут платить больше и охотнее, чем сами разработчики, именно в дарквеб и будет уходить информация о новых уязвимостях.

Этот выпуск мы посвятили тому, как защититься от этой открытой угрозы, разбору — кто стоит на страже данных, что мотивирует хакеров совершать цифровые набеги и какой арсенал есть у защищающейся стороны. Здесь же вы найдете краткую эволюцию киберугроз, карту российского программного обеспечения, схему проведения кибератаки в формате комикса.

Мы искренне надеемся, что вам понравится этот выпуск!

Будем признательны за отзыв, комментарии и предложения, которые можно направлять на адрес: research@innopolis.university.

Команда сектора аналитических исследований

ЧТО ТАКОЕ КИБЕР-БЕЗОПАСНОСТЬ?

Кибербезопасность — это совокупность методов и практик защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от кибератак. Другими словами, это то, что помогает защищать все, что подключается к сети и электричеству, от возможных атак (воровство данных, отключения оборудования, компрометация компании или человека и пр.).

Сфера кибербезопасности естественным образом поделена на две стороны: **«черную»** и **«белую»**, одна из которых ищет уязвимости и возможности для атаки (хакеры и мошенники), а другая защищается и пытается эти атаки предотвратить (службы информационной и кибербезопасности).

Угрозы в киберпространстве в зависимости от целей и масштабов могут быть разных видов: от киберпреступления и хактивизма до кибертерроризма и кибервойн.

Объектом для атаки могут быть выбраны разные элементы киберпространства: сети (внешние и внутренние), приложения, данные и базы данных, серверы и сетевое оборудование, веб-ресурсы, промышленное оборудование, в том числе подключенное к сети (IIoT), компьютеры и мобильные устройства.

Вариантов проведения атак множество, в профессиональной терминологии существует понятие **«вектор атаки»** — это путь, способ или средство, с помощью которого киберпреступники проникают в целевую систему. К векторам атаки могут относиться как действия и инструменты злоумышленников, так и человеческий фактор или уязвимые технологии на стороне потенциальной жертвы и ее подрядчиков. Совокупность возможных векторов атаки, доступных в конкретной системе или организации, называется **поверхностью атаки**.

Элементы кибербезопасности

Угрозы

КИБЕРПРЕСТУПЛЕНИЕ

Это деятельность (атака), которая включает в себя использование компьютерных сетей в качестве основного средства совершения преступления, направленная на компьютер, компьютерную сеть или сетевое устройство. Целью киберпреступления может быть похищение данных с целью нанесения репутационного вреда, подлог данных в личных интересах, похищение персональных данных с целью незаконного обогащения, шантаж с целью незаконного обогащения, отмывание денег, доступ к интеллектуальной собственности, выведение компьютеров, сетей или оборудования из строя. Чаще всего, конечно, целью преступников является получение денежного вознаграждения.

КИБЕРТЕРРОРИЗМ

Это своего рода протест в форме предназначенных политически мотивированных атак на информационные, компьютерные системы, компьютерные программы и данные. Однако, кибертерроризм не ограничивается политическим заявлением, а преследует иные цели, создающие угрозу государственной безопасности, личности и обществу, в виде нанесения вреда вроде серьезных экономических затруднений, длительных остановок энергоснабжения, водоснабжения, порчи материальных объектов, искажения информации и др. Основной целью кибертерроризма является дестабилизация деятельности органов власти, либо воздействие на принятие ими социальных, экономических и политических решений.

ХАКТИВИЗМ

Это электронная форма гражданского неповиновения и протеста, когда с помощью кибератак стремятся обратить внимание общественности на социальные, политические и другие проблемы с целью продвижения политических идей, свободы слова, защиты прав человека, обеспечения свободы информации и пр. Хактивисты, как правило, не ищут финансовой или иной выгоды, а их мишенью становятся крупные корпорации, государственные структуры или публичные лица, чьи действия противоречат идеологии хактивистов. Несмотря на возможные «благие» намерения хактивистов, взлом ИТ-инфраструктуры и неправомерный доступ преследуется уголовным кодексом.

КИБЕРВОЙНА

Если война — это конфликт между политическими образованиями (государствами, племенами, политическими группировками и пр.), происходящий на почве различных претензий, в форме вооруженного противоборства, военных (боевых) действий между их вооруженными силами, то кибервойна преследует те же цели, но перенесена с физической арены в виртуальную, когда в качестве оружия выступает информация, а инструментами являются компьютеры и интернет. Все операции кибервойны направлены на нарушение функционирования вычислительных систем, отвечающих за работу деловых и финансовых центров, государственных организаций, на создание беспорядка в жизни страны, поэтому в первую очередь страдают инфраструктуры стратегического значения (финансовой, энергетической, промышленной, транспортных сетей, санитарной системы и др.)

Фото: Christian Wiediger / Unsplash

АНАЛИТИКА

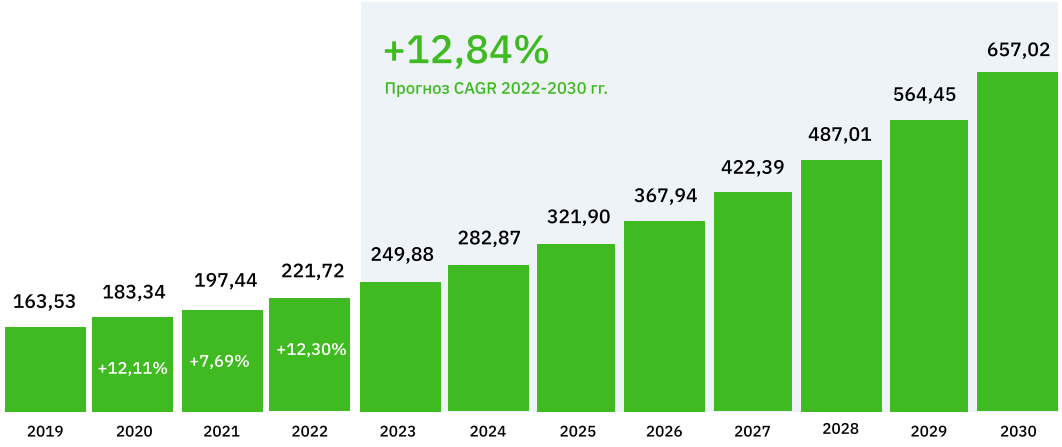
РЫНОК КИБЕРБЕЗОПАСНОСТИ В МИРЕ И В РОССИИ

В мире

В условиях всеобщей цифровой трансформации различных сфер жизнедеятельности человека, политической неопределенности и нестабильности вопросы развития кибербезопасности приобретают критически важное значение для всех стран мира.

Объем мирового рынка кибербезопасности в 2022 году составил 221,7 млрд долларов, показав прирост на 36% по отношению к 2019 году[1]. Значительное влияние на развитие и распространение решений в области кибербезопасности также оказали такие факторы как усложнение кибератак (использование злоумышленниками новых форм и методов доступа в сеть жертвы с применением машинного обучения, специализация хакеров на отдельных инструментах) и увеличение числа инцидентов утечек информации.

Объем мирового рынка кибербезопасности, млрд долл.



Источник: Statista, 2023

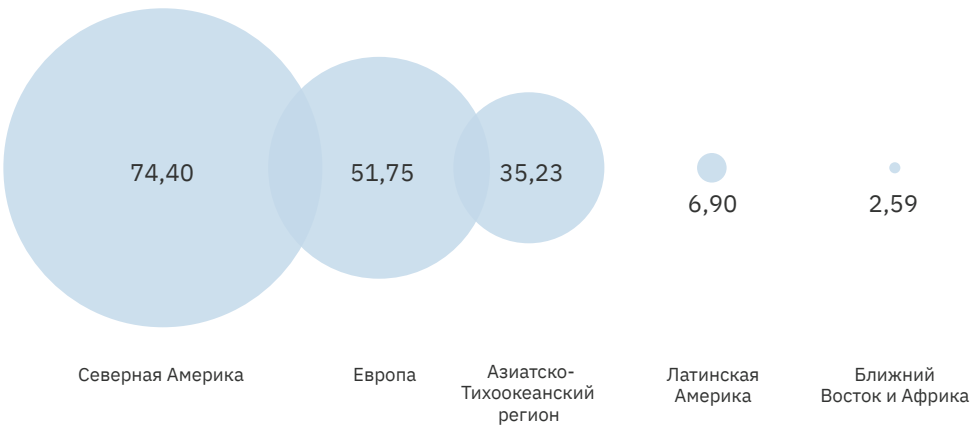
По данным Statista (исследование совместно с Next Move Strategy Consulting), в ближайшей перспективе на рынок кибербезопасности продолжат влиять указанные факторы и он достигнет отметки в 657 млрд долларов к концу 2030 года при среднегодовом темпе роста в 12,84%[2].

Страны-лидеры по объему рынка кибербезопасности в 2023 году — США, Китай, Германия, Великобритания и Япония. При этом ожидается, что самым быстрорастущим рынком в период 2023–2028 гг. станет Азиатско-Тихоокеанский регион[3]. На его активное развитие влияет увеличение числа кибератак, широкое внедрение облачных технологий, ужесточение требований к информационной безопасности и активная поддержка отрасли со стороны государства.

Объем рынка кибербезопасности страны-лидера США был оценен в 2023 году в 73,41 млрд долларов. Ожидается, что к 2028 году он достигнет 108,31 млрд долларов, а среднегодовой темп роста с 2023 по 2028 гг. составит 8,09%. Показатели среднегодовых темпов роста в Великобритании и Германии за аналогичный период составят 10,42% и 11,36% соответственно.

В азиатском регионе традиционно лидером выступает Китай с одним из самых высоких прогнозируемых среднегодовых темпов роста рынка за рассматриваемый период — 21,31%. По оценкам экспертов, рынок Китая уже в 2023 году достигнет отметки в 15 млрд долларов. Большим потенциалом роста обладают рынки Индии и Бразилии со среднегодовыми темпами роста 18,33% и 10,30% соответственно[4].

Объем мирового рынка кибербезопасности по макрорегионам в 2023 г., млн долл.

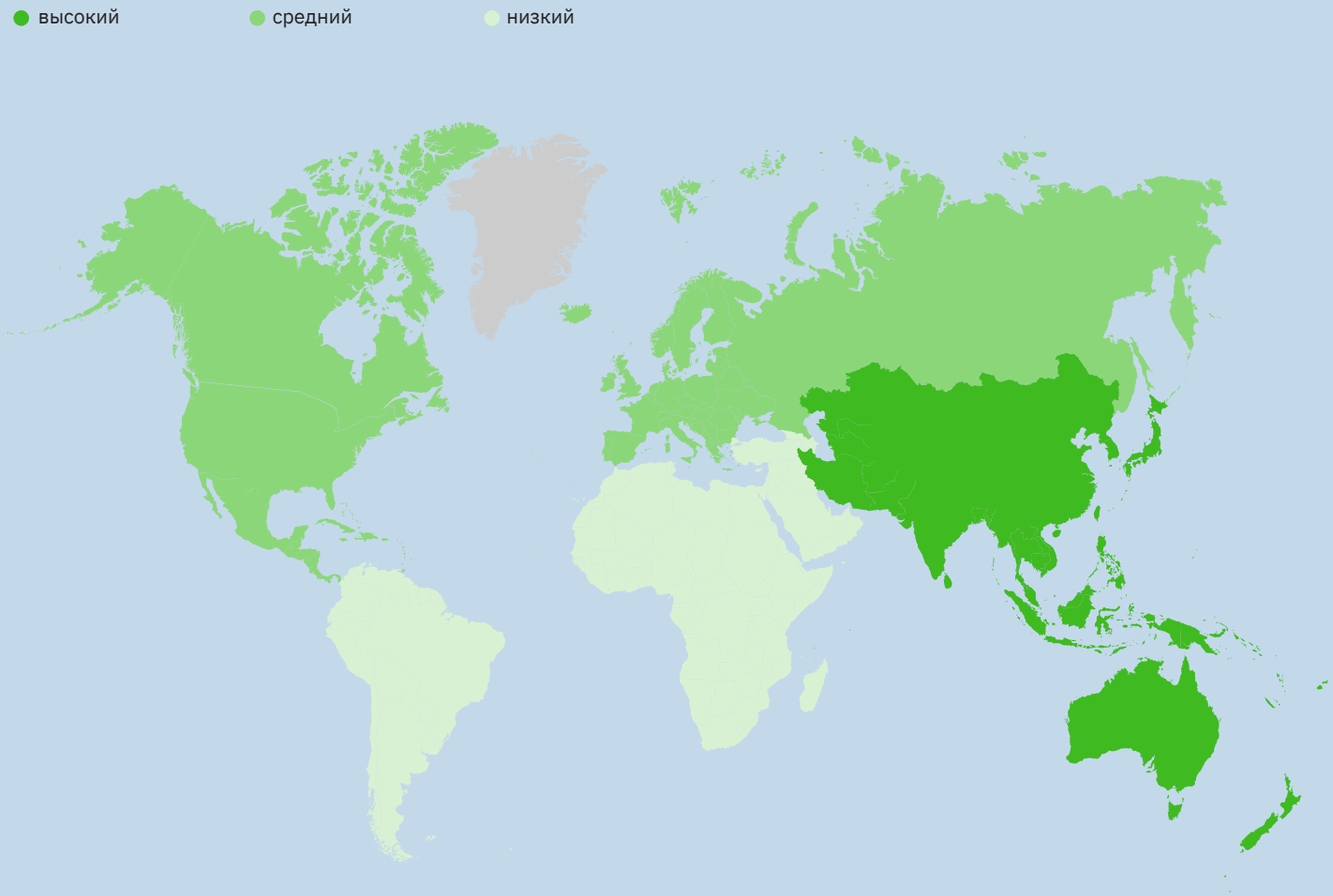


Источники: Statista, Mordor Intelligence, 2023

Для всех стран остается приоритетным рынок защиты критической инфраструктуры (услуги и решения в области физической безопасности и кибербезопасности инфраструктуры ключевых сфер жизнедеятельности государства и общества: правительство, аэрокосмическая и оборонная промышленность, банковский сектор и страхование, транспорт и логистика, электроэнергетическая и нефтегазовая отрасли и др.), который прирастает в среднем на 7,8%[5] ежегодно и по итогам 2022 года достиг 138,5 млрд долларов[6]. Самым крупным сегментом рынка является сегмент решений в области физической безопасности и кибербезопасности инфраструктуры с долей 63,57%, а рост рынка обеспечивается, в первую очередь, ростом сегмента кибербезопасности.

Азиатско-Тихоокеанский рынок стал самым быстрорастущим за счет прогресса цифровизации и политики Китая в области защиты инфраструктурных объектов, а лидирующие позиции на мировом рынке защиты критической инфраструктуры занимают компании-крупнейшие игроки из США и стран ЕС: BAE Systems PLC (Великобритания), Honeywell International Inc. (США), Raytheon Co. (США), Airbus SE (Франция, ЕС), Hexagon AB (Швеция, ЕС)[7]. Ожидается, что он достигнет 254,51 млрд долларов к 2032 году.

Карта стран по рейтингу защищенности критической инфраструктуры



Источники: Mordor Intelligence, 2023

Объем мирового рынка информационной безопасности по сегментам за 2021-2022 гг., млрд долл.

Источники: Sapphire, 2023

Согласно данным о расходах потребителей рынка информационной безопасности, самый крупный его сегмент — услуги по обеспечению информационной безопасности (консалтинговые, а также услуги по внедрению, управлению, мониторингу, рисковому и сервисному сопровождению решений в области информационной безопасности, оценке безопасности и проницаемости), который занимает 41,03% в общем объеме рынка в 2022 году. На втором месте — средства защиты инфраструктуры с долей 16,98%, на третьем — сетевое оборудование с долей 11,2%[8].

Сегменты, которые показали наибольший прирост (более 20%) в объеме рынка в 2022 году — защита приложений и облачная защита. Основными факторами их роста стали увеличение числа приложений и данных, доступ к которым осуществляется удалённо. Дорогостоящее содержание собственной информационной инфраструктуры также побуждает бизнес использовать облачные сервисы.

Компании с наибольшей долей мирового рынка кибербезопасности расположены в основном в США[9]. Лидером по объему выручки (5,51 млрд долларов) в 2022 году стала компания Palo Alto Networks[10], которая специализируется главным образом на разработке межсетевых экранов и облачных решений и контролирует 8,7% рынка по итогам I квартала 2023 года[11].

На втором месте располагается транснациональная корпорация Fortinet с объемом выручки 4,42 млрд долларов по итогам 2022 года[12] и долей рынка 7%[13]. Это мировой лидер в области разработки решений кибербезопасности — от антивирусного ПО до безопасности конечных точек.

Третье место занимает компания Cisco, лидер в области корпоративной безопасности, а также сетевой и облачной защиты, с долей рынка 6,1%[14].

Мировые лидеры — CrowdStrike, Check Point, Okta, Microsoft, IBM, Symantec, Trelix, — контролируют от 2,7% до 3,6% рынка кибербезопасности[15].

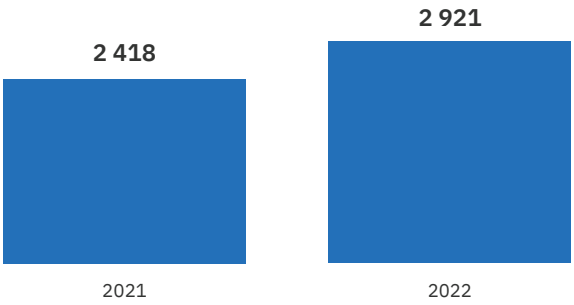
Топ-10 лидеров мирового рынка кибербезопасности за I квартал 2023 г.

Компания	Доля рынка	Страна
Palo Alto Networks	8,7%	США
Fortinet	7,0%	США
Cisco	6,1%	США
CrowdStrike	3,6%	США
Check Point	3,5%	Израиль
Okta	3,2%	США
Microsoft	3,2%	США
IBM	2,9%	США
Symantec	2,9%	США
Trellix	2,7%	США

Источник: Canalys, 2023

Общее количество успешных кибератак (инцидентов), которые приводят к негативным последствиям для компаний или частных лиц, ежегодно растет. В 2022 году количество таких инцидентов достигло 2 921, что на 21% больше, чем в 2021 году[16].

Общее количество успешных кибератак за 2021-2022 гг., ед.



Источник: Positive Technologies, 2023

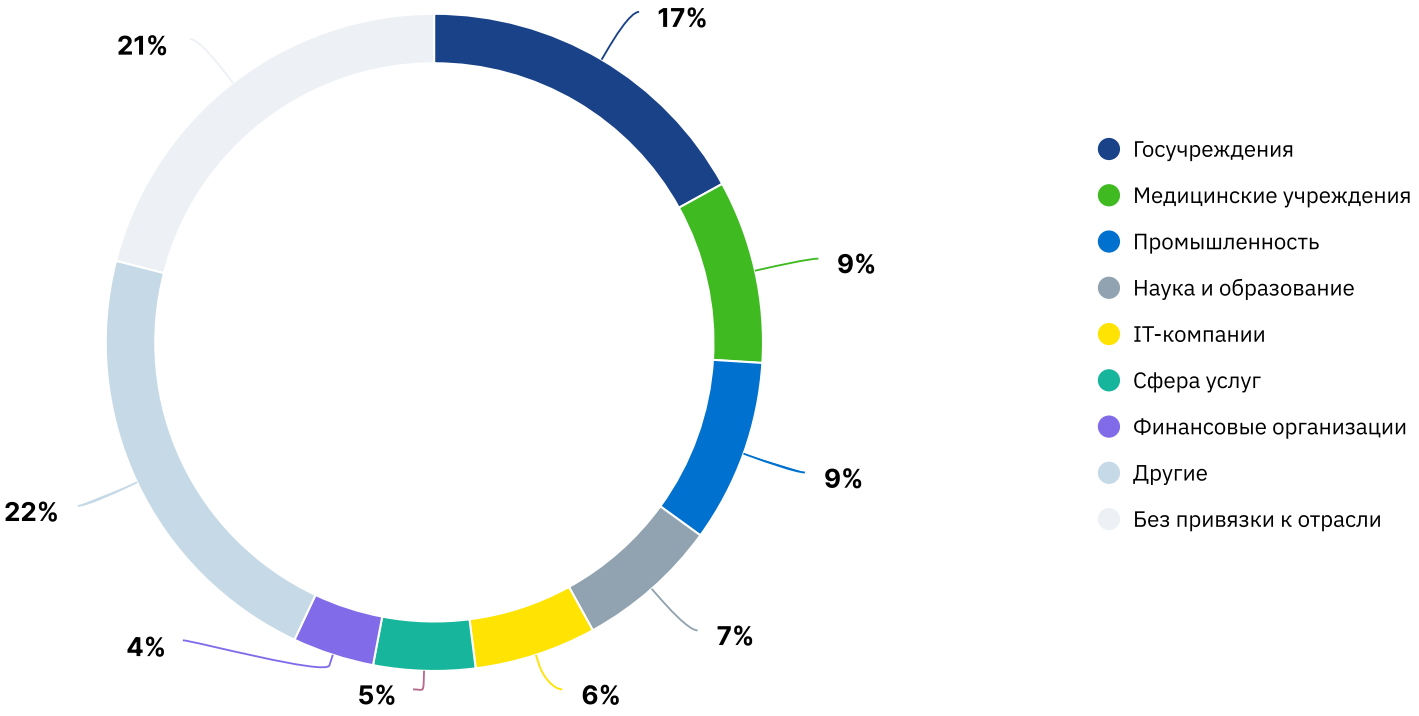
В отраслевом разрезе главными направлениями для злоумышленников остаются госучреждения, доля атак на них составляет 17%, на медицинские учреждения и промышленный кластер — по 9%[17].

В I квартале 2022 года количество атак, направленных на госучреждения, увеличилось практически в два раза по сравнению с последним кварталом 2021 года, а затем продолжало расти в течение всего года[18]. Злоумышленники использовали вредоносное ПО почти в каждой второй атаке на госучреждения. Наиболее популярными типами вредоносного ПО оказались шифровальщики (56% среди атак с применением ВПО) и вредоносные программы для удаленного управления (29%)[19].

В промышленности за 2022 год было зафиксировано 223 атаки на отраслевые компании, что на 7% больше по сравнению с 2021 годом. Преступников все чаще интересует не финансовая выгода или получение крупных сумм выкупа, а перебои в деятельности предприятий, аварии, остановка важнейших технологических процессов.

Медицина — отрасль-лидер по утечкам данных. Медучреждения уже пятый год подряд остаются в тройке самых атакуемых организаций, при этом количество атак держится примерно на уровне 2021 года. Более чем в 80% случаев атаки приводили к утечкам данных о клиентах (в основном персональных данных и медицинской информации)[20].

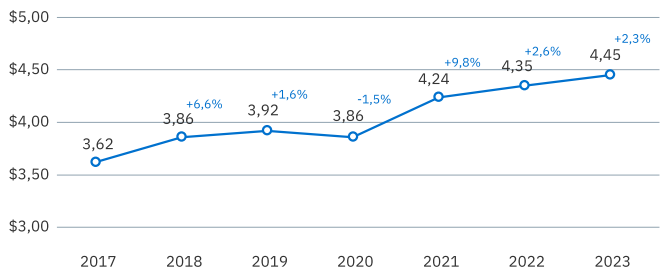
Категории жертв среди организаций в 2022 г.



Источник: Positive Technologies, 2023

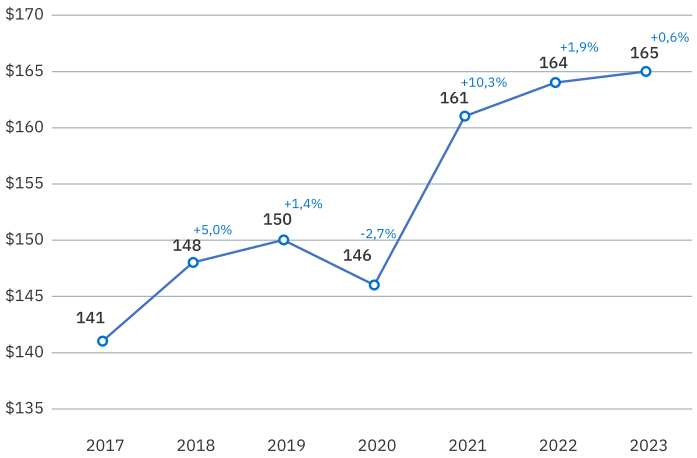
Средняя стоимость утечки данных в 2023 году достигла рекордного значения и составила 4,45 млн долларов, прибавив 15,3% с 2020 года. За этот же период стоимость утечки данных на одну запись выросла на 13,01% и в 2023 году составила 165 долларов[21].

Средняя стоимость утечки данных, млн долл.



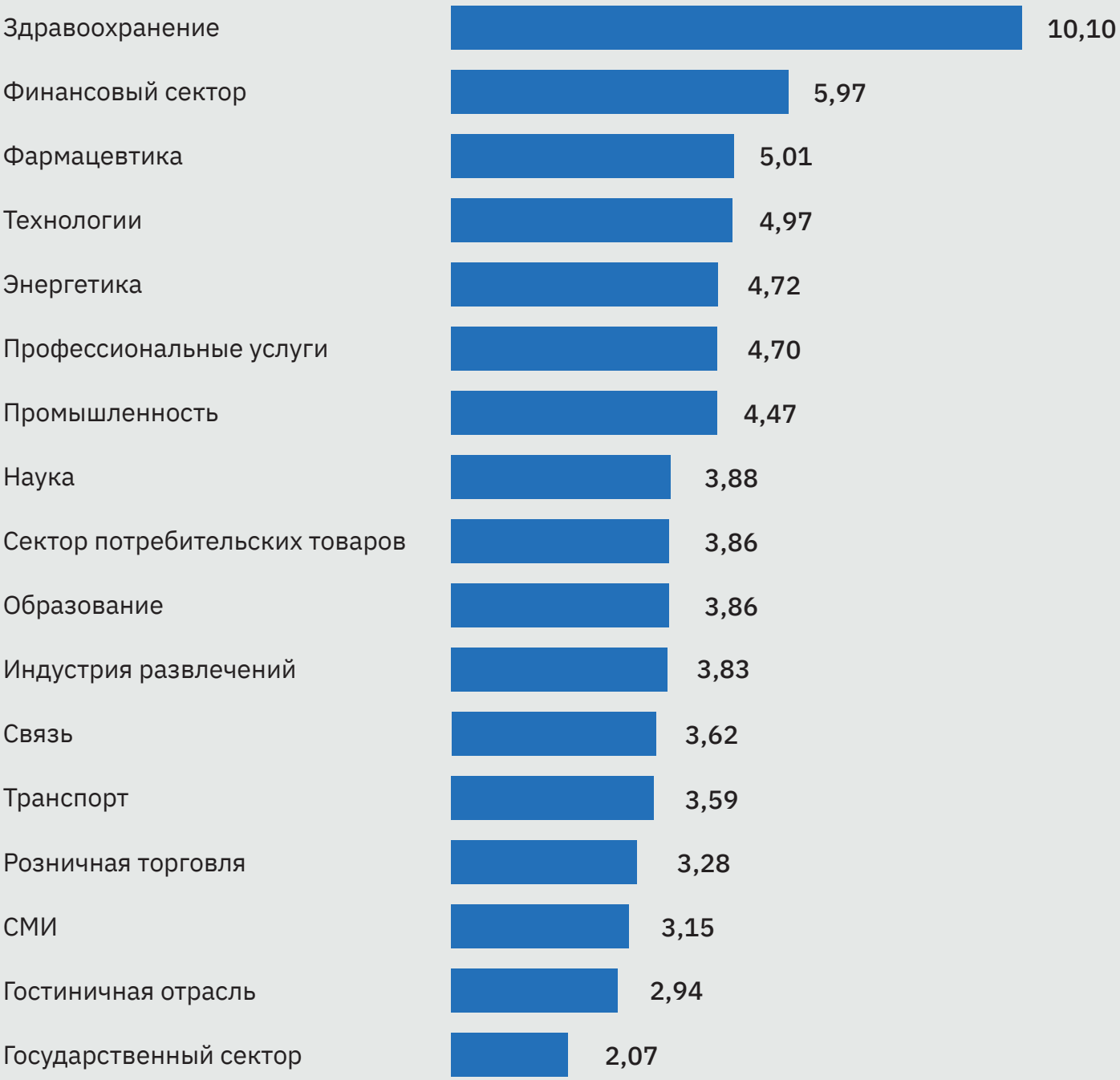
Источник: IBM Security, 2023

Средняя стоимость утечки данных на 1 запись, долл.



Источник: IBM Security, 2023

Средняя стоимость утечки данных по отраслям в 2022 г., млн долл.



Источник: IBM Security, 2023

В отраслевом разрезе дороже всего в 2022 году утечка данных обходится сектору здравоохранения — 10,10 млн долларов, финансовому сегменту — 5,97 млн долларов и фармацевтике — 5,01 млн долларов[22].

Одним из векторов построения устойчивой защиты от вторжений стала интеграция искусственного интеллекта в системы обеспечения информационной безопасности. Организации, которые в 2022 году широко использовали искусственный интеллект в целях защиты, в среднем сократили затраты, понесенные в результате утечек данных, на 1,76 млн долларов. Кроме этого, таким компаниям в среднем требуется на 108 дней меньше для выявления и локализации инцидентов[23].

Стоимость утечки информации выше среднемирового уровня наблюдается в следующих странах и регионах: США, Средний Восток, Канада, Великобритания, Япония и ряд стран Европейского союза. В США в 2022 году зафиксирована самая высокая средняя стоимость утечки данных, которая составила 9,44 млн долларов, что на 4,3% выше стоимости утечки в 2021 году. Наибольший прирост стоимости утечки информации в 2022 году произошел в Великобритании (+8%) и на Среднем Востоке (+7,7%)[24].

Стоимость утечки данных по стране или региону, млн долл.

Страна/регион	2021	2022	Изменение
США	**9,05**	**9,44**	↑ **4,31%**
Средний Восток	**6,93**	**7,46**	↑ **7,65%**
Канада	**5,4**	**5,64**	↑ **4,44%**
Великобритания	**4,67**	**5,05**	↑ **8,14%**
Германия	**4,89**	**4,85**	↓ **-0,82%**
Япония	**4,69**	**4,57**	↓ **-2,56%**
Франция	**4,57**	**4,34**	↓ **-5,03%**
Италия	**3,61**	**3,74**	↑ **3,60%**
Южная Корея	**3,68**	**3,57**	↓ **-2,99%**
Южная Африка	**3,21**	**3,36**	↑ **4,67%**

Источник: IBM Security, 2023

Рассматривая долю успешных атак хакеров в разрезе объектов атак, можно отметить, что атаки хакеров на компьютеры, серверы и сетевое оборудование в организациях были успешными в 79% случаев.

В организациях атаки на сотрудников были успешными в 43% случаев, в отношении частных лиц — в 93%, что демонстрирует популярность социальной инженерии (форма кибератаки, которая предполагает использование манипуляций и обмана для получения доступа к данным или информации). Особое распространение получила модель phishing as a service («фишинг как услуга»). В атаках на частных лиц злоумышленники активно используют социальные сети и мессенджеры, а в инцидентах, затронувших организации, отмечены успешные атаки на второй фактор аутентификации[25].

При атаках на организации в 2022 году самыми эффективными методами стали:

- использование ВПО — в 54% случаев атаки были успешными;
- социальная инженерия — 43% успешных случаев;
- эксплуатация уязвимостей — успешна в 34% случаев;
- компрометация учетных данных преступникам удалась в 17% случаев всех атак.

Хакеры в 93% случаев успешно использовали методы социальной инженерии в отношении частных лиц и в 51% атак — ВПО[26].

Методы атак непрерывно совершенствуются вслед за появлением новых технологий и изменением трендов рынка. Появляются новые виды вредоносного ПО, код для которого хакеры могут как создавать самостоятельно, так и приобретать в даркнете, либо пользоваться услугами представителей своего сообщества. При этом шифровальщики наиболее опасны для организаций, поскольку атаки с их использованием успешны в 51% случаев. В зоне высокой эффективности вредоносного ПО остаются загрузчики, доля результативных атак которых составляет 19%. Использование вредоносного ПО для удаленного доступа в 28% случаев привело к достижению целей злоумышленников, а шпионское ПО — к 13% успешных атак[27]. Ожидается, что в ближайшем периоде вырастет активность политически мотивированных хактивистов, которые чаще используют вайперы и шпионское ПО. При этом уже в 2022 году различные группы хакеров, которые специализируются на взломе компаний среднего бизнеса с невысокими доходами и слабой защищенностью ИТ-систем, организовали торговлю в даркнете правами доступа к ИТ-системам, цена лота стартует от 500 долларов[28]. В организациях похищали в большинстве случаев персональные данные (36%), коммерческую тайну (17%) и учетные данные (14%).

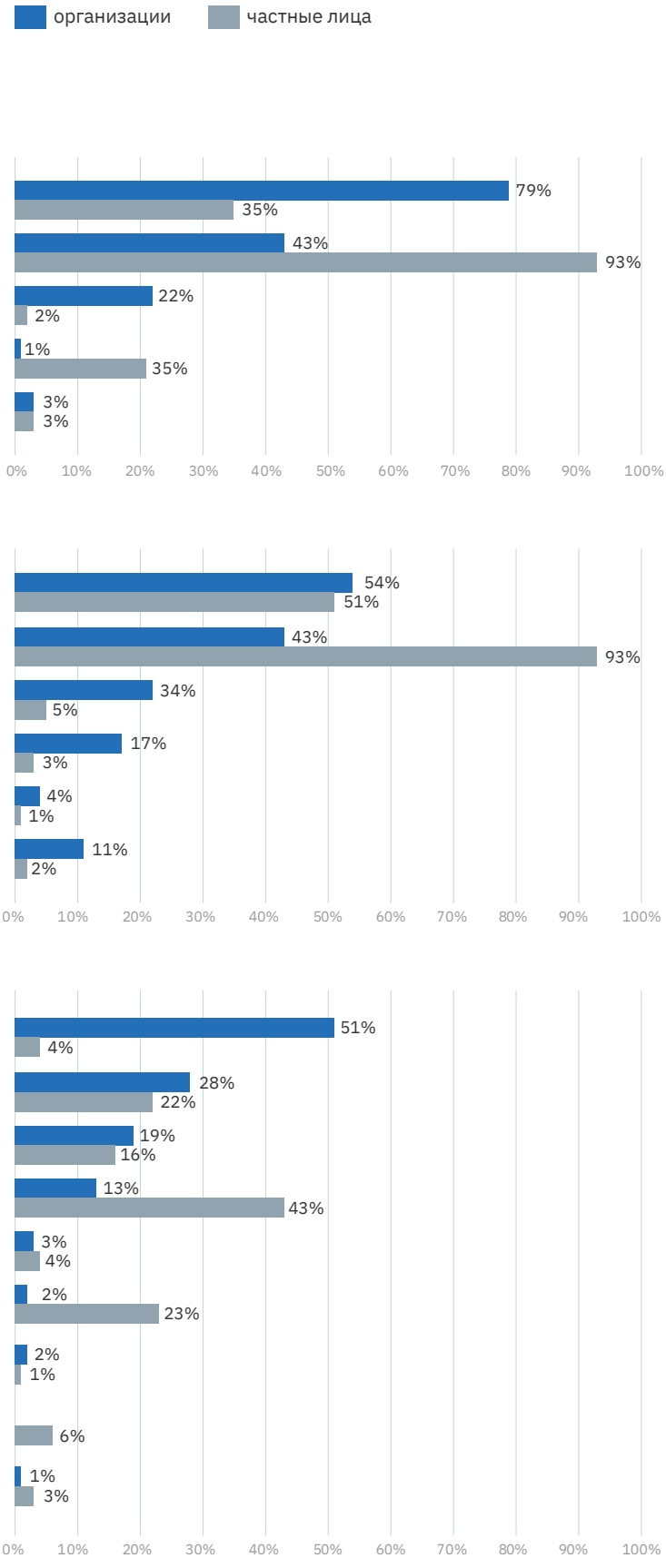
В отношении частных лиц наибольшая доля успешных атак реализуется с помощью шпионского ПО — 43%, банковских троянов — 23%, ВПО для удаленного доступа — 22% и загрузчиков с показателем успешности 16%. Похищали в большинстве случаев персональные данные (28%) и учетные данные (41%), а данные платежных карт стали целью 15% успешных атак[29].

Дополнительным инструментом, используемым в деятельности хакеров, стал ChatGPT от OpenA I. Несмотря на то, что разработчиками предусмотрены механизмы предотвращения создания вредоносного контента, пользователи сумели найти обходные пути и использовали инструмент для создания кода вредоносного ПО, обратного инжиниринга (анализ машинного кода ПО с целью его модификации, получения сведений о протоколах сетевого обмена и т.д.) и написания скриптов.

Атаки на предприятия, госсектор и граждан совершают, в большинстве случаев, группы злоумышленников или хакерские группировки. Организованные группы чаще преследуют финансовые интересы и используют специализированное ПО — программы-вымогатели. В первой половине 2023 года наибольшую активность проявили хакерские группы BlackCat, Lockbit, Black Basta, Royal, Akira. В 2023 году 38% атак вымогателей было сосредоточено на компаниях сферы услуг, 19,8% пришлось на производственный сектор, остальные 42,2% распределились между сферой социальных услуг, здравоохранением и отраслью высоких технологий.

Интересно, что процент компаний, которые заплатили выкуп, в первом полугодии 2023 года составил 19%, что на 10% меньше, чем во второй половине 2022 года[30]. Эксперты объясняют подобную тенденцию, во-первых, изменением политики страховых компаний в отношении возмещения жертвам суммы выкупа для программ-вымогателей. Во-вторых, управление по контролю за иностранными активами США (OFAC) в сентябре 2021 года вынесло предупреждение всем компаниям о наложении санкций в случае выплаты по требованиям хакеров[31]. Также дополнительными факторами в вопросах снижения частоты выплат хакерам стали улучшенная безопасность компаний, особенно на фоне громких атак с 2020 по 2022 год, и налаживание систем резервного копирования информации[32].

Доля успешных атак за 2022 г.



Источник: Positive Technologies, 2023

ДЕЙСТВУЮЩИЕ ХАКЕРСКИЕ ГРУППИРОВКИ

Для каждой организации мы указали процент атак от общего числа за I квартал 2023 г.
18,8% составляют прочие группы

BlackCat

18,71%

Группа атакует компании различных отраслей. Отличается уникальными методами уклонения от схем защиты и пост-компрометационных действий. Используют разнообразное ПО: Cobalt Strike, Trickbot и Qakbot.

Lockbit

18,71%

Группа обычно использует метод двойного вымогательства, а в некоторых случаях даже тройное вымогательство, в ходе которого они запускают DDoS-атаки на сеть жертвы. LockBit набирают опытных партнеров, которые получают первоначальный доступ к сетям жертв в обмен на процент от уплаченного выкупа. Программа-вымогатель LockBit 3.0 постоянно развивается, и в апреле 2023 года образцы, предназначенные для шифрования на устройствах Apple были обнаружены с помощью службы VirusTotal.

Black Basta

12,90%

Киберпреступная организация, которая предлагает услуги-вымогатели (RaaS) другим хакерам. Осуществляет атаки за процент от выкупа с использованием собтвенного ПО и инфраструктуры.

Royal

12,90%

Группа работает обособленно и использует самописный шифратор, атакует крупный бизнес без привязки к какому-либо сектору экономики.

Akira

12,30%

Первое упоминание о группировке в апреле 2023 г. Организация активно развивается. Akira шифрует и экспортирует данные на удаленный сервер и вымогает деньги, угрожая опубликовать конфиденциальную информацию на их сайте. Программа-вымогатель добавляет расширение «.akira» для зашифрованных файлов и использует защищенный паролем сайт TOR для ведения переговоров с жертвами

Luna Moth

6,40%

Группировка активно использует социальную инженерию и инструменты для удаленного администрирования. Классические инструменты - фишинг с целью установки жертвой RAT (трояна удаленного доступа) и получением полного контроля с последующими действиями по вымогательству

Источник: CRIMEWARE TRENDS AND HIGHLIGHTS, 2023

Ключевые выводы

1. Мировой рынок кибербезопасности активно растет: в 2022 году его объем составил 221,7 млрд долларов, показав прирост на 36% по отношению к 2019 году. Прогнозируется, что к 2030 году он достигнет отметки в 657 млрд долларов при среднегодовом темпе роста в 12,84%. Факторы роста: активная цифровизация всех отраслей экономики и развитие технологий (искусственный интеллект, облачные технологии, IoT и т.д.), рост и усложнение кибератак, в том числе увеличение числа инцидентов утечек информации, поддержка кибербезопасности на государственном уровне в условиях политической нестабильности.

2. Страны-лидеры по объему рынка кибербезопасности в 2023 году — США, Китай, Германия, Великобритания и Япония. При этом ожидается, что самым быстрорастущим рынком в период 2023–2028 гг. станет Азиатско-Тихоокеанский регион.

3. Самый крупный сегмент рынка информационной безопасности — услуги по обеспечению информационной безопасности, которые занимают 41,03% в общем объеме рынка в 2022 году. На втором месте — средства защиты инфраструктуры с долей 16,98%, на третьем — сетевое оборудование с долей 11,2%.

4. Сегменты, которые показали наибольший прирост (более 20%) в объеме рынка в 2022 году — защита приложений и облачная защита. Основными факторами их роста стали увеличение числа приложений и данных, доступ к которым осуществляется удалённо.

5. Компании с наибольшей долей мирового рынка кибербезопасности расположены в основном в США. Лидером по объему выручки (5,51 млрд долларов) в 2022 году стала компания Palo Alto Networks, которая специализируется главным образом на разработке межсетевых экранов и облачных решений и контролирует 8,7% рынка.

6. В 2022 году общее количество инцидентов в мире, которые привели к негативным последствиям для компаний и частных лиц, достигло 2 921, что на 21% больше, чем в 2021 году.

7. В отраслевом разрезе главными направлениями для злоумышленников остаютс госучреждения, доля атак на них составляет 17%, медицинские учреждения и промышленный кластер — по 9%.

8. Средняя стоимость утечки данных в 2023 году достигла рекордного значения и составила 4,45 млн долларов, прибавив 15,3% с 2020 года. За аналогичный период стоимость утечки данных на одну запись выросла на 13,01% и в 2023 году составила 165 долларов.

9. В отраслевом разрезе дороже всего в 2023 году утечка данных обходится сектору здравоохранения — 10,93 млн долларов, финансовому сегменту — 5,9 млн долларов и фармацевтике — 4,82 млн долларов.

10. Рассматривая долю успешных атак хакеров в разрезе объектов атак, можно отметить, что атаки хакеров на компьютеры, серверы и сетевое оборудование в организациях были успешными в 79% случаев.

11. В организациях атаки на сотрудников были успешными в 43% случаев, в отношении частных лиц — в 93% случаев, что демонстрирует популярность и эффективность социальной инженерии.

12. При атаках на организации в 2022 году самыми эффективными методами стали: использование ВПО — в 54% случаев атаки были успешными; социальная инженерия — 43% успешных случаев, эксплуатация уязвимостей — успешна в 34% случаев, компрометации учетных данных — в 17% случаев всех атак.

13. Процент компаний, которые заплатили выкуп, в первом полугодии 2023 года составил 19%, что на 10% меньше, чем во второй половине 2022 года в связи с изменением политики страховых компаний в отношении возмещения жертвам суммы выкупа для программ-вымогателей, усилением безопасности компаний на фоне громких атак с 2020 по 2022 год и налаживанием систем резервного копирования информации.

В России

По данным эстонской Академии электронного государственного управления (NCSI), на сентябрь 2023 года Россия занимает 30 место среди 176 стран по национальному индексу кибербезопасности (71,43%). Национальный индекс кибербезопасности показывает готовность страны к предотвращению киберугроз и управлению киберинцидентами. Геополитическая обстановка в 2022 году значительно повлияла на рынок кибербезопасности России: с одной стороны наблюдается рост количества атак во всех отраслях экономики и уход с рынка крупных международных игроков, с другой - стремительное развитие отечественных технологий, которое в конечном итоге усилит позиции российских разработчиков ПО на международной арене.

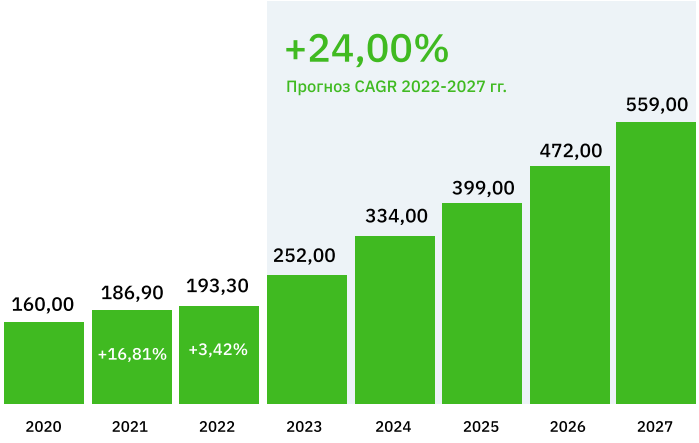
Национальный индекс кибербезопасности

Страна	Индекс	Позиция в рейтинге
Бельгия	**94,81**	**1**
Литва	**93,51**	**2**
Эстония	**93,51**	**3**
Чехия	**90,91**	**4**
Германия	**90,91**	**5**
Румыния	**89,61**	**6**
Греция	**89,61**	**7**
Португалия	**89,61**	**8**
Великобритания	**89,61**	**9**
Испания	**88,31**	**10**
Российская Федерация	**71,43**	**30**

Источник: National Cyber Security Index, 2023

Объем рынка кибербезопасности Российской Федерации за 2022 год составил 193,3 млрд рублей с темпом прироста 3,42% относительно 2021 года[33]. С 2020 по 2021 год рынок вырос на 16,8% и по прогнозам экспертов продолжит расти в ближайшие 5 лет с совокупным среднегодовым темпом роста (CAGR) в 24%, достигнув в 2027 году 559 млрд рублей[34]. Основные факторы роста рынка: необходимость замены западных решений, повышенное внимание к кибербезопасности со стороны государства и рост хакерских атак во всех отраслях экономики в связи с геополитическими событиями 2022 года.

Объем российского рынка кибербезопасности, млрд руб.



Источник: Центр стратегических разработок, 2023

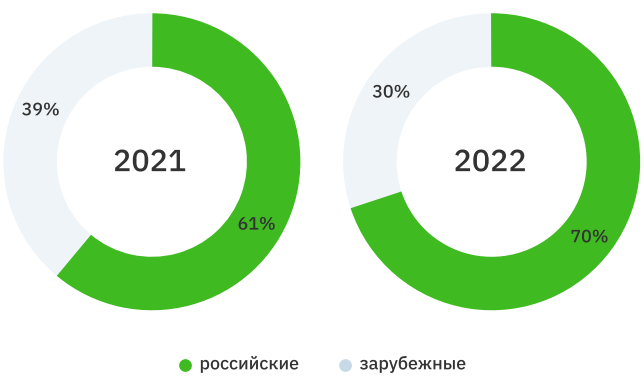
Существенных изменений в структуре рынка кибербезопасности в 2022 году по сравнению с предыдущим периодом не произошло: доля средств защиты информации (СЗИ) в общем объеме рынка составляет 74%, доля услуг — 26%. В структуре продуктов СЗИ выросла доля сегментов «защита рабочих станций (конечных точек)», «защита инфраструктуры», «защита приложений». Данный рост в большей степени был обусловлен повышением рисков реализации инцидентов, связанных с рабочими станциями и инфраструктурными объектами, а также адаптацией отечественных компаний к усилению контроля в части информационной безопасности со стороны государства.

Структура российского рынка безопасности по продуктам

Источник: Центр стратегических разработок, 2023

В России на рынке продуктов СЗИ усиливается положение российских вендоров: в 2022 году они занимают 70% рынка (в 2021 году — 61%)[35].

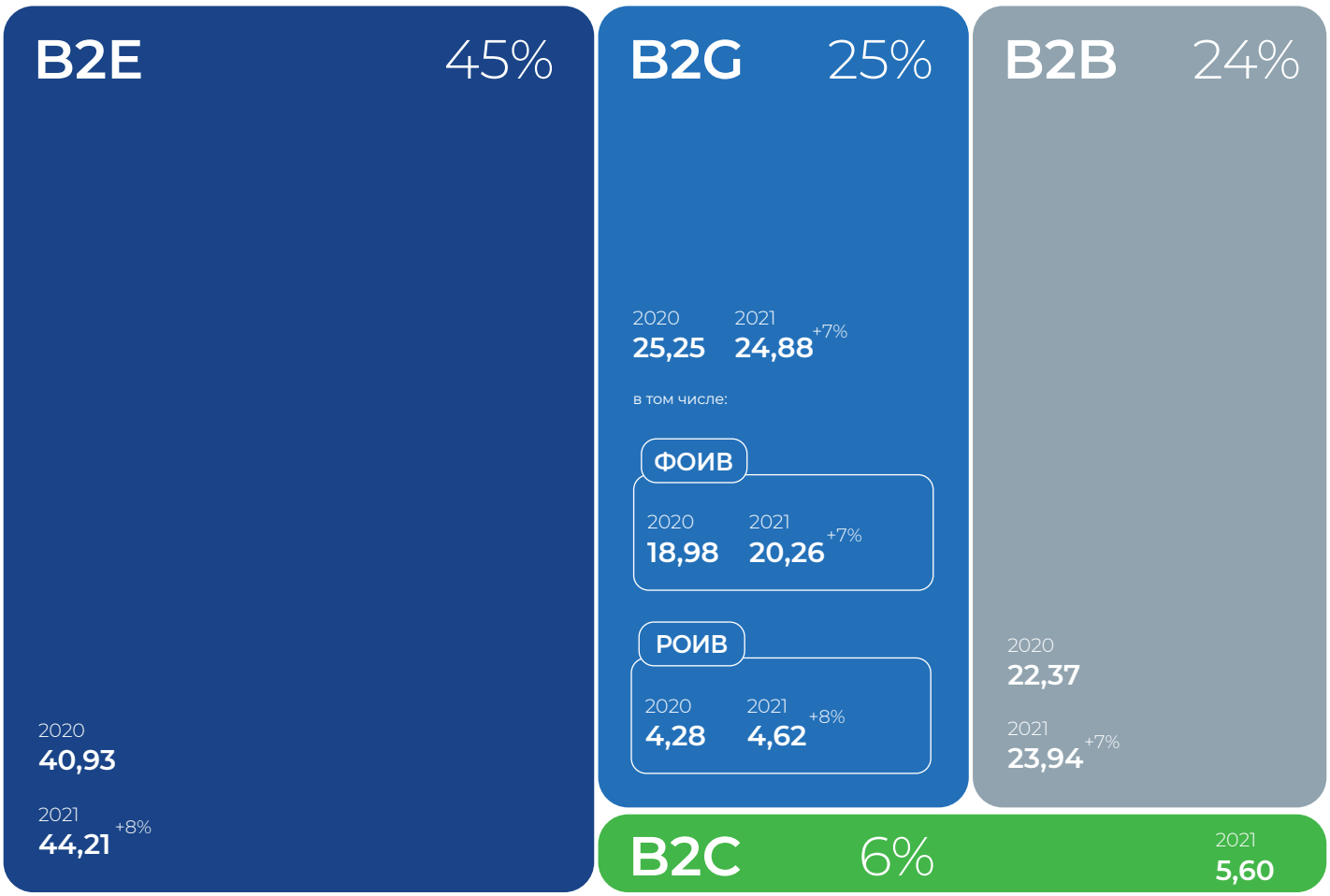
Доля российских и зарубежных вендоров средств защиты



Источник: Центр стратегических разработок, 2023

Рассматривая структуру рынка информационной безопасности по клиентским сегментам в 2021 году, мы видим, что наибольшую долю на нем занимает сегмент B2E — 45%. Компании сегмента столкнулись с кратным ростом угроз кибербезопасности начиная с февраля 2022 года, однако не сократили расходы на ИБ, а переориентировали их в рамках комплексных подходов к защите[36]. На рынки B2B и B2G приходится по 24% и 25% глобального отечественного рынка соответственно. Государство усилило давление как на бизнес, так и на собственные структуры с целью повышения их киберзащиты, что нашло отражения в требованиях Указа Президента Российской Федерации от 01.05.2022 No 250, Указа Президента Российской Федерации от 30.03.2022 No 166 и ряда других нормативных документов[37]. На сегмент B2C в 2021 году приходится 5,7% рынка.

Структура российского рынка ИБ по клиентским сегментам и объему трат за 2021-2022 гг., млрд руб.



B2C — Business-to-Consumer — сегмент рынка, в котором продажи товаров или услуг осуществляются в отношении домашних пользователей (частных лиц) и индивидуальных предпринимателей.

B2B — Business-to-Business — продажа услуг другим компаниям (крупные предприятия, средние предприятия, средний и малый бизнес, малые и микропредприятия)

B2E — Busines- to-Enterprise — сегмент рынка, в котором продажи товаров или услуг осуществляются в отношении крупнейших предприятий с годовой выручкой свыше 70 млрд руб.

B2G — Business-to-Government — сегмент рынка, в котором продажи товаров или услуг осуществляются в отношении федеральных и региональных органов исполнительной власти (ФОИВ и РОИВ), силовых ведомств.

ФОИВ — федеральные органы исполнительной власти

РОИВ — региональные органы исполнительной власти

Источник: Ростелеком-Солар, 2022

Крупнейшие вендоры средств защиты информации на российском рынке в 2022 г.

Компания	Доля рынка	Страна
Лаборатория Касперского	16,0%	Россия
Positive Technologies	12,4%	Россия
Check Point Software Technologies	4,8%	Израиль
BI.ZONE	4,3%	Россия
Cisco	4,1%	США
Fortinet	4,1%	США
ИнфоТеКС	3,3%	Россия
IBM	2,8%	США
Фактор-ТС	2,3%	Россия
Крипто-Про	2,2%	Россия
Актив-Софт	2,0%	Россия
Другие	41,7%	

Источник: Центр стратегических разработок, 2023

Эксперты рынка отмечают, что решения киберзащиты от российских компаний не только не уступают зарубежным аналогам по своей эффективности и возможностям, но и более прогрессивны[38].

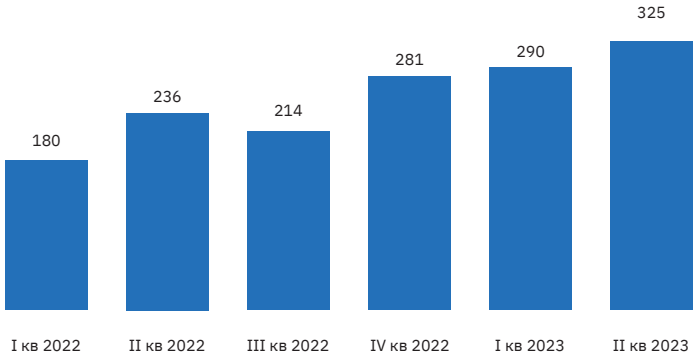
Объем рынка услуг в области информационной безопасностиг в 2022 году составил 49,8 млрд рублей, а к 2027 оценочно составит 145,3 млрд рублей[39], лидерами в данной области являются следующие компании:

1. Ростелеком-Солар
2. Лаборатория Касперского
3. BI.ZONE
4. Код Безопасности
5. Positive Technologies

В 2022 году в России и СНГ наиболее атакуемыми отраслями по данным аналитического отчета «Лаборатории Касперского» были промышленность (24%), финансовые организации (20%), ИТ-компании (17%), транспорт (14%) и СМИ (12%)[40]. В презентации советника генерального директора компании по кибербезопасности Positive Technologies отмечается, что число кибератак на российские госучреждения в 2022 году увеличилось на 25% по сравнению с 2021 годом, до 403 атак[41]. Среднее время обнаружения инцидента высокого уровня критичности составляло 43,8 минуты, что на 6% больше в сравнении с прошлыми периодами[42].

По данным компании «РТК-Солар»[43], количество событий информационной безопасности (подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний) в I полугодии 2023 года составило 615 тысяч, что на 47,8% больше, чем в аналогичном периоде 2022 года и на 24% превышает показатель II полугодия 2022 года. При этом доля подтвержденных инцидентов в общем объеме сократилась на 22%. Злоумышленники генерируют большое количество «фонового шума», но для большинства компаний такие атаки не являются критичными и не влекут за собой последствий, однако при этом явно выделяются группы, координируемые централизованно[44].

Количество кибератак за 2022-2023 гг., тыс. ед.



Источник: Ростелеком-Солар, 2023

В среднем на одного клиента во II полугодии 2022 г. приходилось 1 813 событий ИБ, тогда как в I полугодии 2023 — уже 2 112, то есть рост составил 17%. Среднее количество подтвержденных инцидентов, напротив, снизилось на 38% (с 76 до 55 на клиента)[45].

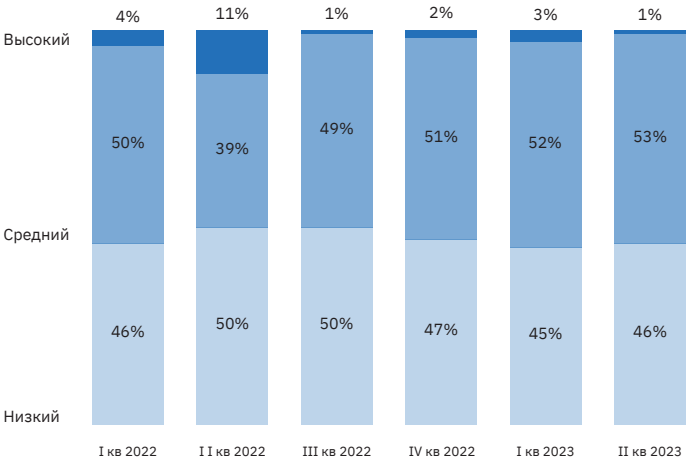
В части распределения инцидентов по уровню критичности в I полугодии 2023 года можно отметить низкую долю событий **«высокой степени критичности»** (3% в I квартале и 1% во II квартале 2023 года), **к которым относятся инциденты, способные оказывать влияние на работу ключевых систем более 30 минут, компрометация критически важной информации и учётных записей, прямые финансовые потери на сумму более 1 млн. рублей[46].**

Сложившиеся тренды демонстрируют повышение защиты ИТ-периметра российских компаний, несмотря на уход зарубежных вендоров[47].

Наиболее популярным инцидентом в I и II кварталах 2023 года, как и в целом в 2022 году, стало заражение ВПО (56% и 49% соответственно). Заметен тренд на увеличение доли сетевых атак и эксплуатации уязвимостей.

Рост доли сетевых атак, по мнению экспертов, говорит о том, что в ближайшие годы злоумышленники будут активно использовать киберразведку для поиска уязвимостей в инфраструктуре компаний. Сетевые атаки сигнализируют о том, что компания попала в поле зрения хакеров и не исключено, что в будущем она столкнется с более серьезной кибератакой[48].

Распределение кибератак по уровню критичности



Источник: Ростелеком-Солар, 2022-2023

Увеличение доли эксплуатации уязвимостей аналитики компании «РТК-Солар» связывают с переходом российских компаний на отечественное ПО: часть решений разрабатывалась и внедрялась в ускоренном режиме, что дало злоумышленникам широкое поле для выявления и использования «дыр» в безопасности[49].

Распределение кибератак с разным уровнем критичности по категориям

	I кв 2022	I I кв 2022	III кв 2022	IV кв 2022	I кв 2023	II кв 2023
Заражение ВПО	25%	32%	79%	55%	56%	49%
Веб-атаки	10%	12%	0%	1%	1%	1%
Компрометация учетных записей	18%	5%	2%	10%	4%	4%
Эксплуатация учетных записей	0%	15%	4%	8%	7%	15%
Использование нелегитимного ПО	7%	7%	3%	8%	9%	4%
Сетевые атаки	7%	5%	1%	6%	8%	7%
Несанкционированный к информационным системам и серверам	16%	14%	4%	5%	6%	7%
Другое	17%	10%	7%	7%	9%	13%

Источник: Ростелеком-Солар, 2022-2023

Ключевые выводы

1. Объем рынка кибербезопасности Российской Федерации за 2022 год составил 193,3 млрд рублей с темпом прироста 20,8% относительно 2020 года и по прогнозам экспертов продолжит расти в ближайшие 5 лет с совокупным среднегодовым темпом роста (CAGR) в 24%, достигнув в 2027 году 559 млрд рублей. Основные факторы роста рынка: необходимость замены западных решений, повышенное внимание к кибербезопасности со стороны государства и рост хакерских атак во всех отраслях экономики в связи с геополитическими событиями 2022 года.

2. В структуре продуктов СЗИ выросла доля сегментов «защита рабочих станций» (конечных точек), «защита инфраструктуры», «защита приложений» в связи с повышением рисков реализации инцидентов, связанных с рабочими станциями и инфраструктурными объектами, а также адаптацией отечественных компаний к усилению контроля в части информационной безопасности со стороны государства.

3. В России на рынке продуктов СЗИ усиливается положение российских вендоров: в 2022 году они занимают 70% рынка (в 2021 году — 61%).

4. Топ-5 крупнейших вендоров средств защиты информации на российском рынке в 2022 году: «Лаборатория Касперского», Positive Technologies, Check Point Software Technologies, BI.ZONE, Cisco.

5. Лидеры в части оказания услуг информационной безопасности в 2022 году — «Ростелеком-Солар», «Лаборатория Касперского», BI.ZONE, Код Безопасности, Positive Technologies.

6. В 2022 году в России и СНГ наиболее атакуемыми отраслями по данным аналитического отчета «Лаборатории Касперского» были промышленность (24%), финансовые организации (20%), ИТ-компании (17%), транспорт (14%) и СМИ (12%).

7. По данным компании «РТК-Солар» количество событий информационной безопасности (подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний) в I полугодии 2023 года составило 615 тысяч, что на 47,8% больше, чем в аналогичном периоде 2022 года. При этом доля подтвержденных инцидентов в общем объеме сократилась на 22%. Злоумышленники генерируют большое количество «фонового шума», но для большинства компаний такие атаки не являются критичными и не влекут за собой последствий, однако при этом явно выделяются группы, координируемые централизованно.

8. В части распределения инцидентов по степени критичности в I полугодии 2023 года можно отметить низкую долю событий «высокой степени критичности» (3% в I квартале и 1% во II квартале 2023 года). Сложившиеся тренды демонстрируют повышение защиты ИТ-периметра российских компаний, несмотря на уход зарубежных вендоров.

9. Наиболее популярным инцидентом в I и II кварталах 2023 года, как и в целом в 2022 году, стало заражение ВПО (56% и 49% соответственно). Заметен тренд на увеличение доли сетевых атак и эксплуатации уязвимостей. Причина роста последних — переход российских компаний на отечественное ПО и наличие незащищенных областей в ИТ-периметре организаций.

Инструменты кибератаки

Доставка

Процесс кибератаки многоступенчатый и состоит из множества этапов, на каждом из которых требуется свой набор инструментов. Одной из первых задач хакеров является проникновение в сеть, компьютер, данные жертвы. Этот этап называется **«доставка»**. Для этого мошенники используют различные инструменты и уловки.

Фишинговая атака представляет собой поддельные уведомления от банков, провайдеров, платежных систем и других организаций, которые приходят на электронную почту или в мессенджеры жертвы. Как правило, такие сообщения содержат требование перейти по ссылке, иногда — очень похожей на адрес реального сайта реальной организации. Однако, если пользователь сделает требуемое, он попадет на фейковый сайт, где оставит пароли, реквизиты банковских карт или другую конфиденциальную информацию, находясь в полной уверенности, что производит все действия на официальной, а поэтому безопасной площадке. Фишинг — одна из разновидностей социальной инженерии, эксплуатирующей человеческие слабости, такие как алчность, тщеславие, чрезмерная доверчивость, лень, сострадание, поспешность в принимаемых решениях. Социальная инженерия — это эпидемия нашего времени, 91% атак на частных лиц реализовано именно этим способом, 50% атак на организации оказались успешны также благодаря человеческому фактору[50].

Мошенники прибегают к подобной практике, потому что так значительно проще добыть учетные данные, нежели взламывать системы безопасности. Социальная инженерия включает в себя «маскировку» под сотрудника компании, совершение телефонных звонков, отправку электронных писем и использование служб мгновенного обмена сообщениями, чтобы завоевать доверие жертвы, которая выдает личную информацию, невольно раскрывает коммерческие тайны и делится интеллектуальной собственностью компании, дает доступ к своему компьютеру.

Спам — еще один вариант воздействия на слабое звено в системе безопасности — человека, он представляет собой распространение нежелательных сообщений в любой форме и в большом количестве. Чаще всего спам отправляется в форме коммерческих электронных писем, через мгновенные и текстовые сообщения (СМС), социальные медиа, голосовую почту. Подобного рода сообщения могут носить рекламный или коммерческий характер, а также политический, «благотворительный», мошеннический (фишинг), «цепочечные письма» — письма с просьбой переслать знакомым и пр.

Близко к этой категории стоит и **телефонное мошенничество**, представляющее собой телефонную коммуникацию, где мошенники, играя определенную роль, выманивают деньги от имени родственника; шантажируют от имени работника правоохранительных органов; выманивают данные платежной карты или стимулируют к совершению операций по банковским счетам, представляясь сотрудником банка или службы безопасности; вынуждают установить мошенническое приложение или перейти по ссылке в СМС.

Одним из традиционных способов заражения техники и проникновения во внутренние сети компаний являются **физические носители**, когда злоумышленники загружают вредоносные программы на USB-накопители и ждут, пока их подключат к компьютерам. Этот прием, как правило, используется в корпоративном шпионаже и зачастую не обходится без социальной инженерии (злоумышленники используют доверчивость и невнимательность сотрудников компании).

Если социальная инженерия не сработала, хакерам приходится полагаться на свои силы и взламывать сети, серверы и веб-ресурсы, чтобы проникнуть в периметр жертвы. Как это может быть реализовано:

- **DoS-атака** (сетевая атака, Denial of Service — отказ в обслуживании) производится с целью срыва или затруднения нормальной работы веб-сайта, сервера или другого сетевого ресурса. При DoS-атаке вредоносные запросы отправляет одна система;

- **DDoS-атака** (Distributed Denial of Service — распределенная сетевая атака) исходит из нескольких систем, так называемых зомби-машин или ботнетов — сети удаленно управляемых устройств, зараженных вредоносным ПО. Цель атак — сделать систему жертвы недоступной и заблокировать доступ к серверам, устройствам, службам, сетям, приложениям и даже определенным транзакциям внутри приложений;

- **DeOS-атака** (Destruction of Service, прерывание обслуживания) выводит из строя компьютерную сеть или систему, приводя их к полному отключению. При такой атаке возможно уничтожение резервных копий и страховочных систем, позволяющих восстановить систему и данные после атаки. Появление интернета вещей (в том числе промышленного IIoT), когда все больше операций переводится в режим онлайн, расширяет горизонт атак и масштабы последствий.

На стадии разработки во все программы и сети встраиваются механизмы защиты от хакеров по типу замков, предупреждающих несанкционированные атаки извне. Уязвимости или дефекты безопасности могут обеспечить несанкционированный доступ вредоносных программ к компьютеру, оборудованию или сети.

Эксплойт — это фрагмент кода программы, который позволяет использовать уязвимости и получить несанкционированный доступ к приложению или операционной системе. Разработчики программ, выпуская обновления, устраняют найденные дефекты, но до этого момента программа является уязвимой для злоумышленников. Эксплойты часто являются исходной точкой для заражения системы вредоносными программами.

Атака на цепочку поставок эксплуатирует отношения между организацией и ее контрагентами (вендорами, поставщиками и пр.) для получения доступа к сети и системам компании-жертвы. Хакеры взламывают одну организацию, а затем продвигаются вверх по цепочке поставок, чтобы получить доступ к системам другой. Эта схема справедлива и для компаний-разработчиков ПО, когда продукт создается различными компаниями и после собирается в единый код, систему или приложение; а также для любых организаций, сотрудничающих с десятками поставщиков ингредиентов или производственных материалов, аутсорсинга технологий и пр.

Цепочки поставок могут быть значительными по охвату и сложными по взаимоотношениям, поэтому некоторые атаки сложно отследить. Подобные атаки действуют путем внедрения вредоносного программного обеспечения через поставщика или вендора, путем поиска небезопасных сетевых протоколов, незащищенных серверных инфраструктур.

Атаки на цепочки поставок бывают программными (внедрение вредоносного кода в программное обеспечение или выпускаемое разработчиками обновление), аппаратными (внедрение вредоносного ПО в оборудование, связанное со всей цепочкой поставок — веб-камеры, маршрутизаторы, клавиатуры). Например, клавиатурный шпион, который крадет пароли к учетным записям. И микропрограммными (внедрение вируса в загрузочный код компьютера для получения доступа ко всей инфраструктуре). Поэтому важно защитить не только периметр своей компании, но и цепочку поставок, проверяя компании-поставщики на предмет информационной безопасности.

Вредоносное программное обеспечение (ВПО) — это один из инструментов внедрения. Вредоносным считается любое программное обеспечение, предназначенное для тайного доступа к устройству без ведома его владельца, для доступа к информации, хранящейся в компьютерной системе, для скрытого нецелевого использования ресурсов системы, либо другого воздействия, препятствующего нормальному функционированию компьютерной системы.

Типов ВПО множество: черви, троянцы, шифровальщики, кейлоггеры и другие. Ниже описаны некоторые из них: что они из себя представляют, как работают и как внедряются в систему.

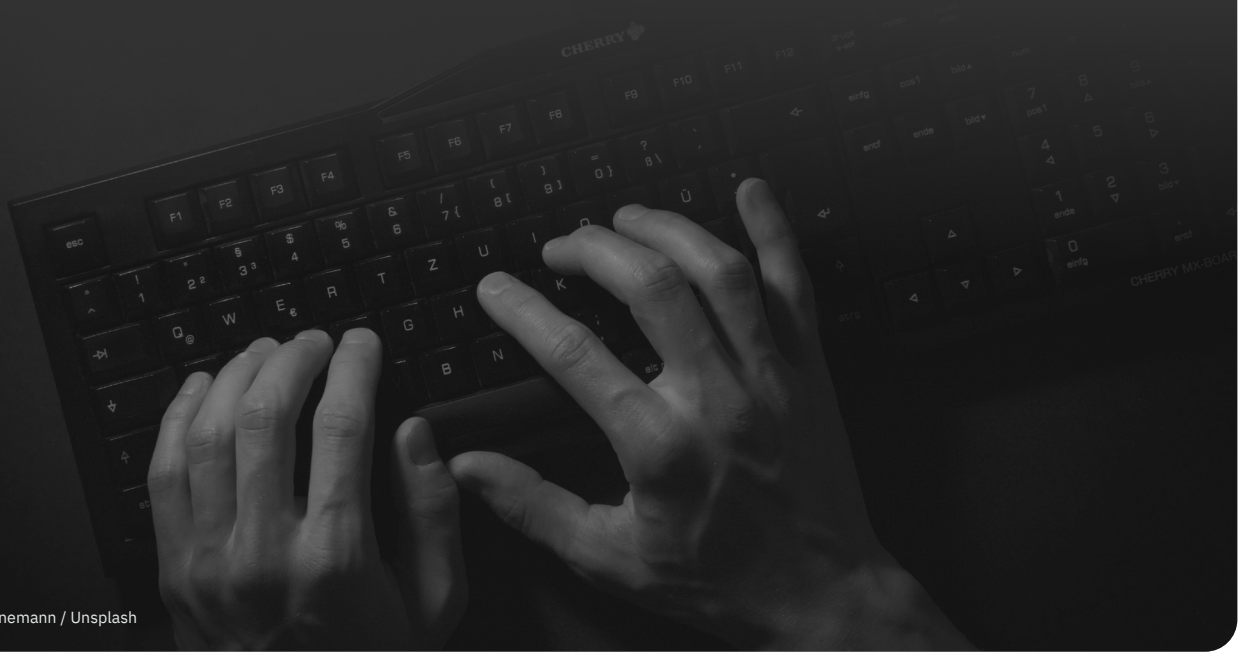


Фото: Stefan Heinemann / Unsplash

Внедрение

Проникнув или получив доступ к необходимому объекту, хакеры приступают к кибератаке. Этот этап называется **«внедрение»**. Исходя из цели, они выберут подходящий инструмент.

Червь — это вид ВПО, способный к автономному преодолению систем защиты автоматизированных и компьютерных систем, он самостоятельно распространяется, создавая собственные копии. В зависимости от путей проникновения в операционную систему черви могут быть: почтовыми, IM-черви (использующие интернет-пейджеры), P2P-черви (распространяющиеся при помощи пиринговых (peer-to-peer) файлообменных сетей), черви в IRC-каналах, сетевые черви (интернет черви, LAN-черви, распространяющиеся по протоколам локальных сетей). Большинство червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл, файл в каталоге обмена и пр. Из-за широкой доступности Интернета черви распространяются по всему миру за несколько часов или даже минут после появления. Последствия работы червя: замедленная работа компьютера, уменьшение места на жестком диске и объема свободной оперативной памяти, возникновение посторонних файлов, проблемы с работой какой-либо программы или приложения, появление ошибок, внезапное выключение и самопроизвольная перезагрузка компьютера, потеря данных. Черви могут кооперироваться с вирусами, такая пара самостоятельно распространяется (благодаря червю) и заражает ресурсы компьютера (используя функции вируса, может устанавливать троянцев, бэкдоры, шпионское ПО и пр.)

Троянец — программа, которая внешне выглядит как легальный программный продукт, но при запуске совершает несанкционированные пользователем действия: уничтожает, блокирует, модифицирует или копирует информацию, нарушает работу компьютеров или компьютерных сетей. Троянские программы не могут распространяться сами по себе, поэтому они проникают с помощью червей или через фишинг. Троянцы могут быть разных видов, но все они создаются для выполнения конкретной зловредной функции: бэкдор-троянцы (утилиты удаленного администрирования, часто включают в себя клавиатурные шпионы), троянцы-шпионы (отслеживают действия жертвы, в т.ч. нажатия клавиш и снимки экрана, сохраняют информацию и передают ее своему хозяину), троянцы для кражи паролей и другой учетной информации (могут извлекать сохраненные ключи из браузеров и утилит, анализировать кэш и файлы cookie и получать доступ к данным криптокошельков), троянцы-кликеры (превращающие компьютер в машину для рассылки спама, осуществления распределенной DDoS-атаки, увеличения дохода от переходов по рекламным ссылкам), троянцы-банкеры (крадут данные учетных записей электронных банковских систем, систем электронных платежей, пластиковых карт пользователей), троянцы-майнеры (программы, которые генерируют криптовалюту, используя мощности компьютера без ведома владельца).

Руткит (Rootkit) — вредоносная программа, предназначенная для получения злоумышленниками прав суперпользователя на устройстве без ведома жертвы, позволяющая скрыть присутствие вредоносного ПО в системе, которое под прикрытием руткита предоставляет злоумышленникам удаленный доступ, перехватывает сетевой трафик, шпионит за пользователями, похищает данные и пр. Руткиты не способны самораспространяться и, как правило, являются частью более сложных угроз в составе многофункционального ВПО. Задачей руткита становится маскировка нелегитимной активности (работы вирусов).

Программа-шпион скрытым образом устанавливается на компьютер пользователя с целью сбора данных о нем и его системе, не нанося вреда операционной системе, программам или файлам. Его присутствие практически незаметно для пользователя и часто не поддается обнаружению. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы или кейлоггеры), историю поиска, собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности вашей работы в Интернете, также они неизбежно снижают производительность компьютера. Некоторые приложения позволяют удаленно контролировать устройство, просматривать фотографии и файлы, хранящиеся на нем, подсматривать за человеком через камеру, видеть календарь, определять местоположение и пр. Шпионские программы чаще всего проникают на компьютер вместе с программами и файлами, загружаемыми с файлообменных сайтов или через фишинговую рассылку.

Программа-вымогатель атакует компьютерные системы, шифрует файлы в системе (шифровальщик), препятствует работе с браузерами или блокирует доступ к системе компьютера и требует оплаты за разблокировку. Такая программа может проникнуть на устройство через файл-вложение в сообщении электронной почты или через браузер в случае посещения сайта, инфицированного данным типом вредоносного ПО, из локальной сети.

Бэкдор (backdoor, черный вход) — программа, которую устанавливает хакер на взломанный компьютер с целью получения повторного доступа к системе. Бэкдоры родственны официальным утилитам для удаленного администрирования, но функциональность их шире: кроме управления процессами на уровне системы или Bios, бэкдоры могут воровать персональные данные, скачивать и отправлять по сети файлы, открывать доступ для вирусов и червей, подключаться к удаленным хостам, превращать компьютер в «зомби», делая его частью ботнета, и все это незаметно. Бэкдоры могут быть созданы разработчиком (намеренно или нет) как встроенная программная уязвимость или как способ обхода аутентификации и как дополнительный вариант доступа. Также они проникают на устройство во время загрузки файлов или как часть других ВПО.

Вайпер — это полезная нагрузка вредоносного ПО, которая полностью уничтожает, шифрует, либо перезаписывает все данные на диске компьютера-жертвы. Это самый разрушительный тип полезной нагрузки, который обычно используется военными в качестве кибероружия.

Рекламное ПО — программы рекламного характера, с помощью которых может распространяться разнообразное ПО. Они существуют за счет демонстрации нежелательной и навязчивой, а иногда и вредоносной рекламы. Чаще всего такие программы раздражают, но не представляют реальной угрозы безопасности. Однако некоторые (программы-угонщики браузеров) способны переадресовывать неправильно набранные или неполные URL-адреса на конкретные веб-сайты для сбора личных данных, отслеживания истории посещений и даже для перехвата вводимого пользователем текста; менять заданную домашнюю страницу, а также направлять поисковые запросы на платные веб-сайты. Иногда рекламная программа загружается и незаметно устанавливается с помощью троянца, также она может попасть в компьютер через уязвимость браузера или операционной системы, но чаще всего встраивается в стороннее ПО, распространяемое бесплатно.

Криптоджекинг (скрытый майнинг) — это тип киберпреступления, при котором вредоносное ПО скрывается в системе и похищает вычислительные ресурсы устройства, чтобы злоумышленники могли их использовать для добычи криптовалюты без ведома владельца. Такие программы могут объединяться в ботнет — сеть зараженных вредоносным ПО устройств, которая управляется хакерами из единого центра. Для эффективности майнинга обычно нужно заразить множество компьютеров, поэтому хакеры чаще обращают внимание на сети крупных компаний. Одна из основных проблем криптоджекинга — чрезмерная нагрузка на процессор и значительное замедление работы систем или полный сбой. Чтобы не вызывать подозрений, умные вирусы подстраиваются под активность пользователя: работают, когда компьютер свободен, и отключаются во время больших нагрузок. Чаще всего майнер попадает на устройство с помощью

дроппера, функция которого состоит в скрытной установке других программ. Дропперы обычно маскируются под пиратские версии лицензионных продуктов, которые пользователи находят на файлообменниках и скачивают.

Джекпотинг — установка и активация вредоносного ПО на банкомате и перехват контроля над ним. Получая доступ в BIOS устройства из-за минимальных требований к шифрованию и аутентификации, хакеры перенастраивают работу диспенсера и отправляют ему команду на выдачу всей имеющейся наличности. В результате за секунды банкомат оказывается пустым. Этот вид атак безвреден для пользователей, но наносит серьезный урон финансовым учреждениям.

Скимминг — вид мошенничества, когда злоумышленники крадут данные банковской карты (реквизиты, ПИН-код и др.) с помощью скиммера — специального считывающего устройства в виде пластиковой накладки на картоприемник, миниатюрной видеокамеры, переносного считывателя магнитной полосы и пр. Скиммеры накапливают информацию о пользователях и передают данные при помощи радиоканала или через встроенную сим-карту по сетям сотовой связи. Модернизированная версия скимминга, когда вместо накладок на картоприемник используется очень тонкая гибкая плата, считывающая магнитную полосу, называется шиммингом. Полученные данные используются для выпуска клонов карт, с которых позже снимаются средства.

SQL-инъекция — уязвимость веб-безопасности, позволяющая злоумышленнику вмешиваться в запросы, которые приложение делает к своей базе данных. Большинство сайтов отслеживает запросы типа «имя пользователя — пароль», и хакер может воспользоваться этим, чтобы отправить серверу свой запрос. Именно это и называется внедрением SQL-кода в базу данных. В результате хакеры могут создавать, считывать, обновлять, изменять или удалять данные, хранимые в серверной части СУБД, такие как номера социального страхования, данные банковских карт и др.

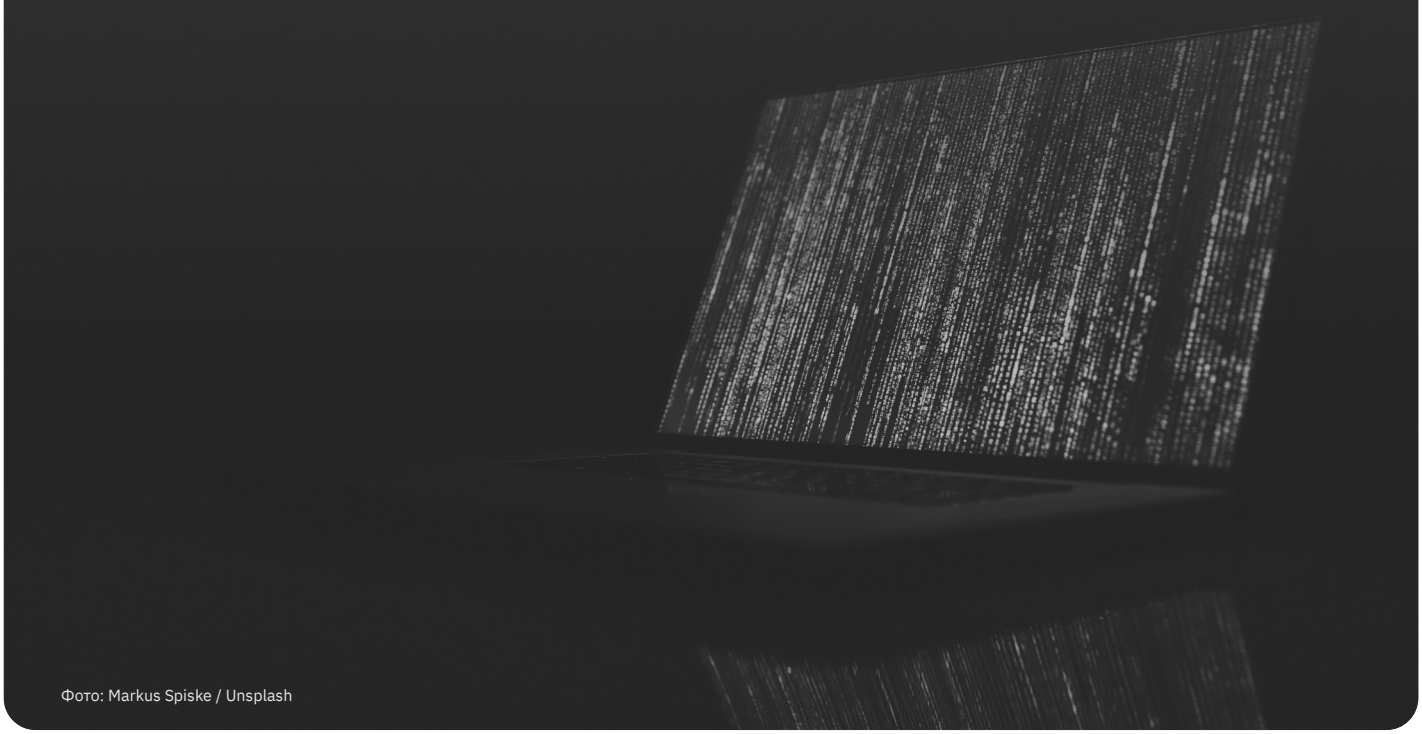
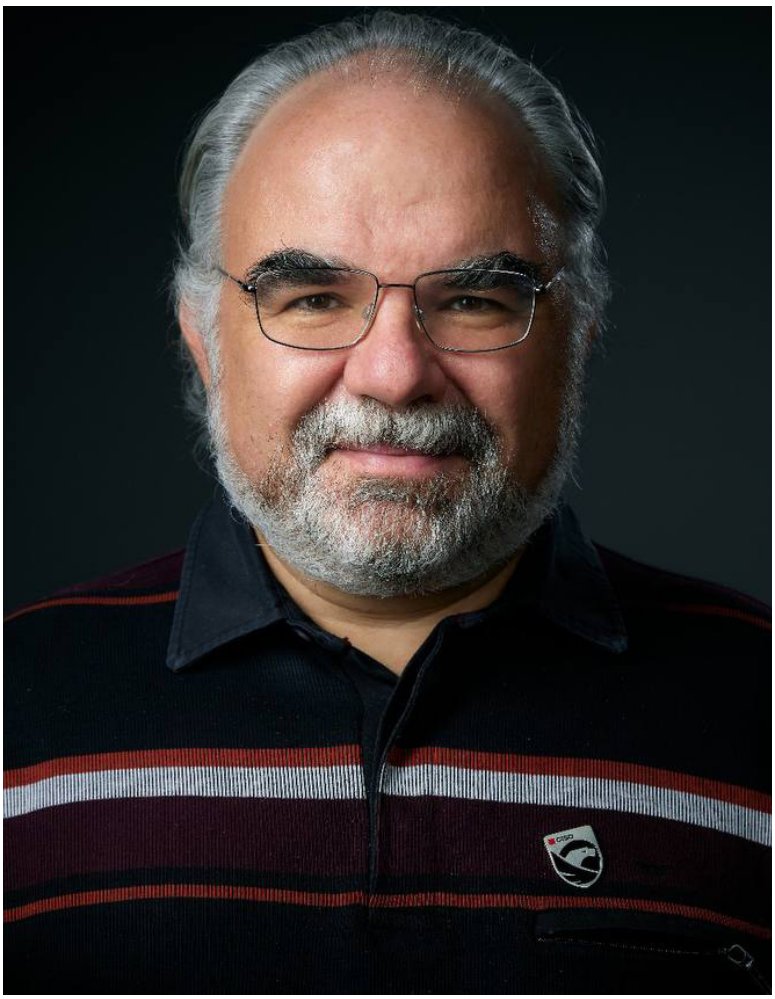


Фото: Markus Spiske / Unsplash

Алексей Лукацкий

Бизнес-консультант по информационной безопасности,
Positive Technologies

«Как только у компании появляется хоть какой-то информационный актив, она должна задуматься о кибербезопасности»



Беседовал Михаил Исаев

Фото: пресс-служба

УИ
Считается, что самым уязвимым местом в системе информационной безопасности все еще является человек. Насколько современные системы способны это нивелировать?

А. Л.
Надо понимать, что средства защиты создаются людьми, а им свойственно ошибаться. Так и выходит, что из-за некорректной разработки, неучета угроз или особенностей эксплуатации технологий в области кибербеза не выходит нивелировать человеческий фактор. Но в идеализированном мире технологии помогают сократить или выявить ошибки человека. Самый яркий пример — борьба с фишингом. Ежеквартально появляются сотни тысяч вредоносных доменов в интернете. Очевидно, что человек не способен выявить их самостоятельно, когда переходит по ссылке на сайт, поэтому здесь без технологий проблему решить невозможно. Хотя и технологии тоже не на 100% выявляют фишинговые домены, они существенно сокращают вероятность попадания пользователей на удочку мошенников. Существуют DLP-технологии, которые позволяют выявлять утечки информации, и сканеры безопасности для обнаружения оставленных разработчиками уязвимостей. Технологии способны снизить эффект от человеческого фактора как угрозы для кибербеза, но побороть на 100% при текущем уровне развития — нет. Возможно в перспективе, когда машина обучения разовьется до иных высот, ситуация поменяется кардинально.

УИ
В качестве предположения: в течение какого времени это может произойти?

А. Л.
Машинное обучение активно развивается. Если не будет законодательных ограничений на исследования в этой области и на применение таких технологий, я думаю, в перспективе двух-трех лет в отдельных нишах ML-решения сильно изменят ландшафт и сократят количество угроз. В каких-то нишах потребуется лет пять, чтобы выйти на совершенно другой качественный уровень обеспечения информационной безопасности.

УИ
Насколько система защиты зависит от отрасли, в которой работает компания? Если убрать за скобки политический контекст и увеличение атак на госучреждения, то какие отрасли в наибольшей степени подвержены киберугрозам?

А. Л.
Не существует универсального топ-3: он меняется, к примеру, не только от страны к стране, но и от квартала к кварталу. Где-то в прицел злоумышленников попадают финансовые организации. По нашей статистике, последнее время злоумышленники активно атакуют ретейл и образование. Для Запада характерны другие отрасли — фармацевтика и автомобильная промышленность. Можно сказать, что сегодня нет ни одной сферы деятельности, которая бы не столкнулась с хакерами. Хотя последнее время мотивация хакеров немного поменялась. Если раньше они атаковали в основном организации, которые могли заплатить выкуп, то сегодня основная задача — заявить о себе в геополитическом контексте.

УИ
Что компаниям выгоднее с экономической точки зрения: тратить деньги на системы защиты и пытаться предотвратить угрозу или же нести потери?

А. Л.
К сожалению, нет однозначного ответа. Все сильно зависит от конкретной организации и условий, в которых она будет осуществлять расчет. Надо признать, что у нас безопасность зависит от требований регуляторов, которые иногда избыточны или не учитывают специфику организации, поэтому затраты на приведение себя в соответствие могут быть больше, чем потенциальный ущерб в случае атаки. Среднестатистическая компания тратит на приведение себя в соответствие с законом о персональных данных от 12 млн до 60 млн рублей. А штраф на текущий момент времени за утечки персональных данных — 60 тыс. рублей. С другой стороны, если мы возьмем европейские требования по защите персональных данных и прав субъектов персональных данных, то там средняя цифра о приведении себя в соответствие — 1,3 млн евро, в то время как штрафы могут достигать десятков миллионов евро. Там картина прямо противоположная, то есть защита эффективнее экономически, потому что в случае инцидента можно попасть на большую сумму. Поэтому экономика в кибербезе — очень непростая тема, это высший пилотаж, к которому только начинают подступаться, и не всегда результаты устраивают тех, кто занимается экономическим расчетом.

УИ
Атаки, которые приводят к реальной остановке производственных мощностей, очень чувствительны для бизнеса и экономики. Как часто они бывают и как тяжело проходят?

А. Л.
В промышленной истории инцидентов гораздо меньше в сравнении со взломами соцсетей или банков, потому что монетизация этих действий не всегда понятна. Но, с другой стороны,

последствия гораздо более серьезны. Например, остановка ядерных реакторов — это, наверное, самый худший вариант. Подобные события, к счастью, носят единичный характер на сегодняшний день, но последствия от них будут более серьезными, чем от привычных нам киберугроз. Уже известны случаи попыток изменения рецептуры химикатов в системах водоочистки и отравления систем водоочистки.

УИ
В 2022 году в каждой второй успешной атаке на организации использовались шифровальщики и вайперы. Как часто в своей работе вы сталкиваетесь с такими атаками, сложно ли им противостоять?

А. Л.
За последние годы количество атак шифровальщиков и вайперов возросло. Если группировка хочет просто заявить о себе или нанести ущерб, после которого не получится восстановить данные, то обычно в качестве своего инструментария она использует вайперы. А если у группировки помимо этого есть еще и желание заработать, то, как правило, используются шифровальщики. Суммы выкупов за возврат данных доходят до сотен миллионов рублей. Но надо сказать, что у нас пока количество этих атак гораздо меньше, чем в Европе или Америке.

УИ
Какие хакерские группировки сейчас атакуют госучреждения и компании?

А. Л.
Все группировки совершенно разные и насчитывают от пары до нескольких сотен человек. Задачи у них тоже разнятся, начиная от шпионажа и заканчивая выведением из строя каких-то ресурсов или взломом веб-сайтов. Если представить пирамиду, то наверху у нас находится две-три высокопрофессиональные группировки, которые занимаются шпионажем, и об их деятельности мало известно. Обычно для таких взломов необходимо несколько недель: собрать информацию о цели, закрепиться, проникнуть внутрь и потом вытягивать данные незаметно для специалистов безопасности.

УИ
Насколько руководители осознают важность кибербезопасности и с какого момента развития компания должна задуматься о ней?

А. Л.
Как только у компании появляется хоть какой-то информационный актив, она должна задуматься о кибербезопасности. Даже индивидуальный предприниматель, у которого всего один компьютер, должен быть заинтересован в его защите, чтобы не потерять заказы, не сорвать сроки и не потерять персональные данные. Сейчас набирает популярность оценка эффективности информационной безопасности и инвестиций, сделанных в нее. Мы видим, что бизнес готов инвестировать большие средства в безопасность, но он готов и спрашивать за это. Поэтому специалисты по кибербезу должны изучать бизнес: понимать, как могут увеличить доходную часть и снизить расходную, в том числе через предотвращение штрафов и выплат выкупа шифровальщиком.
Самый яркий пример — автозаправочные станции. Мы думаем, что они зарабатывают деньги на топливе, а на самом деле основные деньги заправки получают на кофе. Получается, что на заправке надо защищать кофейный аппарат и процедуру оплаты этого кофе.

УИ
Какие системы должны быть в обязательном порядке у любой компании?

А. Л.
Как правило, основной результат в кибербезе можно достичь базовыми и правильными настройками, встроенными в инфраструктуру. Например, оперативное и автоматическое обновление операционных систем, приложений, плагинов к этим приложениям, внедрение многофакторной аутентификации, сегментация внутри инфраструктуры — все это уже закрывает до 90% всех кибергугроз. И только 5–10% достигается за счет дополнительных приобретений дорогостоящих игрушек. Сегодня на мировом рынке существует уже за сотню типов средств защиты, и у каждого из этих типов есть своя ниша.

Да и все упирается в то, что специалистам по безопасности необходимо автоматизировать свой труд, поэтому начинаются закупки Next-generation firewall, антивирусов, решений класса Endpoint detection and response. Если у компании есть свой сайт, то в обязательном порядке ставится Application Firewall, потому что 95% атак реализуются именно через взломы веб-сайтов. И как вишенка на торте — обязательное наличие решений класса Change Manager, которое позволяет выявлять то, что по отдельности средства защиты не выявляют.

УИ
Получается, что обеспечение кибербезопасности может быть бесплатным для компаний и нет необходимости в закупке дорогостоящих систем?

А. Л.
Элементы кибербезопасности должны быть бесплатными, как, например, настройка многофакторной аутентификации, обновление операционной системы или браузера. А так, конечно, компаниям нужны специалисты с квалификацией и желанием работать. Когда нет ни того ни другого, компании

начинают тратить много денег на то, что можно автоматизировать или решить в несколько кликов.

УИ
Можете дать совет обычным пользователям, чего делать точно не следует, чтобы не подвергать себя киберопасностям?

А. Л.
Здесь сложно давать советы, потому что поведение человека иррационально. Даже если мы говорим, что не надо регистрироваться в соцсетях, публиковать там фото, он все равно будет это делать. Всем полезно вовремя обновлять операционную систему, приложения и плагины, устанавливать пароли и делать резервное копирование данных — это основные вещи, которые можно сделать абсолютно бесплатно. А вот дальше, конечно, можно порекомендовать использовать антивирус для защиты стационарного компьютера или ноутбука. Но пока что наш рынок кибербезопасности никак не настроен на рядового гражданина.

УИ
Насколько российские системы конкурентоспособны в мире? Можно ли говорить, что уход иностранных вендоров в кибербезопасности прошел незаметно?

А. Л.
Сказать, что он прошел незаметно — невозможно, потому что 50% рынка, а в некоторых сегментах и до 100% рынка, занимали иностранцы. Что касается российских решений, то у нас есть аналоги почти для всех основных ниш в области кибербеза за редким исключением, и с иностранными решениями мы находимся на одном технологическом уровне, а по ряду направлений даже опережаем. Но у большинства российских вендоров есть большая проблема с удобством продукта и его эргономикой. Многие продолжают ориентироваться на регуляторов, которые не предъявляют никаких требований к удобству пользования средствами защиты и к качеству техподдержки. Поэтому, если российские игроки не пересмотрят свою стратегию и не будут выходить на международный рынок, чтобы конкурировать там с другими игроками, качество наших продуктов сильно упадет.

УИ
Какая-нибудь российская компания, на ваш взгляд, уже совершила рывок в сфере информационной безопасности?

А. Л.
С точки зрения корпоративного применения, сейчас происходит огромный всплеск интереса к теме инфобеза. Уже почти три десятка вендоров занимаются Next-generation firewall, и в этом или в следующем году появится еще около 20 продуктов в этой сфере. Достаточно активно сейчас развивается рынок поиска уязвимостей. Если раньше было два-три сканера, то сейчас их становится гораздо больше, то же самое касается и мониторинга сетевых аномалий. Рынок Application Security в России вообще растет семимильными шагами, потому что раньше там в основном были иностранные игроки. Поэтому конкуренция на российском рынке в следующем году будет достаточно жесткая и это, возможно, приведет к улучшению ситуации. Останутся те, кто сможет гибко реагировать на потребности пользователей не только по функциональности, но и по удобству применения продуктов.

УИ
В связи с санкциями одной из проблем стал недостаток «железа». Как отечественный рынок кибербезопасности справляется с этим?

А. Л.
Сейчас появляются российские компании, например, Yadro, «Аквариус», Kraftway, которые выпускают собственное «железо». Поэтому серьезной проблемы я сейчас не вижу, хотя в первый год с момента блокировки поставок она была. Сейчас уже логистика налажена, в Китае и внутри страны активизировалось производство.

УИ
Как должна измениться кибербезопасность, если экономика будет идти в сторону цифровизации, автоматизации и внедрения интернета вещей, искусственного интеллекта и роботов?

А. Л.
На мой взгляд, кибербезопасность должна развиваться по трем направлениям. Первое направление — идеология Security by design. Она предполагает, что мы начинаем думать о безопасности еще до начала разработки архитектуры. Например, при разработке беспилотных автомобилей сразу закладываются механизмы защиты. Второе направление связано с учетом угроз для прорывных технологий — это биохакинг, Web 3.0, соответственно, блокчейн, VR/AR и искусственный интеллект. И третье направление — сетевая безопасность, которая подразумевает анализ сетевых коммуникаций и их защиту.

От крипера до вайпера

Как развивались киберугрозы

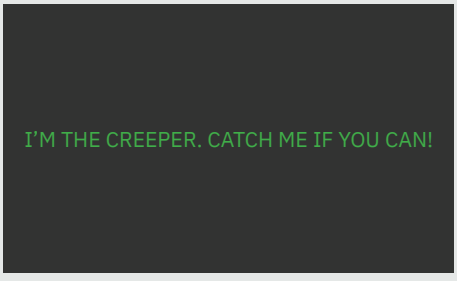
Фото: Wikipedia, Unsplash

Не все вирусы создавались как вирусы, часть программ разрабатывалась энтузиастами и просто экспериментаторами, а дальше, как часто бывает, процесс распада атома можно использовать для обеспечения людей энергией (АЭС), а можно для уничтожения (атомные бомбы). Мы проследили путь киберугроз от первых программ и вирусов, до наших дней, выделив главные вехи, когда веб-мир сталкивался с новыми типами и видами киберугроз.

1971

Creeper, первая самовоспроизводящаяся программа

Creeper стала первой программой, которая самостоятельно могла перемещаться по компьютерной сети и создавать собственные копии. Не являлась ни вирусом, ни «червем», при этом она стала предвестником развития методов распространения вредоносного ПО.



1974

Вирус Rabbit

Самовоспроизводящаяся программа, способная привести к отказу компьютера за счет создания множества собственных копий.

1975

Первый «троянец» Animal

Один из первых «троянцев» (программа Prevade) был создан автором компьютерной игры Animal и поставлялся вместе с игрой как средство, упрощающее копирование игры для новых пользователей. Хотя программа и не преследовала вредоносных целей, она осуществляла копирование игры во все папки на компьютере, где ее не обнаруживала, и таким образом соответствовала признакам «троянца».

1986

Brain. Первая глобальная эпидемия

Программа была создана братьями Алви из Пакистана для защиты своего ПО от нелегального копирования. Она при копировании ПО меняла имя дискеты на «(c) Brain», помечая таким образом нелегальную копию. Вирус не портил данные и стал первым вирусом-невидимкой, способным прописывать без пользовательского разрешения фразу «(c) Brain» на дискетах.

1988

Пятница-13. Вирус с «логической бомбой»

Вирус родом из Израиля заражал файлы с расширениями .com, .exe, .sys и распространялся путем самокопирования на дискеты, пересылки по электронной почте и т.д. Вирус приводил к сокращению доступной памяти, замедлял работу компьютера, а каждую пятницу, выпадающую на 13 число месяца, удалял с компьютера все файлы, которые были использованы в тот день. Действовал циклично до момента нейтрализации. Это один из самых известных вирусов в истории благодаря массовости и «зловещему поведению».

1995

Появление макровирусов и их распространение

Первый вирус на макроязыке, заражавший текстовый процессор MS Word, получил название «Concept». Носителем вируса был текстовый документ Word, который мог инфицировать любую операционную систему, поддерживающую работу с документами MS. Любой документ, созданный на таком компьютере, становился носителем вируса. В конце второго тысячелетия макровирусы обзавелись функциями почтовых «червей», что обеспечило экспоненциальный рост «заразности».

1998

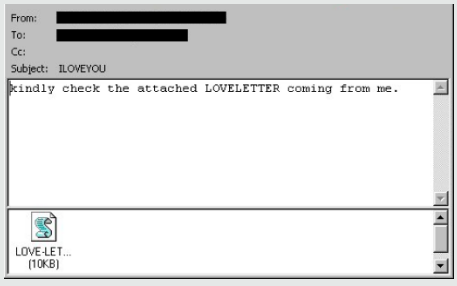
«Чернобыль», активируется 26 апреля

Вирус был создан тайваньским студентом Чэнь Инхао с целью доказать неэффективность антивирусных программ. Заражение началось с компьютеров университета Датун. Вирус быстро распространялся по компьютерным сетям, а эпидемия случилась 26 апреля в 1999 году, после наступления установленного дня X — дня активации «логической бомбы». При запуске вирус загружает свой код в память Windows, перехватывает EXE-файлы и записывает в них свою копию, стирает содержимое дисков и микросхем BIOS. Автор вируса признался в создании вредоносной программы и принес публичные извинения в интернете всем гражданам Китая, чьи компьютеры пострадали.

2000

«ILoveYou»

Первый «червь», который вызвал глобальную эпидемию вследствие развития широкополосного интернета. Распространялся классически по электронной почте в виде вложенного скрипта Visual Basic с темой письма «I love you». «Червь» заражал компьютер жертвы, а затем рассылал свои копии всем контактам. Пользователи без опаски открывали инфицированные письма от знакомых, что подтвердило высокую эффективность социальной инженерии.



2000

Эпидемии «червей» через почту, веб, пейджеры

2009

Backdoor, первый «троянец» для банкоматов

Превращает весь банкомат в скимминговое устройство, позволяющее считывать данные карт жертв.

Вирусы-шпионы, взлом Пентагона, похищение информации о вооружении

Группа хакеров в результате атаки с использованием вируса-шпиона взломала серверы Пентагона и похитила несколько терабайт данных. Доставка вируса производилась через фишинговые письма, электронные носители и пр., далее вирус оставался в сети незамеченным, находил нужные файлы и пересылал их «хозяину» по сети. В частности, была украдена информация о новом истребителе пятого поколения известном как F-35 Lightning II.

2010

Stuxnet, первое кибероружие

Stuxnet использовался в атаке на ядерную программу Ирана для саботажа процесса по обогащению урана на некоторых заводах. «Червь», проникнув в сеть через инфицированный USB-накопитель, позволил хакерам получить доступ к промышленному компьютеру в Натане (Иран), и, используя его уязвимости, вывести из строя центрифуги по обогащению урана.

2011

Утечки данных, взлом PlayStation Network (PSN), похищение данных 77 млн пользователей, что привело к отключению сервиса по всему миру

2014

Heartbleed, уязвимость в криптографической библиотеке OpenSSL (протокол шифрования)

Позволила хакерам получить доступ к содержимому оперативной памяти серверов, где содержались личные данные пользователей (логины, пароли, данные кредитных карт и пр.), цифровые ключи для шифрования переписки и внутренних документов компаний и т.д.

Moker, «троянец» нового поколения

Открывает протоколы подключения к RDP-каналам (удаленным рабочим столам), предоставляя «хозяину» полный контроль над устройством жертвы.

2017

Эпидемия сетевого «червя»-вымогателя Wannacry

Программа сканировала диапазон IP-адресов локальной сети в поисках компьютеров с уязвимостью в операционной системе Microsoft Windows, после чего устанавливала бэкдор, через который загружался и запускался исполняемый код программы WannaCry. При этом для загрузки на компьютер от пользователя не требовалось никаких действий. Заражая компьютер, «червь» шифровал почти все файлы, а затем требовал выкуп в криптовалюте для расшифровки.

2019

Таргетированные атаки на инфраструктуру

Ярким примером целенаправленных атак стала деятельность группировки Calypso, атаковавшей государственные структуры шести стран. Хакеры получали доступ к внутренним сетям жертв путем взлома сетевого периметра и размещением в нем ВПО (вредоносного программного обеспечения). Продвигались во внутреннем сетевом периметре преступники с помощью эксплуатации уязвимостей или с использованием украденных учетных записей. Целью таких атак, как правило, является некая компания или государство, а целью — воровство данных, шпионаж или шантаж.

2020

CovidLock и другие вымогатели

Вирус-шифровальщик для Android CovidLock появился на заре пандемии коронавируса. Преступники создали сайт для отслеживания ситуации по пандемии с предложением установить мобильное приложение для оперативного информирования пользователя. Android-программа получала права администратора под видом запросов на оптимизацию батареи устройства и проч., после чего происходила атака, блокировка устройства и требование выкупа.

Маскировка вредоносного ПО под сервисы видеоконференций

2021

Волна атак на веб-ресурсы

Яркий пример — атаки на ресурсы Wordpress и Magento через эксплойты (вредоносные коды, использующие ошибки или недостатки системы безопасности), которые позволяли внедрять на серверы «троянцев» посредством эксплуатации уязвимостей веб-сайтов. Хакеры взламывали сайт, заменяя или дополняя первоначальный код страницы. После чего путем оформления заказа, создания нового аккаунта и пр. на сервер уходил запрос с эксплойт-кодом. Получив доступ к серверу и его бэкенду, хакеры воровали данные с целью их продажи или шантажа.

Атака на Calonial Pipeline

Атака приостановила на шесть дней транспортировку топлива по трубопроводу компании Calonial Pipeline. До сих пор нет достоверных данных, как вредоносный код проник в систему жертвы. Среди вероятных схем проникновения — фишинг, эксплуатация уязвимостей, использование украденных учетных данных сотрудников к удаленным рабочим местам и проч.

2022

Взломы блокчейн-мостов и кража криптовалюты

Самый крупный инцидент — взлом моста (звено, обеспечивающее связь и взаимодействие между двумя блокчейнами) блокчейн-платформы Ronin, поддерживающей блокчейн-игру Axie Infinity. Неизвестные хакеры совершили фишинговую атаку, получив доступ к инфраструктуре компании и валидаторам. В сети Ronin для подтверждения транзакции нужны были подписи 5 из 9 валидаторов. Хакерам в результате взлома блокчейн-моста удалось похитить и вывести более 600 млн долларов.

Массовые атаки на госучреждения и ретейл

Политическая обстановка в мире обуславливает рост хактивизма (политически мотивированных хакеров), при этом доля успешных атак с использованием ВПО финансово мотивированных преступников посредством шифровальщиков и вымогателей превысила 50% от их общего числа.

Развитие модели фишинга как услуги (Phishing-as-a-Service, PhaaS)

Преступники становятся провайдерами услуг фишинга, взлома, шифрования, предоставляя за оплату личные данные, аккаунты, доступ к данным и пр.

Ярослав Каргалев

Руководитель Центра Кибербезопасности F.A.C.C.T.,
экс-руководитель группы мониторинга и реагирования на инциденты информационной безопасности CERT-GIB компании Group-IB

«Первый рубеж для хакера — человек, и обойти его проще всего»

Беседовал: Константин Евсеев
Фото: пресс-служба

УИ

Мы просмотрели много информации по кибербезопасности и самыми интересными нам показались кейсы с расследованиями. Есть ли у вашей компании кейс, с помощью которого удалось предотвратить серьезную атаку, найти критическую уязвимость или выйти на след киберпреступников?

Я. К.

Да, есть довольно много подобных кейсов, которыми мы гордимся, но не все из них публичные. Из того, что можно назвать: мы участвовали в совместных с правоохранительными органами операциях по ликвидации преступных групп Carberp, Cron, TipTop, которые атаковали клиентов ведущих российских банков. Благодаря этому в России практически сошла на нет преступная активность с использованием банковских троянов. Вы удивитесь, но нашим специалистам приходится работать не только с уголовными преступлениями. Например, несколько лет назад организаторы шоу «Голос» просили нас провести исследование, использовались ли накрутки при голосовании. Мы подтвердили «аномалии» и руководство Первого канала учло наши рекомендации.

Вот еще, например, последний хороший кейс — помощь МВД в ликвидации группы мошенников, которая на протяжении полутора лет похищала деньги у россиян, решивших воспользоваться популярным сервисом по поиску попутчиков. Осенью прошлого, 2022 года, в ходе совместного расследования полицейские и специалисты нашей компании вычислили и задержали жителя Ижевска, который признался в создании фишинговых сайтов. Интересно, что до суда ему была избрана мера пресечения в виде подписки о невыезде, но мы продолжили за ним наблюдать. И даже находясь под следствием, этот гражданин продолжил заниматься мошенничеством. Опрометчивое решение. В мае 2023 года МВД сообщило о ликвидации всей преступной группы — задержания и обыски прошли одновременно в нескольких регионах России.

УИ

А как ведутся расследования кибератак, есть какие-то основные принципы?

Я. К.

Расследование кибератак требует времени, процесс схож с традиционным расследованием — нужно собрать как можно больше данных и на их основе провести идентификацию преступников. Сегодняшние технологии при правильном использовании позволяют хакерам сохранять анонимность. Но происходят новые атаки, данные о них накапливаются. И вот по не связанным, на первый взгляд, данным можно построить аналитику, составить профиль поведения злоумышленников и идентифицировать хакеров. В такой идентификации часто помогает шаблонное поведение — особенности развертывания сетевой инфраструктуры, выбор хостинг-провайдеров, использование IP-адресов, доменных имен, почт, аккаунтов в мессенджерах. Мы исследуем эти разрозненные данные и находим закономерности в поведении злоумышленников в сети, что позволяет вычислить индивидуума или целую преступную группу. Особенно важно правильно собрать данные, чтобы эффективно использовать их в суде и доказать вину всех членов группировки. Важно понимать, что за всеми киберпреступлениями стоят люди, которые совершают ошибки, что часто и позволяет нам установить личность злоумышленников.

Хочу еще раз подчеркнуть, что сегодня важно тесное взаимодействие частных компаний из сферы кибербеза с правоохранительными органами. Только исключительно совместными усилиями можно добиться ареста киберпреступников. Киберпреступность — транснациональна, зачастую члены преступной группы могут быть географически распределены, и, находясь в одних странах, совершать кибератаки на объекты из других. Разрыв отношений между государствами из-за текущего геополитического кризиса играет на руку хакерам, поэтому они могут действовать более активно, открыто и безнаказанно. Ведь ничто не мотивирует совершать преступления в таком количестве, как чувство безнаказанности.

УИ

Как вы думаете, почему многие талантливые программисты выбирают такой карьерный путь и становятся хакерами?

Я. К.

Сегодня невозможно описать собирательный образ хакера, такого типового портрета не существует. Это достаточно разношерстная аудитория, и поэтому причины выбора такого пути тоже отличаются. Сначала нужно понять мотивы — зачем вообще совершается киберпреступление. А традиционно основная цель киберпреступлений заключается в заработке денег. Можно атаковать физическое лицо с целью похитить у него денежные средства, хранящиеся на криптокошельках, на банковском счете. Можно атаковать организацию с целью похитить денежные средства на ее балансе. Можно еще похитить информацию, нарушить бизнес-процесс и далее заниматься шантажом. Это основная масса сегодняшних киберпреступлений.

Злоумышленники с данной мотивацией, как правило, имеют высокие технические компетенции, но ограничены в ресурсах, например, во времени. Если хакеры понимают, что при атаке конкретной цели будет затрачено слишком много усилий, то они просто перейдут к другой. Сегодня в России мы видим некую территориальную закономерность: в большинстве случаев финансово мотивированные хакеры — это выходцы из регионов со сложной и неблагоприятной экономической обстановкой. Бывает так, что человек просто не может реализоваться на «белой стороне» как ИТ-специалист, поэтому он переходит на «темную».

Следующий мотив — шпионаж и диверсии. Здесь, как правило, кибератаки проводятся спецслужбами или прогосударственными группировками. Такие группы хорошо организованы, мотивированы и зачастую не ограничены в ресурсах. Участниками таких групп могут быть люди на службе или контрактники, например, по ИТ-специальности. Часто такие группы вербуют хакеров, которые ранее промышляли атаками с целью заработка, потом были пойманы и получили предложение, от которого невозможно отказаться — сесть на много лет или поработать в интересах страны, где был пойман.

Последний мотив на сегодняшний день — хактивизм, совершение преступлений по идеологическим или политическим мотивам с целью дестабилизации деятельности организаций или обстановки в обществе. Последний год мы называем «Годом хактивизма», потому что многие киберпреступники активизировались и начали проводить атаки в соответствии с той позицией, которую они занимают в нынешнем конфликте.

УИ
Считается, что слабым звеном в системе кибербезопасности остается человек. Так ли это, и могут ли системы кибербезопасности это нивелировать?

Я. К.
Да, человек в кибербезе — по-прежнему самое уязвимое место, это видно по ежегодно растущим фишинговым вредоносным email-рассылкам. Даже несмотря на то, что компании инвестируют огромные суммы в защиту от киберугроз, злоумышленники продолжают получать доступ к инфраструктуре, просто используя различные уловки, нацеленные на человека. Конечно, применение средств защиты не решит сразу все проблемы, потому что не бывает стопроцентной защиты. Получится лишь снизить вероятность успешной атаки, но не исключить ее полностью. Первый рубеж для хакера — человек, и обойти его проще всего. Я всегда и всем говорю, что кибербезопасность должна быть комплексной: кроме внедрения средств защиты информации должна проводиться работа с людьми — обучение их безопасной работе, внедрение внутренних регламентов и процедур, которые позволят обезопасить действия сотрудников в корпоративной сети и в интернете.

УИ
Интернет вещей сейчас все больше проникает во все сферы жизни. Насколько чувствителен интернет вещей в производстве?

Я. К.
Для хакеров IoT, или интернет вещей, — это лишь возможность или точка доступа, позволяющая сегодня эффективно проводить атаки. Например, цель — остановка производственных мощностей компании с целью ее шантажа. Какой-то уязвимый сенсор на производстве, подключенный к интернету, будет лишь первой целью во всей цепочке атаки. Если не будет этого уязвимого сенсора, то атакующие выберут другой вектор атаки, например, фишинговое письмо инженеру производства с целью получить доступ к его персональному компьютеру. Поэтому я не придавал бы какого-то такого особого значения именно Io T. Производители ПО и IoT в перспективе заложат больше безопасности в архитектуру, и злоумышленники с этого вектора перейдут на другой, вот и все.

УИ
В прошлом году каждая вторая успешная атака была совершена с использованием шифровальщиков и вайперов. Как часто вы в своей работе сталкиваетесь с подобными атаками и сложно ли им противостоять?

Я. К.
Уже четыре последних года шифровальщики остаются киберугрозой номер один и останутся ею в 2024 году. Киберпреступники с помощью шифровальщиков получили в руки инструмент монетизации атак независимо от отрасли и сферы деятельности жертвы. Одной из причин распространения вымогателей стало появление партнерских программ. Вот взломал кто-то компанию, а как ему заработать на этом? Партнерские программы часто объединяют разных людей, каждый из которых разбирается в определенной сфере, но по отдельности не может заработать на своих умениях. Разработчик шифровальщика получает процент за успешную атаку, когда жертва заплатила денежные средства. Группа, которая занимается распространением вредоносной программы,

получает процент от операторов за то, что в рамках рассылки жертва заразилась и заплатила выкуп. Наша Лаборатория цифровой криминалистики за первую половину этого года, участвуя в расследованиях киберпреступлений, столкнулась с тем, что уже 9 из 10 инцидентов были связаны именно с программами-вымогателями. В целом количество атак программ-вымогателей в России в этом году выросло на 50–60% по сравнению с прошлым годом. Сегодня эта деятельность связана еще и с хактивизмом. Все чаще киберпреступники применяют шифровальщиков и тех же самых вайперов не с финансовой мотивацией, а с целью скрыть свои следы и реальные мотивы, запутать ход расследования.

УИ

А можете выделить любимые приемы у хакеров и мошенников?

Я. К.

Знаете, у каждой группировки есть свои излюбленные популярные техники проведения атак. Как я уже говорил, самый популярный вектор первоначального доступа — социальная инженерия, а именно фишинговые рассылки, особенно красочные и грамотно оформленные электронные письма, в которых эксплуатируется актуальная повестка. Потенциальные жертвы думают, что это письма по работе, открывают их и запускают приложенные к письму вложения, которые на деле содержат вредоносный код. В результате на компьютере оказывается вредоносная программа, например, стиллер, похищающая все учетные записи жертвы, хранящиеся на скомпрометированном компьютере. Далее атакующие будут использовать похищенные учетные данные для развития своей атаки. Еще один излюбленный способ как первичный вектор проникновения в инфраструктуру — использование уязвимостей в ПО на периметровом оборудовании, например, IoT или сервере. Другие популярные у хакеров приемы появились с введением удаленного и гибридного формата работы, потому что границы ИТ-инфраструктуры размылись: работник изначально не находится в локальной сети — он к ней подключается извне. Поэтому атакующие начали активно подбирать слабозащищенные корпоративные учетные записи в сервисах удаленного доступа или VPN.

УИ

По итогам прошлого года доход хакеров-вымогателей снизился на 40%. Почему, с вашей точки зрения, жертвы стали все чаще отказываться от уплаты выкупа?

Я. К.

Сначала скажу подробнее про выкупы. Изначально компаниям достаточно сложно определить все последствия от совершенной атаки. Они могут преследовать бизнес еще много лет. Это, например, удар по репутации, который сложно выразить в денежном эквиваленте. Шифровальщики применяют сейчас тактику двойного вымогательства, чтобы жертва была сговорчивей. Они не просто шифруют компьютеры, проникнув в сеть. Они тихо изучают ее, распространяются на большее количество узлов, собирают информацию, похищают ее и только после этого шифруют инфраструктуру, в том числе выводя из строя бэкапы. И теперь, если жертва отказалась от выкупа за расшифровку своей инфраструктуры, хакеры угрожают выложить все похищенные данные в интернете. Как правило, тут уже совсем другие риски. Если раньше мы говорили про риск остановки бизнес-процессов и операционной деятельности компании, то в этом случае, который я описал, появляется угроза утечки информации, в том числе клиентской, например, персональных данных, а это уже ответственность на уровне законодательства. Именно поэтому сегодня мы слышим такие невероятные суммы выкупа, которые требуют атакующие. Например, есть группировка Гремлины («OldGremlin»), она специализируется на атаках шифровальщиков в России и странах СНГ. И вот от одной из российских компаний они требовали 1 млрд рублей выкупа за восстановление доступа к инфраструктуре. Тут хочется отметить, что нет еще точной картины происходящего, например, мы не знаем, кто из компании заплатил выкуп. Как правило, те, кто платит, об этом особо не говорят. Поэтому сказать, почему сейчас упал доход у хакеров, достаточно сложно.

УИ

Как вы оцениваете общую культуру руководителей наших компаний в сфере кибербезопасности, насколько они реально осознают необходимость развития этого направления?

Я. К.

Анализируя результаты опросов компаний, я вижу, что ландшафт киберугроз кардинально изменился за последние несколько лет. Теперь жертвой атаки может стать любая компания, независимо от размера, сферы и места деятельности: региональный малый бизнес, крупная федеральная компания, образовательное учреждение, медицинская организация, государственное предприятие, — повторюсь, любая… Кибератаки приобрели массовый характер, и тут хочется отметить, что чем раньше на пути своего развития компания всерьез задумается о кибербезопасности, тем дешевле ей выйдет внедрение средств защиты и меньше

будет последствий от атак. Мы видим, как бизнес начинает вкладываться в кибербезопасность, ведь сегодня кибератаки становятся одной из основных угроз для его существования.

УИ
Что бизнесу защищать в первую очередь, какие места самые уязвимые?

Я. К.
Нет какого-то общего шаблона. Кибербезопасность должна реализовываться на основе ландшафта угроз определенной компании. И при разработке этой персональной модели угроз должно учитываться множество факторов: размер ИТ и штата, индустрия, партнерские отношения, количество подрядчиков, ретроспектива предыдущих атак на отрасль — именно эта информация должна быть отправной точкой при выстраивании эффективной защиты, иначе компания просто потратит впустую много денег на предотвращение нерелевантных угроз. Часто бывает так, что мы приезжаем на реагирование на случившийся инцидент в крупную компанию и видим, что у нее есть своя служба безопасности с большим штатом специалистов, но, тем не менее, инцидент произошел, а это значит, что что-то не так. Нельзя выстраивать защиту только на основе того, что так делают все. Нельзя просто обложиться средствами защиты и почувствовать себя в безопасности. Бизнесу необходимо знать свой периметр, следить за трафиком компании, проводить независимый аудит безопасности и закрывать наиболее эксплуатируемые векторы атак в ее отрасли и в общих случаях, например в виде фишинговых рассылок. В последнем случае поможет обучение сотрудников кибербезопасности: они должны хотя бы частично понимать риски и знать, куда обратиться в случае какого-то подозрительного события. Должна быть простая коммуникация с ИБ-подразделением: «Здравствуйте, что-то пришло подозрительное. Проверьте, пожалуйста». Если этого не делать или этот процесс сложен, то сотрудник, скорее всего, проигнорирует этот инцидент, а это рано или поздно приведет к серьезным последствиям.

УИ
Как вы можете оценить конкурентоспособность российских вендоров в сфере кибербезопасности? Можно ли говорить, что уход иностранных компаний сильно повлиял на нас?

Я. К.
Могу сказать, что в России сегодня существует очень сильный конкурентный рынок комплексной кибербезопасности. Не каждая страна имеет таких крупных вендоров и в таком количестве. Я вообще считаю, что в России импортозамещение лучше всего проходит именно в сфере кибербезопасности, потому что у нас есть серьезные альтернативы, и в некоторых случаях они даже лучше западных продуктов. Это связано с тем, что в России всегда был высокий риск кибератак. И раскрылся этот риск намного раньше, чем в других странах. На рубеже 2010-х годов Россия была неким полигоном для киберпреступников. То есть, на наших финансовых организациях и компаниях хакеры оттачивали тактики проведения атак. Они учились, и для отечественных компаний это тоже были дорогие уроки. Потом киберпреступники начали атаковать организации по всему миру, а наши вендоры кибербезопасности, первыми столкнувшись с масштабом киберугроз, стали развивать и предлагать эффективную защиту.

УИ
А какие отечественные разработки вы бы выделили?

Я. К.
У нашей компании есть молодой облачный продукт Attack Surface Management. Мы первые в России, кто запустил этот класс решений. Это ответ на сегодняшнюю активную цифровизацию бизнес-процессов в компаниях, которая приводит к появлению скрытых неоднозначных рисков в инфраструктуре, связанных с теневыми активами и некорректной конфигурацией. Наш продукт обеспечивает полный мониторинг всех доступных извне цифровых активов организации, дает возможность компании увидеть свою инфраструктуру глазами атакующих. Обогащая собранную информацию данными сервиса нашей киберразведки, мы позволяем клиенту выявить все активы с высоким для него уровнем риска и даем инструмент, позволяющий правильно подстроить инфраструктуру под текущую повестку кибербезопасности.

УИ
Можете дать совет обычным людям, которые пользуются интернетом, как избежать киберугроз?

Я. К.
Здесь все вертится вокруг простого соблюдения цифровой гигиены. Нельзя скачивать и устанавливать ПО из непонятных источников, только с официальных сайтов или магазинов приложений. Необходимо использовать двухфакторную аутентификацию везде, где это возможно, оплачивать покупки в интернете отдельно созданной для этого картой с установленным лимитом. Да, не всегда это удобно, но это дело привычки. Безопасность — это всегда компромисс с удобством. А еще я рекомендую обезопасить

SIM-карту: прийти в офис оператора и написать заявление на запрет ее перевыпуска по доверенности. Перевыпустив вашу SIM-карту, используя простую поддельную доверенность, злоумышленники могут получить доступ к аккаунтам, которые привязаны к определенному номеру телефона, например к интернет-банку или к социальным сетям. И не проверяйте себя в ботах, которые предлагают возможность по небольшому количеству данных о человеке узнать о нем всю основную информацию, даже номер СНИЛС. Часто эти боты работают так, что собирают от вас данные в единую базу. Не стоит говорить, как она может использоваться в дальнейшем, да?

УИ
Как вы видите кибербезопасность в России в перспективе 5–10 лет, куда движется эта сфера?

Я. К.
Достаточно сложно сейчас делать прогнозы на долгосрочную перспективу, потому что все меняется кардинально даже в короткий срок. Что тут могу добавить? Думаю, автоматизация будет иметь особое значение в предотвращении и обнаружении атак, в расследовании преступлений. Например, можно взять такое классическое направление, как Security operations center, — отделы мониторинга. Вот на протяжении последних полутора лет мы видим, как все компании побежали строить отделы мониторинга, а на рынке не хватает кадров под это несмотря на то, что порог входа в профессию достаточно низкий. Я уверен, что в ближайшее время все эти отделы начнут сокращаться именно по причине автоматизации своей деятельности и применения более продвинутых инструментов киберзащиты, в ядре которых будет задействован искусственный интеллект.

УИ
Можете поделиться условным топом хакерских группировок, приемов, наиболее опасных для реального сектора экономики?

Я. К.
Если говорить о типах угроз, то на первом месте стоят шифровальщики. Наиболее часто используемыми и опасными программами-вымогателями в России в 2023 году стали шифровальщики под названием Loki Locker, BlackBit, Phobos, а традиционно популярные — LockBit, Conti и Babuk. Сегодня жертвами этих шифровальщиков чаще всего становятся российские ретейлеры: производственные, строительные, туристические, страховые компании.

На втором месте среди типов угроз стоят коммерческие стилеры, главные из которых: FormBook, Loki Stealer, Agent Tesla. Эти вредоносные программы предназначены для хищения логинов и паролей пользователей.

Следом за шифровальщиками и стилерами идут программы-шпионы и деятельность хактивистских группировок, цель которых сегодня — дестабилизация обстановки.

УБИЙСТВЕННАЯ ЦЕПОЧКА

Как хакеры планируют и реализуют атаку

В мире развитых технологий все больше внимания уделяется изучению типичных схем проведения хакерских атак. Фраза «хочешь поймать преступника — думай как преступник» актуальная и для мира развитых технологий. Действительно, если проанализировать все хакерские инциденты, то можно выявить определенную закономерность в действиях злоумышленников

Так, компания Lockheed Martin предложила модель, по которой действуют хакеры, и назвала ее «Убийственная цепочка», или Cyber Kill-Chain. Эта модель описывает основные этапы хакерской атаки и представляет собой нелинейный круговой процесс, когда злоумышленник осуществляет непрерывное горизонтальное движение внутри сети. Сейчас она состоит из семи этапов, однако стремительное развитие ИТ-сферы неизбежно ведет к усложнению атак, появлению новых приемов и инструментов как со стороны злоумышленников, так и со стороны специалистов по кибербезопасности. Именно поэтому появляются расширенные модели Cyber Kill-Chain или матрицы тактик и методов хакеров, основанные на реальных наблюдениях и исследованиях кибератак. Дальше мы расскажем подробнее о расширенной модели «Убийственной цепочки», построенной на основе классической модели матрицы MITRE ATT&CK[51] для предприятий.

ЭТАП 1

НАЧАЛЬНАЯ РАЗВЕДКА

Хакеры проводят исследование внешнего периметра компании. Основные задачи — определить цель взлома, найти лучшие «точки проникновения», выявить особенности компании-жертвы, изучить активности и каналы передачи информации. После выполнения всех этих задач хакер выбирает, какой метод атаки будет эффективнее и потребует меньше ресурсов.

Злоумышленники используют разные способы, чтобы добраться до «жертвы». Это может быть сканирование с использованием встроенных функций сетевых протоколов от простой проверки работоспособности сети через эхо-запрос по протоколу ICMP (Internet Control Message Protocol) до более сложных запросов, которые могут выявить версии и конфигурации программного обеспечения, IP-адреса, функциональные возможности устройства и пр. Для первичной разведки хакеры используют и другие пути: фишинг, социальные сети, поиск информации на открытых ресурсах или закрытых сайтах с утечками данных.

ЭТАП 2

ОСНАЩЕНИЕ И ПОДГОТОВКА РЕСУРСОВ

После получения информации о «жертве» злоумышленники подбирают подходящие инструменты для воплощения своего плана.

Что могут использовать хакеры:

- взломанную чужую инфраструктуру: физические или облачные серверы, домены, веб-сервисы, ботнеты;
- собственноручно разработанные инструменты: вредоносное ПО, фишинговые сайты, эксплойты, поддельные учетные записи, которые тяжело отличить от реальных;
- рынки информации о начальном доступе, где участники обмениваются установленными в чужих информационных системах бэкдорами, или существующими доступами к корпоративным VPN.

3 ЭТАП
ДОСТАВКА

В результате третьего этапа хакеры получают начальный доступ в сеть жертвы. Получить доступ можно с использованием множества различных способов: скрытая загрузка эксплойта в теле интернет-страницы, доступ через цепочки поставок, использование действительных или недействительных скомпрометированных учетных записей и иных векторов атаки. Самые популярные способы реализуются через взаимодействие со слабейшим звеном в системе безопасности компании — через человека: хакеры активно используют социальную инженерию, отправляя фишинговые рассылки или «подкидывая» зараженные съемные носители, в том числе мобильные устройства и пр.

4 ЭТАП
ВНЕДРЕНИЕ

Хакер запускает вредоносный код и обеспечивает его функциональность в контролируемой локальной или удаленной сети. Для выполнения команд злоумышленники могут использовать облачные службы (например, AWS System Manager, Azure RunCommand) или командные оболочки (вроде cmd и Unix), в которых можно отдавать команды операционной системе. Команды и сценарии могут быть написаны на популярных языках программирования, таких как Python или JavaScript, а в целях обхода защиты хакеры могут использовать развертывание контейнеров через Docker. Часто хакеры прибегают к социальной инженерии, чтобы подтолкнуть пользователя запустить исполнение вредоносного кода. В целом данный этап включает более тридцати возможных способов запуска кода злоумышленников.

5 ЭТАП
ЗАКРЕПЛЕНИЕ

После внедрения в систему хакеры стремятся не потерять к ней доступ. Это может произойти при перезапуске системы или изменении учетных данных.

Чтобы закрепиться в системе, хакеры используют:

- манипуляции с аккаунтами, среди которых обновление паролей в обход политик безопасности, продление срока действия скомпрометированных учетных данных, добавление дополнительных ролей или разрешений в учетной записи;
- настройку системных параметров для автоматического запуска вредоносного кода при загрузке или входе в систему;
- модификации загружаемых модулей ядра операционной системы.

На текущий момент хакерам доступно более ста инструментов для успешного закрепления в системе жертвы, и их выбор зависит от конкретного кейса. В результате злоумышленники закрепляются на конечных точках и могут контролировать все, что происходит в системе, без ведома жертвы.

ПОВЫШЕНИЕ ПРИВИЛЕГИЙ И УПРАВЛЕНИЕ

6 ЭТАП

Для входа в сеть и ее исследования хакеры могут использовать непривилегированный доступ. А уже для достижения целей атаки злоумышленники повышают уровень своего присутствия в системе, то есть становятся не просто пользователями, а администраторами.

7 ЭТАП

СБОР ДАННЫХ

После всех манипуляций хакеры приступают к внутренней разведке и поиску данных. Они аккуратно собирают информацию, которая важна для их целей. Найденные данные могут быть извлечены из локальной сети, общего сетевого хранилища, съемных носителей, облачных серверов и электронной почты.

На этом этапе хакеры обрабатывают собранные данные, сжимая их для сокращения объема и шифруя для избежания обнаружения. Так они делают последующую передачу данных менее заметной для защитной системы.

ЭТАП 8

ДЕЙСТВИЯ

Последний этап — самая важная часть атаки, во время которой хакеры отправляет собранную и упакованную информацию. Этот процесс может длиться от пары дней до нескольких месяцев в зависимости от ее объема. Как правило, похищаемые данные разделяют на архивы и отправляют по сети небольшими партиями, чтобы скрыть следы. Так заканчивается первый цикл цепочки, но хакеры, как правило, не останавливаются: они пытаются выявить новые цели, расширить привилегии и транспортировать данные. «Убийственная цепочка» повторяется раз за разом в сети жертвы до тех пор, пока злоумышленники не будут обнаружены и нейтрализованы.

52

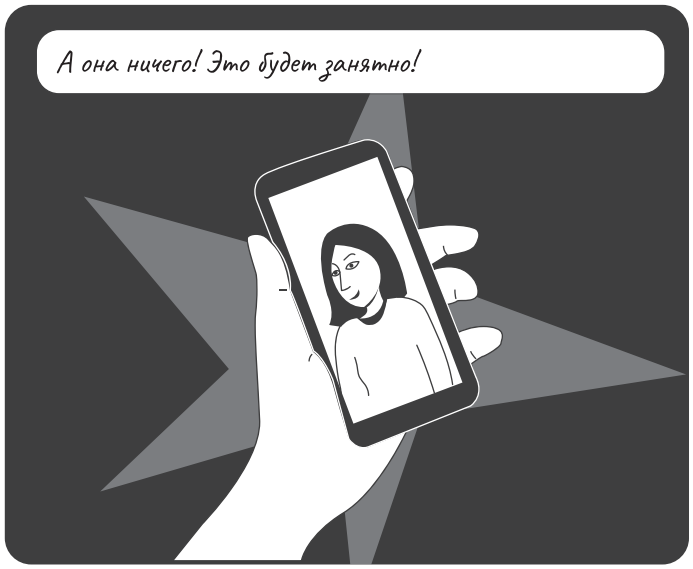
Добро пожаловать в мир кибербезопасности, где каждый клик мышью может стать решающим шагом на пути защиты ваших секретов. Готовы окунуться в захватывающее путешествие по таинственному миру хакеров, темных интриг и невидимых угроз?

Комикс состоит из трех частей, в нем рассказана увлекательная выдуманная история, которая может произойти практически с любым из нас.

ФЛЕШКА, СКРИПТ И AUTORUN

ДЕТЕКТИВНАЯ МЕЛОДРАМА

Влад мечтает заработать денег на хакинге компании «Мист-Буфф», которая занимается производством кондитерских изделий.



Ося — тщеславный хакер. Он пытался устроиться на работу в крупную зарубежную компанию Cisco, но ему отказали. Теперь он хочет доказать всему миру, что он гениальный программист. Деньги для него не главное.


Привет! Давай немного подрегулируем твой тренажер! Меня, кстати Владимир зовут, для друзей просто Влад!
Ну, подрегулируй! Я Лили...


Так завязались романтические отношения Лили и молодого человека Влада, желающего использовать любовь в качестве оружия для взлома системы «Мист-Буфф» и стать богаче!


Рыбка на крючке! Что у тебя по «Мисту»?


Что-то ты долго с ней! Давно уже написал хороший скрипт на Сишке. Лучше, если она занесет на флешке мой код.

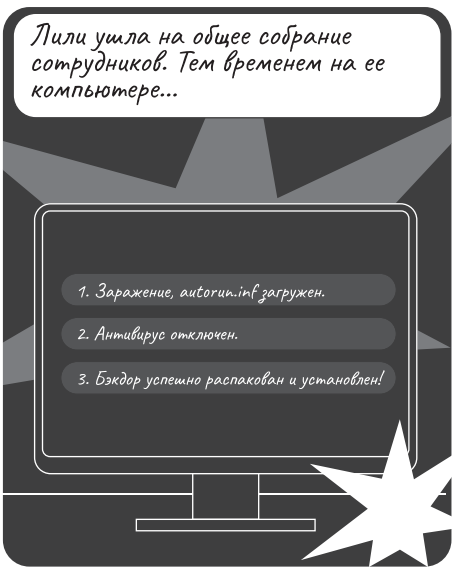

Помнишь нашу конную прогулку на прошлой неделе? Вот сюрприз – все фотографии на одной флешке, специально старался, обрабатывал в редакторе!
Ты такой романтичный сегодня! Только как мне посмотреть фото, ведь у меня нет дома ноутбука?


Попробуй на рабочем компьютере, а если что-то не откроется, ты всегда можешь позвонить мне, я немного разбираюсь в компьютерах!


На следующий день Лили приезжает на работу пораньше и вставляет флешку в рабочий компьютер...


На флешке нет фотографий, один файл всего! Похож на архив, я попыталась открыть, но ничего не произошло!


Видимо, файловая система флешки повредилась. Не переживай, сейчас все фотографии загружу в облако, тебе направлю ссылку. Флешку мне можешь вернуть, я буду ее чинить!

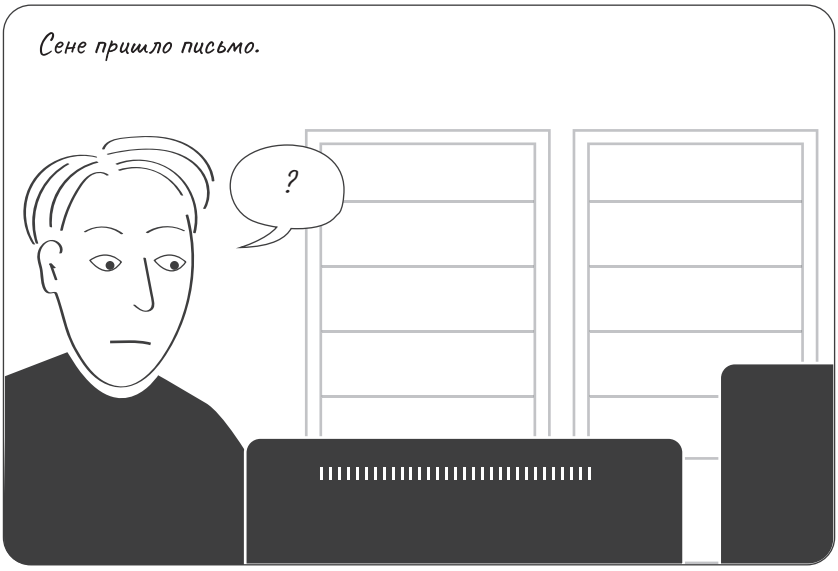

Лили ушла на общее собрание сотрудников. Тем временем на ее компьютере...
1. Заражение, autorun.inf загружен.
2. Антивирус отключен.
3. Бэкдор успешно распакован и установлен!


На собрании специалист по ИБ Арсений рассказывает о правилах информационной безопасности...
Запрещается открывать фишинговые письма и ссылки в этих письмах! Использовать личные флешки и подключать телефон для копирования файлов также запрещено!
Пока в компании нет специального отдела ИБ, все должны следовать этим простым правилам!


Снова Сеня включил свою шарманку... Кто позарится на наши конфетки?!


Ося звонит Владу:
Нам повезло, твоя подруга бухгалтер. С ее компьютера видна вся их «серая бухгалтерия»! Дай мне еще 4 дня для копирования всех данных!


Свидание Влада и Лили:
И правда, ничего страшного. Ты вот флешку с фотографиями вставила и он ведь не знает об этом?
Каждый месяц Сеня, наш сисадмин, нам рассказывает одно и то же: что у нашего производства могут украсть данные. Только вот никому не понятно, что у нас воровать — дизайн оберток для конфет?
Конечно нет, это ведь личные фотографии, хотя флешка и оказалась сломанной.



«Вы были неосторожны! Ваша бухгалтерия похищена! Получите ее обратно за 1 000 BTC. Иначе всем будут известны ваши серые дела!»


С твоего компьютера украли бухгалтерские документы! Если хакеры разместят все в открытый доступ, то нашу компанию ждет крах! Ты открывала ссылки или может использовала какие-то флешки личные?

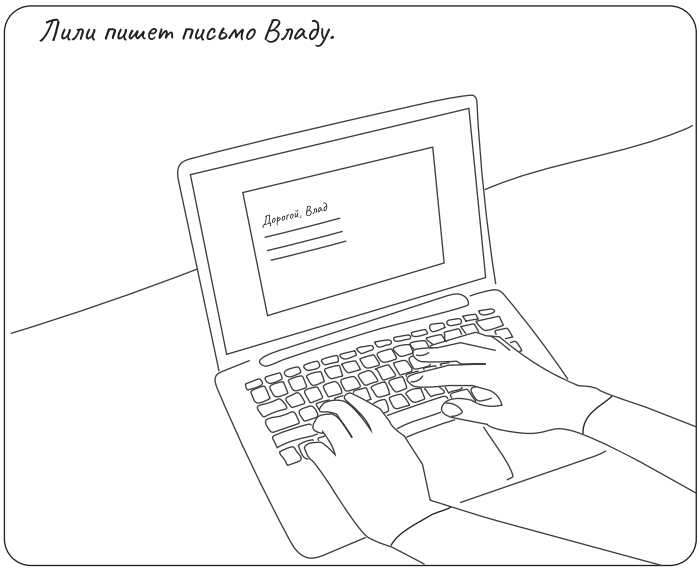

Уж точно это не я заражала свой компьютер....Хотя...Нет, этого не может быть...


Лили позвонила Владу, номер оказался недоступен.
А ведь и правда, кроме номера телефона мне о нем ничего не известно, даже странички в соцсетях нет. Что же теперь будет!


Срочное совещание руководства компании
Заражение, развертывание трояна и шифровальщика произошло через компьютер бухгалтера. Все данные восстановлены из резервных копий. Однако остаются юридические риски утечки данных в сеть. Технически платить выкуп мошенникам не имеет смысла.
Не нужно поддаваться панике. Юристы дадут рекомендации сегодня-завтра. А тебе, Сеня, нужно написать хакерам, что нам нужно 3 дня для сбора средств.
В полицию заявите, пусть ее посадят!


Юристы решили, что нужно выплатить выкуп, хотя у нас и не будет гарантий от хакеров.
...


Будем платить... Хотя ты могла бы попробовать написать своему любимому и попросить отказаться от идеи выкупа. Все равно его скоро поймают и посадят за такие дела!
Хорошо, я напишу ему...


Лили пишет письмо Владу.
Дорогой, Влад


Я отказался от выкупа из-за Лили. Она оказалась мне очень дорога... Не хочу чтобы она пострадала.
Ну и ладно, деньги для меня не так уж и важны, тем более это твоя тема была.
У меня сейчас в разработке рыба покрупнее - Cisco. Я уже прикупил софта для захода! Подключайся!

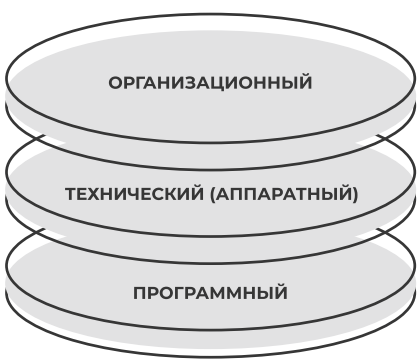

Сообщение от неизвестного абонента:
Это был мой последний и настоящий подарок тебе!
Так закончилась одна история.

ЗАЩИТА ОТ КИБЕРАТАК

Как специалисты по информационной безопасности противостоят хакерам

Если по одну сторону экрана стоят хакеры с арсеналом вирусов и систем взлома, то по другую — специалисты по информационной безопасности, задача которых предотвратить и отразить возможные атаки.

Архитектура кибербезопасности представляет собой набор слоев, каждый из которых призван защитить тот или иной элемент киберпространства (сети внешние и внутренние, приложения, данные и базы данных, серверы и сетевое оборудование, веб-ресурсы, промышленное оборудование, в том числе подключенное к сети (IIoT), компьютеры и мобильные устройства), а также обеспечить системное управление рисками и политиками в области информационной и кибербезопасности.



Верхний **организационный слой** отвечает за управление кибербезопасностью как системой, регламентируя деятельность организации, подразделений и сотрудников через политики и процедуры защиты от потенциальных угроз, через внедрение систем управления кибер рисками (средства защиты инфраструктуры), через обучение пользователей и повышение цифровой грамотности.

Следующий **технический (аппаратный)** слой обеспечивается физической защитой, вроде режима допуска людей на объект, в различные его сектора, к объектам информационной инфраструктуры (например, серверная), в подразделения с промышленным оборудованием (IIoT), средствами видеонаблюдения, электронными замками, сетевыми фильтрами, которые позволяют перекрыть каналы возможной утечки информации или повреждения инфраструктуры.

Программный слой представлен совокупностью программного обеспечения, направленного на защиту различных элементов информационной системы. Рынок информационной безопасности в большей степени представлен именно программным слоем и внедрением средств защиты на уровне общей инфраструктуры, сетей, приложений, данных, пользователей и конечных точек вроде компьютеров и телефонов.

СРЕДСТВА ЗАЩИТЫ СЕТЕЙ

Средства защиты сетей направлены на мониторинг и фильтрацию внутреннего и внешнего потока данных, а также на блокировку нежелательного трафика и предотвращение несанкционированного доступа (межсетевые экраны — FW, firewall; NGFW, next generation firewall); сбор и анализ данных для выявления необычного поведения в сети и оперативного реагирования на потенциальные угрозы (системы анализа трафика — NTA, network traffic analysis); обнаружение попыток вторжения в сеть или систему через анализ сетевого трафика и поиск признаков вредоносной активности (система обнаружения вторжений — IDS, intrusion detection system) а также их предотвращение через механизмы блокировки и остановки сетевого трафика для защиты сети и данных (система предотвращения вторжений — IPS, intrusion prevention system).

Защита сетей также предполагает контроль подключения различных устройств к корпоративной инфраструктуре через их идентификацию и ограничение доступа неавторизованных пользователей (средства контроля доступа к сети — NAC, network access control); на программно-аппаратном уровне контроль и фильтрация входящей и исходящей информации, а также блокировка потенциально опасной активности происходит на уровне шлюзов информационной безопасности (SWG/SMG, security web/mail gateway).

Существуют специальные средства безопасности, которые создают контролируемую среду, где возможно безопасно запускать и анализировать потенциально опасные файлы и программы, не подвергая реальную сеть и устройства риску (сетевые песочницы — Network Sandbox). Известные вредоносные коды блокируются на уровне межсетевого экрана, а в песочницу отправляются файлы, на которые не набирается достаточного объема информации для принятия решения. Локальные песочницы входят в состав многих антивирусов.

Для защиты от сложных и неизвестных вредоносных программ используют инструменты, которые изучают не отдельные файлы на предмет опасности, а сетевые коммуникации в целом для обнаружения новых и сложных типов угроз (средства защиты от сложных и неизвестных киберугроз — NDR, network detection & response).

Защиту сетей также обеспечивает VPN (виртуальные частные сети — VPN, virtual private network). Этот термин стал настолько общеупотребимым на территории страны, что перестал быть частью арго специалистов по информационной безопасности. Он может быть реализован в программно-аппаратном комплексе (VPN-шлюз), шифруя трафик для множества устройств, подключенных к локальной сети, и обычно применяется для построения защищенных корпоративных сетей, например, при объединении нескольких филиалов в целостную инфраструктуру. Программная часть (VPN-клиент), уже знакомая обычным пользователям, устанавливается непосредственно на устройство, шифрует трафик, предназначенный только для этого устройства, и применяется для защиты удаленного доступа.

Решения для защиты сетей могут быть как фрагментарными, направленными отдельно на разные аспекты (мониторинг, анализ, блокировку и пр.), так и многофункциональными, объединяющими в себе несколько инструментов и функций (многофункциональные решения — UTM, unified threat management) для обеспечения комплексной защиты, упрощая управление и обновление систем безопасности. Часто такие комплексы включают в себя возможности VPN, межсетевых экранов, антивирусов и систем обнаружения и предотвращения вторжений.

СРЕДСТВА ЗАЩИТЫ ПРИЛОЖЕНИЙ

Средства защиты приложений помогают найти уязвимости и ошибки в программном обеспечении еще в процессе его создания, анализируя структуру и синтаксис исходного кода (средства поиска уязвимостей в исходном коде ПО — AST, application security testing). Подобные уязвимости могут быть использованы для несанкционированного доступа или нарушения безопасности, через эксплойты и бэкдоры.

Поиск уязвимостей работающих приложений осуществляется через анализ системы с целью выявления возможных

проблем безопасности (средства контроля и оценки уязвимостей — VA, vulnerability assessment). Далее идет процесс приоритизации уязвимостей и планирования сроков и этапов их устранения с последующим отслеживанием (средства управления уязвимостями — VM, vulnerability management).

Так же как в процессах защиты сетей здесь используются межсетевые экраны (межсетевой экран для веб-приложений — WAF, web application firewall) для защиты приложения и данных через анализ трафика между пользователем и веб-приложением и блокировку попыток эксплойта, SQL-инъекции или других атак.

Для предотвращения воздействия распределенных атак на серверы, сети и приложения используются специальные средства защиты (средства защиты от DDoS-атак — DDos protection), которые обнаруживают и блокируют вредоносный трафик, способный парализовать или отключить целевые ресурсы.

СРЕДСТВА ЗАЩИТЫ ДАННЫХ

Средства защиты данных применяются для предотвращения попыток несанкционированного доступа, удаления и модификации конфиденциальных данных без соответствующего разрешения, согласованного с политиками безопасности компании (средства защиты от несанкционированного доступа — UAP, unauthorized access protection). Они основаны на принципах обязательной идентификации и двухфакторной аутентификации пользователей, регистрации всех запусков и завершений программного обеспечения. Кроме того, такие системы позволяют разграничить права доступа пользователей, регистрируют и хранят данные об их действиях и ведут учет всех используемых носителей информации (флеш-накопители, CD-приводы и др).

Предотвращение несанкционированной передачи или раскрытия конфиденциальных данных происходит за счет технологий отслеживания и контроля за движением информации, а также через блокировку такой передачи, если она не соответствует заданным политикам безопасности (средства защиты от утечек информации — DLP, data loss prevention).

Также применяются методы и алгоритмы, преобразующие исходную информацию в непонятный и неразборчивый вид (средства шифрования — encryption) путем замены или перестановки символов, чтобы только получатель с правильным ключом мог расшифровать информацию.

СРЕДСТВА ЗАЩИТЫ ПОЛЬЗОВАТЕЛЕЙ

Средства защиты пользователей связаны с процессами идентификации, аутентификации и контроля доступа (IAM/IGA, identity & access management/governance & administration) к информационным ресурсам через систему выдачи прав и выставления ограничений для каждого пользователя, а также проверки их подлинности и подтверждения их идентификации перед предоставлением доступа к системам и данным. Отдельное внимание уделяется администраторам и привилегированным пользователям с дополнительными правами в системе и базах данных.

Специальный набор инструментов позволяет организовать и проверить доступ и действия такого круга пользователей в системе через контроль их действий и установку лимитов и ограничений на использование привилегий (средства контроля привилегированных пользователей — PAM, privileged access management).

Специальный набор технологий позволяет обеспечить безопасность передачи и хранения данных, используя ассиметричное шифрование и цифровые сертификаты пользователей (типа ЭЦП — электронная цифровая подпись), которые выпускаются удостоверяющим центром и позволяют в цифровом поле идентифицировать человека, осуществлять подписание документов и подтверждение действий (средства криптографической защиты информации пользователей — PKI, public key infrastructure).

ЗАЩИТА РАБОЧИХ СТАНЦИЙ

Защита рабочих станций применяется для защиты конечных устройств (компьютеров, ноутбуков, смартфонов) в сети от вторжений злоумышленников, вредоносных программ и других киберугроз.

Средства антивирусной защиты (**AVP**, antivirus protection) обнаруживают, предотвращают и устраняют известные, типичные и массовые вредоносные файлы и программы через соотнесение их с базой данных антивируса, где хранится информация об известных вирусах со свойствами и признаками каждого (наборы сигнатур).

В настоящее время антивирусы не всегда справляются с обеспечением безопасности организации из-за скорости появления все новых образцов вредоносных программ, которые пока не попали в базу данных антивируса, а также из-за применения безфайловых атак (вроде фишинга). В таких случаях используются системы обнаружения и реагирования на угрозы на рабочих станциях пользователей (**EDR**, endpoint detection and response), которые защищают устройство путем анализа поведения системы, идентификации необычной активности и активного реагирования на угрозы.

СРЕДСТВА ЗАЩИТЫ ИНФРАСТРУКТУРЫ

Средства защиты инфраструктуры выступают своего рода надстройкой над комплексом средств защиты сетей, данных, пользователей, приложений, рабочих станций и позволяют отслеживать весь периметр ИТ-инфраструктуры (компьютерное оборудование, программное обеспечение, сетевые службы, сервисы, электронная почта, политики информационной безопасности, системы контроля, системы резервного копирования и хранения данных, оргтехника, телефония и пр.).

Одним из распространенных типов таких систем является система управления информационной безопасностью и событиями (**SIEM**, security information and event management), которая создает единый централизованный хаб контроля и анализа информации, поступающей из всевозможных систем и средств, сообщает о ключевых рисках, возможных угрозах, попытках проникновения, информируя сотрудников службы ИБ о необходимости обратить внимание или предпринять какие-то действия.

При необходимости добавления автоматизации действий по реагированию на инциденты и сбору дополнительной обогащающей информации по инцидентам используют систему оркестровки (управления) систем безопасности (**SOAR/IRP**, security orchestration, automation and response). SOAR является логическим развитием систем IRP, в них автоматизация реагирования сочетается с управлением средствами защиты и данными о киберугрозах.

Средства анализа киберугроз (**TI**, threat intelligence) помогают идентифицировать и анализировать уязвимости ИТ-инфраструктуры и потенциальные угрозы, подавая эту информацию на вход SIEM-системы, становясь ее элементом.

Платформа управления рисками (**GRC**, governance, risk and compliance) идентифицирует и классифицирует все активы организации с целью упорядочить сведения о защищаемой инфраструктуре и анализирует вероятность реализации ИБ-угроз и возможного ущерба. В отношении рисков формируется план мероприятий по оптимальным мерам защиты и экономическое обоснование для планирования бюджета на обеспечение безопасности, а также проводится аудит и контроль на соответствие регуляторным требованиям. Безопасность и непрерывность работы систем автоматизации и управления производством и промышленными объектами обеспечивается комплексными платформами защиты от киберугроз (средства защиты промышленных систем управления — **ICS**, industrial control system), которые зачастую включают в себя системы управления событиями (SIEM), системы управления уязвимостями (VM), анализ трафика технологических систем, а также систем обнаружения и реагирования на угрозы на конечных точках (EDR).

Продукты и решения в области кибербезопасности

Каждая из описанных выше категорий систем включает множество решений от российских и зарубежных поставщиков программных продуктов в области информационной и кибербезопасности. Санкционный режим и нормативное регулирование привели к уходу или отказу от большинства иностранных ИБ-систем.

Мы подготовили карту востребованности программных продуктов от российских разработчиков, решающие задачи кибербезопасности ИТ-инфраструктуры в каждой из категорий средств защиты. Перечень был составлен на основании анализа публичных источников, рейтингов популярных программных продуктов, информации от крупнейших российских вендоров на рынке ИБ, а также каталога СЗИ независимого информационно-аналитического центра по информационной безопасности Anti-malware.

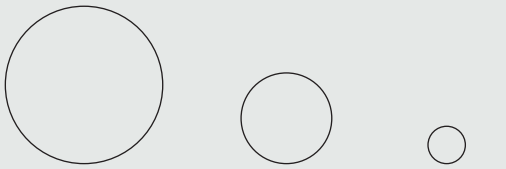
Каждому программному продукту, указанному на карте, присвоено 4 признака.

Признак 1

Категория программного продукта. Описание каждой категории и сфера ее применения приведены на страницах 61-63.

Признак 2

Востребованность программного продукта на рынке труда. Изучив открытые вакансии в сфере ИБ за последние несколько лет, мы собрали перечень требований работодателей к знанию специализированных программных продуктов и систем. Каждую систему защиты информации мы проанализировали на частоту упоминания в вакансиях. Мы проводим данное исследование с середины 2021 года, и на момент подготовки выпуска было собрано более 5,5 тысяч вакансий специалистов по информационной безопасности. Если система упоминается в 15 и более процентах вакансий, то ей присваивается высокая значимость; если упоминаемость на уровне 14%—5%, то значимость средняя; низкая значимость — для упоминаемости менее чем в 5% вакансий.



Более 15% 14%—5% Менее 5%

Признак 3

Наличие лицензии ФСТЭК.

Признак 4

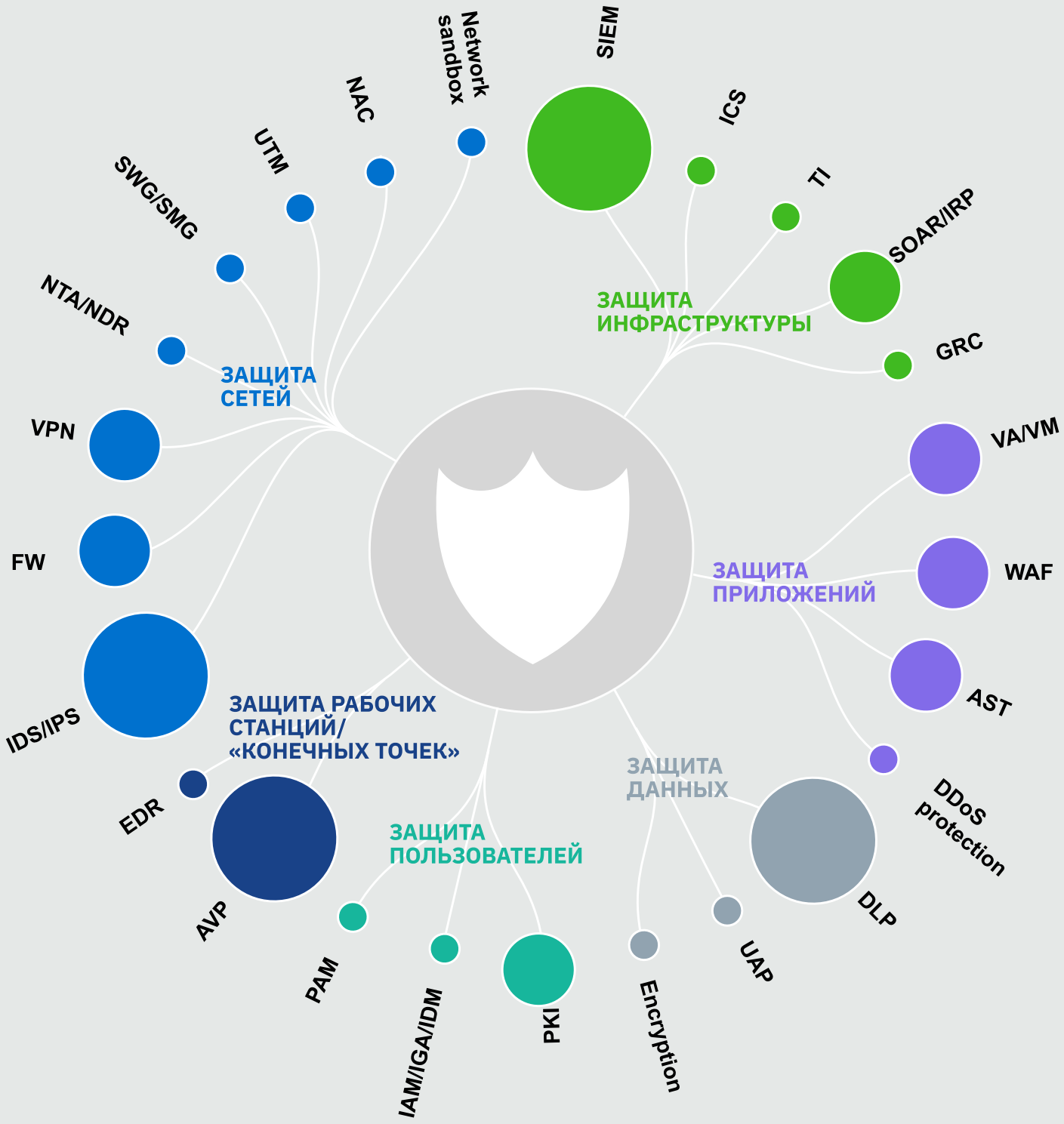
Наличие программного продукта в реестре отечественного ПО.

Согласно действующему российскому законодательству, средства защиты информации должны быть сертифицированы. В России за этот процесс отвечают два ведомства-регулятора: ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ (Федеральная служба безопасности Российской Федерации). ФСБ занимается сертификацией разработок, использующих криптографические методы защиты, и ведет реестр средств защиты информации ФСБ, все остальные системы проходят сертификацию ФСТЭК[52]. Компаниям, которые работают в ГИС (государственные информационные системы), АСУТП (автоматизированные системы управления технологическим процессом), относятся к объектам КИИ (критическая информационная инфраструктура), обрабатывают персональные данные и государственную тайну, необходимо пройти аттестацию ФСТЭК, игнорирование сертификации или переход на несертифицированное ПО наказывается крупными штрафами и даже уголовной ответственностью[53].

Также мы проверили наличие программного обеспечения в реестре отечественного ПО. Вхождение в реестр дает возможность поставлять софт в правительственные учреждения и государственные компании через процедуры госзакупок, где такой пункт является обязательным требованием тендерной процедуры. Кроме того, разработчики имеют право претендовать на льготы по уплате налогов и получение государственной поддержки, что также стимулирует компании проходить процедуру регистрации в реестре.

Средства защиты и технологии, которые применяются в кибербезопасности, постоянно совершенствуются, так же как и способы проведения хакерских атак. В связи с этим нельзя назвать этот перечень конечным и бессменным, он отражает текущую картину на момент подготовки выпуска.

Карта востребованности программных продуктов



Карта востребованности программных продуктов

	Продукт	Вендор		
SIEM	MaxPatrol Siem	Positive Technologies	⬢	★
	Ankey SIEM	Газинформсервис	⬢	★
	Kaspersky Unified Monitoring and Analysis Platform	Лаборатория Касперского	⬢	★
	KOMRAD Enterprise SIEM	НПО «Эшелон»	⬢	★
	RuSiem	RuSiem	⬢	★
	SearchInform SIEM	SearchInform	⬢	★
TI	Threat Intelligence	F.A.C.C.T.		★
	Группа сервиса Kaspersky Threat Intelligencew	Лаборатория Касперского		★
	R-Vision TIP	R-Vision	⬢	★
	PT Cybersecurity Intelligence	Positive Technologies		★
SOAR/ IRP	R-Vision SOAR	R-Vision	⬢	★
	Security Vision Incident Response Platform	Security Vision	⬢	★
ICS	Kaspersky Industrial CyberSecurity	Лаборатория Касперского	⬢	★
	ViPNet Coordinator IG	Инфотекс	⬢	★
	PT ICS	Positive Technologies		
	TDS Industrial	F.A.C.C.T.		
	InfoWatch ARMA	InfoWatch	⬢	★
	DATAPK	СайберЛимфа	⬢	★
GRC	Security GRC Platform	R-Vision	⬢	★
	Security Governance, Risk Management and Compliance	Security Vision	⬢	★
FW	VIPNet xFirewall	ИнфоТеКС	⬢	★
	Континент 4	Код безопасности	⬢	★
	UserGate	UserGate	⬢	★
	С-Терра Шлюз	С-Терра	⬢	★
	Рубикон	ЕПО «Эшелон»	⬢	★
	Ideco UTM	Айдеко	⬢	★
	Zecurion NGFW	Zecurion	⬢	★
UTM	Ideco UTM	Айдеко	⬢	★
	UserGate	UserGate	⬢	★
	Traffic Inspector Next Generation	Смарт-Софт	⬢	★
IDS/IPS	Traffic Inspector Next Generation	Смарт-Софт	⬢	★
	ViPNet IDS 3	Инфотекс	⬢	★
	Рубикон	НПО «Эшелон»	⬢	★
	СОВ Континент	Код безопасности	⬢	★
	С-Терра СОВ	С-Терра	⬢	★

NTA/NDR	EtherSensor	Microolap Technologies		★
	TDS	F.A.C.C.T.		★
	Kaspersky Unified Monitoring and Analysis Platform	Лаборатория Касперского	⬢	★
	PT Network Attack Discovery	Positive Technologies	⬢	★
	Гарда Монитор	Гарда Технологии	⬢	★
NAC	Traffic Inspector Next Generation	Смарт-Софт	⬢	★
	Сакура	ИТ-Экспертиза		★
	Efros ACS	Газинформсервис	⬢	★
SWG/SMG	Kaspersky Security для интернет шлюзов	Лаборатория Касперского	⬢	★
	UserGate	UserGate	⬢	★
	Solar webProxy	Ростелеком-Солар		★
	Indeco UTM	Indeco	⬢	★
	Zecurion SWG	Zecurion	⬢	★
Network sandbox	Kaspersky Sandbox	Лаборатория Касперского	⬢	★
	PT Sandbox	Positive Technologies	⬢	★
	ATHENA	АВ Софт		★
VPN	Континент	Код безопасности	⬢	★
	ViPNet Coordinator HW 5	Инфотекс	⬢	★
	С-Терра Шлюз	С-Терра	⬢	★
	Квазар	Специальная интеграция		
VA/VM	MaxPatrol VM	Positive Technologies		★
	Vulns.IO VM	Фродэкс		★
	Сканер-ВС	НПО «Эшелон»	⬢	★
	RedCheck	АЛТЭКС-СОФТ	⬢	★
	Solar appScreener	Ростелеком-Солар	⬢	★
AST	Traffic Inspector Next Generation	Смарт-Софт	⬢	★
	ViPNet IDS 3	Инфотекс	⬢	★
WAF	Рубикон	НПО «Эшелон»	⬢	★
	СОВ Континент	Код безопасности	⬢	★
	С-Терра СОВ	С-Терра	⬢	★
	EtherSensor	Microolap Technologies		★
	TDS	F.A.C.C.T.		★
DDoS protection	DDoS-Guard	DDoS-Guard	⬢	★
	Kaspersky DDoS Protection	Лаборатория Касперского	⬢	★
	Периметр	Гарда Технологии	⬢	★
	Митигатор	БИФИТ	⬢	★
UAP	Secret Net Studio	Код безопасности	⬢	★
	Dallas Lock	Конфидент	⬢	★
	ViPNet SafePoint	Инфотекс	⬢	★
DLP	Traffic Monitor	InfoWatch	⬢	★
	Zecurion DLP	Zecurion	⬢	★
	Гарда Предприятие	Гарда Технологии	⬢	★
	Solar Dozor	Ростелеком-Солар	⬢	★

encryption	Secret Disk	Алладин Р. Д.	⬢	★
	Kaspersky Security для бизнеса (с уровня «Расширенный»)	Лаборатория Касперского	⬢	★
	Zecurion Storage Security	Zecurion		
IAM/IGA/IDM	Ankey IDM	Газинформсервис	⬢	★
	Avanpost IDM	Аванпост	⬢	★
	КриптоПро IDM	КриптоПро		
	Solar inRights	Ростелеком-Солар	⬢	★
PAM	СКДПУ	АйТи Бастион	⬢	★
	SafeInspect	Новые технологии безопасности	⬢	★
	Indeed Privileged Manager	Индид	⬢	★
	sPace	Web Control		★
PKI	Avanpost PKI	Аванпост	⬢	★
	Indeed Certificate Manager	Индид	⬢	★
	JMS	Алладин Р. Д.	⬢	★
	ViPNet PKI	Инфотекс		★
AVP	Kaspersky Security для бизнеса	Лаборатория Касперского	⬢	★
	Dr. Web	Доктор Веб	⬢	★
	Secret Net Studio	Код безопасности	⬢	★
EDR	Kaspersky EDR	Лаборатория Касперского	⬢	★
	Сакура	ИТ-Экспертиза		★
	ViPNet EndPoint Protection	Инфотекс	⬢	★

СПЕЦИАЛИСТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

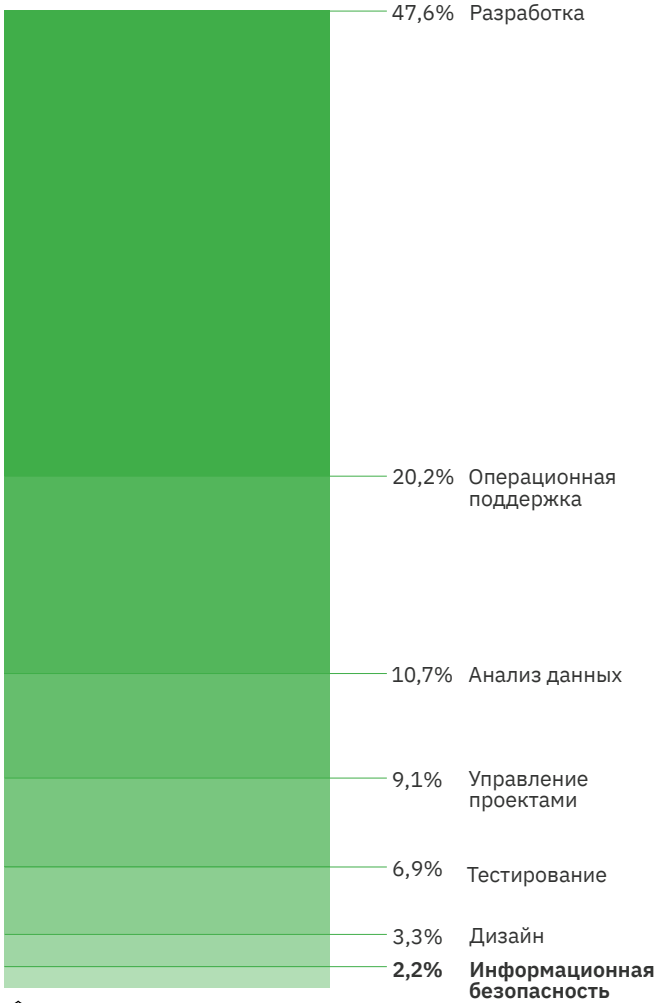
Сколько готовы платить работодатели и что должны уметь соискатели

Узнать больше
и почитать другие
наши исследования

Университет Иннополис регулярно проводит исследование потребности в ИТ-специалистах и необходимых по мнению работодателей и рынка труда ИТ-навыках. Здесь мы представили сведения о профессионалах, относящихся к сфере информационной безопасности, среди которых: специалисты, администраторы, аналитики, руководители и инженеры по информационной безопасности, архитекторы систем информационной безопасности, специалисты по анализу и технической защите информации и программных продуктов, аналитики SOC и другие.

За период с середины 2021 года было изучено более 300 тысяч запросов работодателей с платформ онлайн-рекрутмента, из них на долю безопасников пришлось 5,6 тысяч позиций — около 2% от общего числа ИТ-специалистов. На данный момент это самая малочисленная группа среди всех функциональных областей.

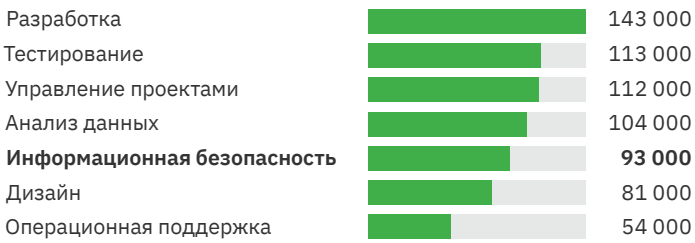
Распределение ИТ-вакансий по функциональным областям



Средняя и медианная зарплата у специалистов по ИБ несколько ниже средних значений по ИТ-отрасли: средняя — 93 тыс. рублей, медианная — 80 тыс. рублей. Рост оплаты труда год к году (2022–2021) составил 10%. Поскольку спрос на специалистов в том числе сказывается на размере оплаты труда, то небольшая потребность в общем объеме ИТ-специалистов удерживает зарплаты на среднем уровне. При этом стоит отметить, что узкие специалисты, опытные сотрудники и эксперты могут получать значительно выше рынка.

Средняя зарплата

по функциональным областям, руб.

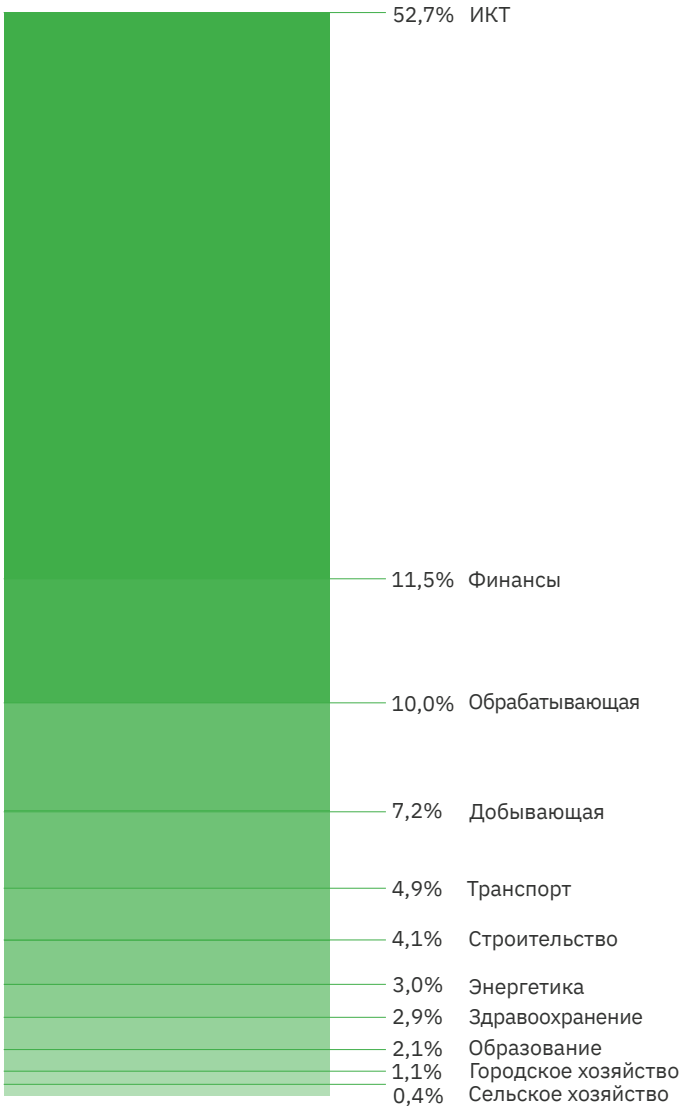


Медианная зарплата

по функциональным областям, руб.

Разные отрасли предъявляют разный спрос на специалистов. Если говорить про безопасников, то самая большая их доля сосредоточена непосредственно в секторе ИКТ (52,7%); следом идет финансовый сектор — один из наиболее подверженных киберугрозам и кибератакам (11,5%); обрабатывающая промышленность как самая многочисленная по количеству подотраслей и производств, требующих обеспечения информационной безопасности (10%) и одна из ключевых отраслей российской экономики — добывающая промышленность (7,2%). Самую высокую среднюю заработную плату предлагают специалистам в отрасли добывающей промышленности: 109 тысяч рублей. Самый высокий рост средней заработной платы был зафиксирован в сельском хозяйстве (+57% в 2022 г. по отношению к 2021 г.), но это говорит скорее о подтягивании зарплат в отрасли к среднерыночным, хотя и после такого роста зарплаты все равно остаются небольшими.

Доля вакансий ИБ-специалистов по отраслям



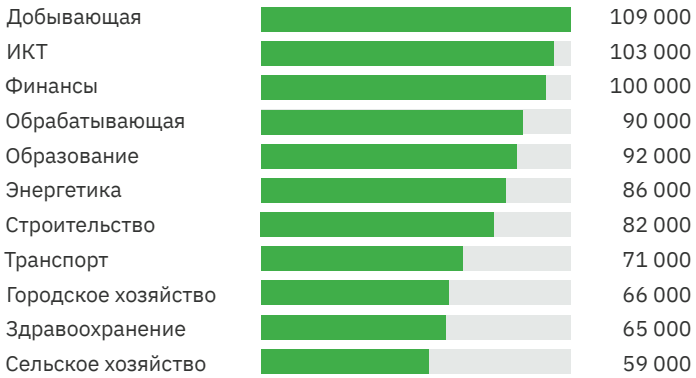
Около половины всех вакансий (46,7%) сконцентрировано в Москве, точке притяжения крупных корпораций, главных вузов-поставщиков кадров и месте сосредоточения головных офисов большинства предприятий, в том числе промышленные базы которых рассредоточены по регионам страны. Здесь же предлагают самую высокую среднюю заработную плату — 118 тысяч рублей. Самый большой рост средней заработной платы наблюдается в Воронеже (+55%), а падение — в Нижнем Новгороде (–11%).

Рейтинг городов по количеству вакансий ИБ-специалистов

№	город	доля вакансий	средняя з/п, руб
1	**Москва**	**46,7%**	**118 000**
2	**Санкт-Петербург**	**14,1%**	**102 000**
3	**Екатеринбург**	**3,6%**	**91 000**
4	**Казань**	**3,2%**	**78 000**
5	**Новосибирск**	**3,0%**	**88 000**
6	**Самара**	**2,5%**	**59 000**
7	**Нижний Новгород**	**2,4%**	**80 000**
8	**Краснодар**	**2,2%**	**69 000**
9	**Уфа**	**1,6%**	**58 000**
10	**Воронеж**	**1,6%**	**82 000**
	Другие	19,0%	79 000

Где больше платят?

Средняя зарплата по отраслям, руб.



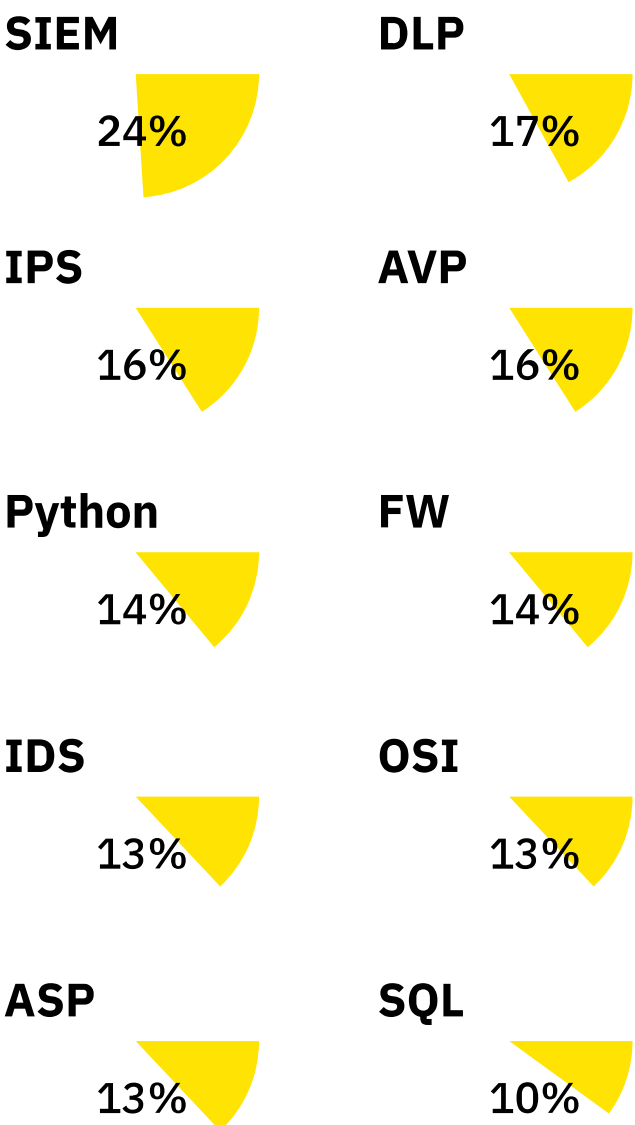
Помимо того, какое количество специалистов нужно в отраслях и регионах, важно и то, какие это специалисты, какими они должны обладать навыками, какими программными продуктами и языками владеть.

Специальность «информационная безопасность» отличается высокой частотой требований к наличию высшего образования (указывается в 55% запросов работодателей) относительно других исследуемых функциональных областей, где в среднем этот показатель составляет лишь 29%. По критерию требования наличия высшего образования можно выделить две группы отраслей. В первой группе отраслей (здравоохранение, обрабатывающая промышленность, образование, энергетическая инфраструктура, добывающая промышленность, строительство) требования к высшему образованию были более жесткими и встречались в 67–83% вакансий. Это вполне объяснимо, так как в данных отраслях сконцентрированы большие массивы персональных данных пользователей и объекты критической инфраструктуры, значимой для информационной безопасности и суверенитета страны. Во второй группе отраслей (городское хозяйство, сельское хозяйство, транспортная инфраструктура, финансовые услуги и ИКТ) требования были на уровне 33–60%.

Если говорить о профессиональных навыках, то практически в трети вакансий упоминается знание на уровне администратора и практический опыт по обеспечению безопасности операционных систем WIndows и Linux. А самым востребованным навыком стала работа с категорией SIEM-систем, которая упоминается в каждой четвертой вакансии. Также широкое распространение имеют требования работать со средствами защиты от утечек информации (DLP) и системами обнаружения вторжений (IPS). А популярными языками для специалистов службы информационной безопасности являются: Python — указан в 14% вакансий, SQL — 10%, Java — 5%.

Интересен и отраслевой разрез в части навыков, поскольку каждая отрасль предъявляет свой набор требований к кандидатам в безопасники. Понимание принципа работы и опыт внедрения SIEM-систем, средств защиты от утечек информации (DLP), уверенные знания и опыт администрирования антивирусного ПО (AVP) и другие навыки, которые вошли в общий топ навыков, имеют относительно равный высокий спрос во всех отраслях. Из особенностей отметим, что средства защиты инфраструктуры пользуются наибольшим спросом в энергетике — на них приходится 23% запросов к навыкам ИБ-специалистов; средства защиты пользователей — самая непопулярная категория среди работодателей во всех отраслях, так же как и средства защиты рабочих станций. Наибольший акцент при поиске безопасников делается на навыки работы с программным обеспечением, относящимся к средствам защиты сетей: это 30–40% запросов. При этом навыки работы с софтом, направленным на защиту приложений, большим спросом пользуется в отрасли городского хозяйства. А самая немногочисленная категория — средства защиты данных, особый спрос к навыкам предъявляется в 3–15% случаев.

Топ-10 навыков ИБ-специалистов



Какие продукты и решения чаще всего упоминается в вакансиях ИБ-спеспециалистов в зависимости от отрасли

	ИКТ	Финансы	Обрабатывающая	Добывающая	Транспорт	Стройка	Энергетика	Здравоохранение	Образование	Городское хозяйство	Сельское хозяйство
FW	7%	4%	5%	7%	7%	8%	3%	7%	7%	–	–
NGFW	5%	2%	2%	4%	4%	5%	1%	4%	5%	–	–
UTM	–	–	–	1%	–	–	–	–	1%	–	–
IDS	6%	6%	5%	7%	6%	8%	5%	7%	5%	3%	6%
IPS	8%	6%	9%	10%	6%	7%	8%	9%	5%	8%	6%
NTA	2%	2%	1%	1%	2%	1%	–	1%	3%	–	–
NAC	1%	–	–	–	–	–	–	–	–	–	–
NDR	1%	1%	1%	1%	2%	–	1%	1%	2%	8%	–
SWG	–	–	–	1%	–	2%	–	–	1%	–	–
SMG	–	–	–	–	–	2%	–	–	–	–	6%
Network Sandbox	2%	1%	1%	1%	1%	–	–	1%	–	–	6%
VPN	5%	4%	4%	3%	6%	4%	4%	7%	4%	3%	6%
VA	4%	6%	2%	7%	2%	4%	3%	2%	6%	24%	–
VM	3%	2%	1%	2%	2%	3%	4%	4%	4%	8%	6%
AST	4%	5%	4%	2%	1%	3%	2%	2%	7%	3%	–
WAF	5%	5%	2%	4%	6%	3%	1%	2%	4%	–	6%
DDoS	2%	1%	–	1%	3%	–	–	–	1%	–	–
UAP	–	–	–	–	–	–	–	–	–	–	–
DLP	7%	10%	12%	11%	11%	14%	13%	10%	3%	3%	13%
Encryption	–	–	1%	–	1%	–	–	–	–	–	–
IDM	2%	1%	2%	2%	2%	1%	1%	1%	1%	–	13%
IAM	–	–	–	1%	–	–	–	–	1%	3%	–
IGA	1%	2%	5%	1%	1%	–	2%	1%	2%	5%	–
PAM	2%	2%	2%	2%	3%	1%	3%	5%	1%	–	–
PKI	3%	7%	2%	5%	2%	5%	7%	4%	5%	8%	–
AVP	5%	10%	13%	8%	11%	12%	18%	10%	14%	21%	25%
EDR	2%	2%	6%	3%	3%	–	–	1%	1%	–	–
SIEM	11%	12%	12%	10%	11%	11%	19%	11%	11%	3%	6%
TI	1%	–	–	1%	–	–	–	1%	–	–	–
SOAR	1%	–	–	1%	–	1%	1%	1%	–	–	–
ICS	2%	2%	1%	1%	1%	1%	1%	–	1%	3%	–
IRP	3%	3%	5%	3%	4%	–	1%	4%	1%	–	–
GRC	2%	1%	1%	3%	1%	1%	–	1%	1%	–	–

Защита сетей
Защита приложений
Защита данных
Защита пользователей
Защита рабочих станций/«конечных точек»
Защита инфраструктуры

Марина Усова

Руководитель управления корпоративных продаж «Лаборатории Касперского» в России

«Все больше и больше компаний отдает приоритет вопросам кибербезопасности и инвестициям в этой области»

Беседовала Анастасия Муфлиханова
Фото: пресс-служба

О кибер-готовности России

По данным ООН на 2020 год, Россия находилась на 8 месте из 194 по уровню киберготовности. Это говорит о том, что наша страна принимает серьезные меры для защиты своей информационной сферы.

Однако необходимо учитывать, что киберугрозы эволюционируют, а тренды быстро меняются, поэтому важно постоянно развивать инструменты кибербезопасности.

За последнее время ландшафт угроз стал более сложным, требования со стороны регуляторов — более строгими, а тренд на импортонезависимость стал ключевым. Это способствовало усилению ответственного подхода к кибербезопасности, который сегодня становится все более распространенным.

На российском рынке исторически представлен широкий выбор отечественных решений по информационной безопасности для разных сфер. Поэтому даже после ухода иностранных вендоров у компаний осталась возможность выстроить долгосрочную стратегию защиты на основе имеющихся продуктов.

До 2022 года повышенное внимание вопросам кибербезопасности уделяли преимущественно средние и крупные российские организации. Хотя стоит признать, что и некоторые из них далеко не всегда относились к этому со всей серьезностью. Сегодня руководство организаций понимает, что от грамотно выстроенной линии киберзащиты зависит финансовая устойчивость бизнеса, сохранность активов и качество предоставляемых услуг или продуктов. Это осознание приводит к тому, что все больше и больше компаний отдает приоритет вопросам кибербезопасности и инвестициям в этой области.

О самых атакуемых отраслях

По данным Kaspersky Managed Detection and Response за 2022 год, наиболее атакуемыми отраслями в России и СНГ были финансовые организации, промышленность, ИТ-компании и транспорт. Эти тренды сохраняются и в 2023 году.

О кадрах

По отрасли кадровый дефицит очень заметен уже много лет. В связи с этим многие компании стремятся передать задачи в области ИБ на аутсорс.

Чтобы помочь в развитии кадрового резерва, обладающего актуальными навыками и знаниями в области информационной безопасности, а также повысить квалификацию существующих специалистов предприятий, «Лаборатория Касперского» работает с вузами, открывает в них лаборатории, поддерживает олимпиады, CTF, проводит тренинги и предоставляет свои решения для киберполигонов. К примеру, мы очень активно сотрудничаем с МАИ.

Как обычным пользователям противостоять киберугрозам

- Не переходите по неизвестным ссылкам.
- Не доверяйте слишком выгодным предложениям.
- Регулярно меняйте пароль и помните, что он должен быть сложным: используйте специальные символы, цифры, строчные и прописные буквы или воспользуйтесь менеджером паролей для генерации надежной комбинации.
- Поддерживайте программное обеспечение и операционные системы обновленными до последней версии.
- Установите защитные решения на все устройства.
- Уделяйте особое внимание тому, что вы размещаете в Сети. В интернете нет возможности полного удаления опубликованной информации.

ТРЕНДЫ

Как развивается сфера кибербезопасности

01. Made in Russia

В 2015 году Правительством РФ было принято Постановление № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»[54]. Это дало возможность отечественным ИТ-компаниям претендовать на госзаказы и сформировать реестр отечественного ПО со своими программными продуктами. Данный период можно считать отправной точкой в процессе формирования импортонезависимой ИТ-отрасли Российской Федерации.

Рассматриваемые процессы затронули и сектор информационной безопасности, который вышел на первый план в приоритетах импортозамещения программного обеспечения России в 2022 году в связи с санкционным режимом. Сегодня в секторе кибербезопасности разработаны конкурентоспособные решения мирового уровня, а компании начинают применять комплексный подход к проектированию и внедрению систем ИТ-безопасности.

Рост российского рынка кибербезопасности обусловлен не только политикой правительства по переходу на отечественное ПО, но и увеличением числа кибератак. В 2022 году на российские компании было совершено 911 тыс. хакерских атак, что вдвое больше, чем годом ранее, по данным компании «Ростелеком-Солар»[55].

Несмотря на укрепление положения российских вендоров на рынке средств защиты (в 2022 году они заняли 70% рынка, в 2021 году — 61%), проблема преодоления разрыва в некоторых технологиях, программных продуктах Запада и отечественных продуктах сохраняет свою актуальность. Эксперты отмечают, что не все отечественные разработки, позиционирующие себя как аналоги известных западных продуктов, обладают соответствующей функциональностью и отвечают требованиям качества и безопасности[56].

Подводя итог, можно сказать, что российский рынок ИТ-безопасности находится в активной стадии развития, разрабатываемые решения конкурентоспособны на мировом уровне, а в части устранения технологических разрывов ведется масштабная работа, которая и обеспечит за период с 2022 по 2027 год совокупный среднегодовой темп роста рынка в 24%[57].

02. Нулевое доверие

Zero Trust («нулевое доверие») — это технология, дающая безопасность организации работы в облачном и мобильном мире. Массовый перевод сотрудников во время пандемии на удаленную работу, сохранение в дальнейшем гибридных форм занятости и использование личных устройств на рабочих местах спровоцировали появление ряда новых уязвимостей и значительный рост киберугроз. На этом фоне модель Zero Trust доказала свою способность противостоять многочисленным вызовам, связанным с использованием облачной и гибридной среды.

Мировое экспертное сообщество заявляет об актуальности и развитии тренда в 2023 году[58], а регулярные массовые утечки персональных данных подтверждают необходимость применения данной модели в целях кибербезопасности. Так, «объем утечек персональных данных в России в 2022 году составил 667 млн записей, что почти в 2,7 раза больше, чем годом ранее»[59].

Zero Trust — это модель безопасности, разработанная бывшим аналитиком Forrester Джоном Киндервагом[60] в 2010 году, которая легла в основу наиболее популярной концепции в сфере кибербезопасности. Суть концепции Zero Trust заключается в том, что весь трафик, даже если он уже находится внутри периметра, рассматривается как враждебный. Архитектура «нулевого доверия» основывается на утверждении, что ни одному пользователю или приложению по умолчанию не следует доверять. Доступ возможен только с наименьшими привилегиями, а доверие устанавливается только на основе проверки на каждом этапе взаимодействия. И поскольку защита не зависит от среды, «нулевое доверие» защищает приложения и службы, даже если они взаимодействуют между сетевыми средами, не требуя никаких архитектурных изменений или обновлений политик.

«Нулевое доверие» надежно соединяет пользователей, устройства и приложения с помощью бизнес-политик в любой сети, обеспечивая безопасную цифровую трансформацию[61].
К 2026 году 10% крупных предприятий будут иметь комплексную и сформировавшуюся инфраструктуру нулевого доверия[62].

03. Под контролем государства

Киберпространство все чаще используется в политических и идеологических целях, что наносит колоссальный урон экономикам всех стран мира, в том числе и российской[63]. Только во втором квартале 2023 года число кибератак на российские ИТ-компании выросло в 4 раза по сравнению с аналогичным периодом 2022-го и достигло 4 тыс. Центр мониторинга кибербезопасности «Лаборатория Касперского» отмечает, что в России и СНГ ИТ-рынок остается в тройке наиболее атакуемых хакерами отраслей[64].

Средняя стоимость одного инцидента утечки данных в 2023 году достигла рекордного значения и составила 4,45 млн долларов, прибавив 15,3% с 2020 года[65].

Сегмент кибербезопасности в России развивается ускоренными темпами, что подтверждает глобальный индекс киберготовности, который поднялся с 28 места в 2019 году[66] на 8 место по итогам 2020 года[67]. Государство постоянно принимает меры по укреплению технологического суверенитета страны. Так, в 2022 году было принято 257 нормативных правовых актов, касающихся регулирования сфер ИБ, ИТ и цифровой экономики в целом, что на 25% больше по сравнению с 2021 годом. Информационная безопасность по активности российских законодателей оказалась на втором месте с долей в 20,6%, а замыкает тройку лидеров категория «Биометрия и персональные данные» (10,9%). Заметные доли принятых нормативно-правовых актов в сфере информационной безопасности в 2022 году также получили безопасность КИИ (5,8%), и импортозамещение — 4,7%[68]. В числе наиболее значимых инициатив, принятых в 2022–2023 годах в области кибербезопасности, можно выделить следующие: 17 января 2022 Президент РФ подписал указ, согласно которому Минобороны наделяется полномочиями по определению политики в области международной информационной безопасности. По этому указу ФСБ вносит сведения об объектах критической информационной

инфраструктуры (КИИ) в список объектов, которые могут быть использованы иностранными организациями против безопасности Российской Федерации[69]. Важнейшими документами стали следующие указы Президента РФ: Указ от 30 марта 2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», запрещающий закупку иностранного ПО для использования на значимых объектах КИИ РФ без согласования с уполномоченным органом и Указ от 1 мая 2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», обязывающий организации сформировать отдельные структурные подразделения, отвечающие за соблюдение ИБ. Этим указом был введен запрет на использование средств защиты информации, странами происхождения которых являются недружественные иностранные государства[70]. В декабре 2022 года Правительство РФ выпустило распоряжение, которым утвердило Концепцию формирования и развития культуры безопасности граждан РФ[71], так как основной целью финансовых киберугроз остаются физи- ческие лица — в 2022 году на их долю пришлось 61,8% атак[72]. Можно сказать, что это активизация продвижения киберкультуры и кибергигиены, без которой невозможна борьба с киберугрозами.

В настоящее время обсуждается рассмотрение законопроекта «об оборотных штрафах за утечки биометрических персональных данных». Итоговая версия предусматривает наказание за подобные инциденты от 0,1 до 3% совокупной выручки компании в зависимости от количества субъектов персональных данных. Документ оформлен как поправки в Кодекс об административных нарушениях[73].

04. Арсенал хактивистов

Геополитическая обстановка с началом СВО создала основу для развития политически мотивированных групп хакеров, интересы которых не связаны в первоочередном порядке с финансовой выгодой. По итогам 2022 года прирост доли рассматриваемых инцидентов преимущественно произошел в секторе СМИ, транспортной отрасли и госучреждениях в связи с атаками хактивистов[74], экспертами рынка прогнозируется сохранение тенденции и в период с 2023 по 2025 год. Не останутся в стороне и широкие возможности хактивистов в использовании ботов, которые способны вести споры и пропаганду в интернете с целью политической дестабилизации общества[75].

Увеличение количества атак наблюдается также на промышленность и критическую инфраструктуру, где можно отметить тенденцию к использованию хакерами новых сложных для выявления способов атак на средства и архитектуры информационной безопасности[76]. Со стороны государства и бизнеса ожидается развитие новых средств защиты с акцентом на проактивную защиту и использование технологий блокчейна для систем аутентификации, хранилищ данных, с целью предотвращения утечек данных.

Следует обратить внимание на новую точку доступа в системы жертв — IoT-устройства. IoT-устройства имеют достаточно ограниченные вычислительные возможности, что обуславливает сложность использования классических средств защиты, таких как сетевые экраны и сканеры ВПО. Ожидается, что и производители и вендоры решат проблему растущей угрозы установкой встроенных систем защиты на устройства интернета вещей на этапе производства и выпуска.

Рассматривая методы атак, в ближайшие годы прогнозируется рост их количества с использованием шифровальщиков и вайперов. Благодаря развитию машинного обучения и «умной» социальной инженерии хакеры разработают новые подходы для организации атак на бизнес и госучреждения. В настоящее время сообщество хакеров переживает свое становление — растет потенциал обмена информацией, данными и ВПО посредством различных каналов, при этом для молодых людей из стран/регионов с низким уровнем финансового благополучия населения атаки на бизнес выступают в качестве социального лифта и инструмента легкого заработка.

05. Биометрия на службе безопасности

Многофакторная аутентификация представляет собой простую, надежную концепцию защиты, которая требует не менее двух способов подтверждения данных аккаунта. При этом факторы аутентификации не должны быть связаны между собой. Многофакторная аутентификация пришла на смену простым парольным системам защиты аккаунтов, поскольку хакерам, использующим современные технологии, не представляет труда скомпрометировать учетные данные пользователя, которые хранятся в зашифрованном виде. Также компрометация учетных данных исходит и от самих пользователей, которые относятся небрежно к правилам хранения паролей. В ближайшие годы ожидается, что многофакторная аутентификация будет становиться все более распространенной и сложной. Она будет включать в себя не только пароль и код подтверждения, но и биометрические данные, такие как отпечатки пальцев, сканирование лица и голоса, а также анализ поведения пользователя. Кроме того, будут использоваться новые методы аутентификации, такие как блокировка лица и голосовое управление.

Рынок многофакторной аутентификации оценивался в 10,64 млрд долларов в 2020 году и, как ожидается, достигнет 28,34 млрд долларов США к 2026 году и будет расти со среднегодовым темпом 17,83% в течение прогнозируемого периода (2021–2026)[77].

Таким образом, многофакторная аутентификация будет становиться все более интегрированной и автоматизированной, что поможет сделать процесс аутентификации более безопасным и удобным для пользователей.

06. Мобильная кибербезопасность

Мобильная кибербезопасность представляется как один из векторов активного роста в ближайшие годы. В первую очередь эта тенденция связана с увеличением числа удаленных рабочих мест и использованием персоналом различных мобильных устройств, подключенных к различным незащищенным сетям. Киберпреступники будут продолжать использовать уже известные уязвимости и методы атак, а также разрабатывать новые способы взлома устройств и получения доступа к конфиденциальным данным. Некоторые возможные угрозы могут включать в себя утечки данных через мобильные приложения, фишинговые атаки на мобильные устройства и использование вредоносного программного обеспечения, способного обходить существующие защитные механизмы. При этом будут разрабатываться новые технологии и инструменты для обнаружения и предотвращения кибератак, такие как машинное обучение и искусственный интеллект.

Отдельно отметим, что киберпреступники начали активно использовать мессенджеры, которые позволяют получить доступ к широкой аудитории при сохранении относительной анонимности. Одной из основных площадок стал Telegram, где активно ведется торговля данными, ВПО, распространяются объявления об услугах взлома различных ресурсов. Пик активности киберпреступности в мессенджерах был зафиксирован в 2022 году[78] и очевидно, что растущий тренд развития криминальных площадок в мессенджерах сохранится в перспективе с 2023 по 2025 год, обеспечивая снижение порога входа новых участников киберпреступности и упрощая торговлю ВПО и предложением услуг хакеров или целых сообществ хакеров.

07. Акцент на контейнерные среды и облачные решения

Недостаток «железа» в нужном объеме на российском рынке в связи с уходом ряда западных компаний в 2022 году вынудил отечественные компании переходить на использование облачных решений в оперативном режиме. При этом даже консервативно настроенные игроки рынка, которые ранее не рассматривали возможности перевода инфраструктуры на облака или в контейнерные среды, все чаще прибегают именно к этим методам, увеличивая долю контейнеризации своей инфраструктуры от 1 до 3%[79].

Поставщики облачных сервисов все чаще будут подвергаться атакам злоумышленников, по мере того как компании переносят свои данные в облачную инфраструктуру. В основном стоит ожидать атак, направленных на компрометацию учетных данных для доступа к ресурсам[80].

Контейнеризация — технология, которая позволяет запускать программное обеспечение в изолированных на уровне операционной системы пространствах. Контейнеры являются наиболее распространенной формой виртуализации на уровне операционной системы. С помощью контейнеров можно запустить несколько приложений на одном сервере (хостовой машине), изолируя их друг от друга. Процесс, запущенный в контейнере, выполняется внутри операционной системы хостовой машины, но при этом он изолирован от остальных процессов. Для самого процесса это выглядит так, будто он единственный работает в системе[81].

Развитие рынка контейнерных технологий в свою очередь увеличит интерес к средствам защиты микросервисов. Эксперты рекомендуют удерживать фокус на безопасность на всех уровнях жизненного цикла контейнера, а инструменты информационной безопасности интегрировать в разработку на как можно более раннем этапе, что в конечном итоге позволит уменьшить количество потенциальных угроз[82].

08. Кибер-преступления как услуга (CaaS)

Киберпреступность все больше стала обретать черты бизнеса, и связано это с усложнением систем защиты с одной стороны, и с желанием хакеров монетизировать свои навыки взлома — с другой. Новая бизнес-модель «Программы-вымогатели как услуга», RaaS (Ransomware-as-a-Service), предполагает сдачу в аренду злоумышленникам программ-вымогателей. При успешном развитии атаки с использованием арендованного ВПО доход получает как непосредственно злоумышленник, так и разработчик. Распространение таких партнерских программ позволяет монетизировать навыки различных специалистов, в случае, когда есть компетенции, но нет возможности или ресурсов действовать самостоятельно. Шифровальщики и вайперы остаются главным источником убытков для компаний[83], а RaaS обеспечит развитие этого тренда в будущем.

Другой трендовой моделью в мире киберпреступности становится «Фишинг как услуга» PhaaS (Phishing-as-a-Service). PhaaS — это вид организованной киберпреступности, когда преступники через интернет предлагают другим услуги фишинга в обмен на деньги. В 2022 году 73%[84] фишинговых атак на организации стали успешными, а модель PhaaS усилит этот тренд в ближайшем будущем. Хакеры, разработчики ВПО, «специалисты по фишингу» готовы предложить широкий спектр услуг в даркнете, при этом порог входа в указанные модели остается скромным, например, купить набор Stampado RaaS можно всего за 39 долларов[85].

Указанные модели стимулируют дополнительный рост киберпреступности, а возможность быть поставщиком таких услуг и получать доход выше средней заработной платы в ИТ-отрасли есть не только у продвинутых хакеров, но и у талантливых ребят из различных регионов Российской Федерации, которые не находят возможностей развиваться в легальных сегментах мира ИТ.

09. Доверчивые пользователи

Социальная инженерия всегда была для хакеров и мошенников одним из самых действенных инструментов для компрометации данных. В 2022 году в организациях атаки на сотрудников были успешными в 43% случаев, в отношении частных лиц — в 93% случаев[86].

Обманом злоумышленники заставляют людей предоставить личные данные, аккаунты и т.д. Дальнейшее развитие киберпреступности будет связано со специализацией хакеров с целью монетизации собственных навыков и компетенций. В ближайшие годы продолжится рост числа атак с использованием социальной инженерии — от создания deepfakes (фальшивых видео- и аудиофайлов) до использования личных данных пользователей социальных сетей для создания убедительных историй и обмана. Отдельно выделим фишинг, который смещается в сторону социальных сетей, мессенджеров и ботов, собирающих информацию. Повсеместное внедрение многофакторной аутентификации может способствовать созданию новых схем мошенничества по подмене SIM-карт, когда мошенники убеждают сотового оператора перенести номер на другую карту. Для нивелирования негативных сторон развития «умной социальной инженерии», которая будет использовать в том числе машинное обучение и искусственный интеллект, в первую очередь будет иметь значение распространение культуры «цифровой гигиены» в обществе.

10. Искусственный интеллект на службе безопасности

Роль искусственного интеллекта и машинного обучения в кибербезопасности будет расти год от года, обеспечивая эффективную систему мониторинга и предупреждения атак, моделирование поведения хакеров, высокую скорость оценки и выявления аномального поведения в сетях. По прогнозам, сегмент ИБ-решений с применением ИИ к 2027 году может составить 46 млрд долларов[87]. И в дополнение: машинное обучение позволит автоматизировать многие рутинные процессы специалистов по кибербезопасности и продолжит свое развитие в синергии с новыми квантовыми вычислительными технологиями. Поддержку тренду окажет текущая конъюнктура рынка кадров, на котором сложилась ситуация, когда в мире около 3,5 млн незакрытых вакансий ИБ-специалистов[88]. При этом безопасность и конфиденциальность будут ориентированы на человека как на главную причину утечек. Компании могут стать более устойчивыми в вопросах кибербезопасности путем внедрения программ безопасности, ориентированных на человека, которые станут частью цифрового профиля. Так, к 2027 году 50% директоров по информационной безопасности внедрят ориентированные на сотрудников подходы в свои программы кибер-защиты[89]. Искусственный интеллект и машинное обучение внесут большой вклад в становление культуры взаимного доверия и осознание общих рисков при принятии решений[90].

Центр информационной безопасности Университета Иннополис

Материал подготовила Оксана Федотова

Центр информационной безопасности — одно из технологических подразделений Университета Иннополис

Специалисты Центра оказывают услуги на любом из этапов, связанных с киберинцидентами и защитой данных:

- **пентест** — исследование защищенности компьютерных систем организации для предотвращения атаки;
- **расследование** уже совершенных киберинцидентов;
- **обучение персонала**, чтобы нападение хакеров не повторились;
- **разработка организационно-распорядительной документации** «О персональных данных» для отлаживания процессов информационной безопасности в компании.

Среди компаний-заказчиков: Татэнергосбыт, Алроса, Казанский юридический институт МВД России, Башнефтегеофизика, УМВД России по г.о. Домодедово и другие.

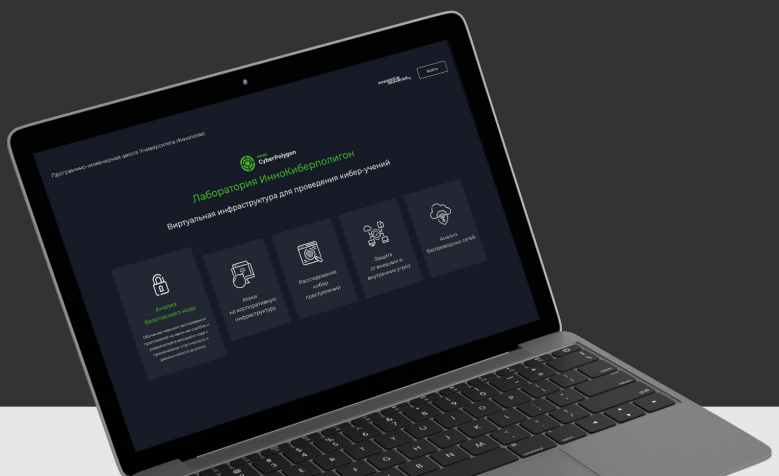
Команда Центра в том числе создает собственные программные продукты для обучения кибербезопасности.

Иннокиберполигон

Передовое решение Центра информационной безопасности. Это виртуальная полностью отечественная инфраструктура для проведения киберучений по ИБ и моделирования инфраструктуры предприятий. Создана в рамках федерального проекта «Передовые инженерные школы».

Модули:

- **Курсы** — практико-ориентированное обучение с подробной теоретической частью
- **Тренажеры** — выполнение лабораторных работ (без теории)
- **Киберучения** — моделирование конкретных кибератак и обучение их противодействию в составе команд — атакующих и защищающихся
- **CTF** — быстрые соревнования по информационной безопасности для школьников и студентов
- **Квалификации** — сборная образовательная программа из курсов, тренажеров, киберучений, CTF



Михаил Серегин
Руководитель центра

m.seregin@innopolis.ru

Никита Кормильцев
Руководитель проекта
Иннокиберполигон

n.kormiltcev@innopolis.ru

Университет Иннополис
ул. Университетская, д. 1

innopolis.university

В зависимости от выбранного уровня обучения, у специалистов формируются компетенции:

1. Тестирование на проникновение
2. Выявление компьютерных атак и расследование инцидентов ИБ
3. Построение эшелонированной защиты и тестирования средств защиты
4. Тестирование на проникновение и защита беспроводных сетей
5. Тестирование приложений на наличие ошибок и уязвимостей в исходном коде с применением статического и динамического анализа

45 секунд

развертывание виртуальной машины в любом браузере

до 90% ресурсов

экономит заказчик благодаря удаленному доступу (оборудование, помещение)

Преимущества:

Интеграция средств защиты основных игроков рынка ИБ

Решения 16 партнеров, что составляет примерно 80% отечественного рынка ИБ интегрированы в Иннокиберполигон

Многочисленные тесты

105 человек обучено на площадке только за последний месяц, при том, что официально продукт будет запущен только в конце осени этого года

Удаленный доступ

Не требует физического присутствия обучающихся, они могут подключиться из любой точки мира

Сноски

1 Size of cyber security market worldwide from 2021 to 2030 / Statista. URL: https://www.statista.com/statistics/1256346/worldwide-cyber-security-market-revenues (дата обращения 07.09.2023). — Текст: электронный

2 Там же

3 Cybersecurity Market Size & Share Analysis — Growth Trends & Forecasts (2023–2028) / Mordor intelligence. URL: https://www.mordorintelligence.com/industry-reports/cyber-security-market (дата обращения 07.09.2023). — Текст: электронный

4 Там же

5 Critical Infrastructure Protection Market Size / Mordor intelligence. URL: https://www.mordorintelligence.com/industry-reports/global-critical-infrastructure-protection-market-industry (дата обращения 12.09.2023). — Текст: электронный

6 Global Critical Infrastructure Protection Market Size To Surpass USD254.51 Billion by 2032 | CAGR of 6.27% / GlobeNewswire. URL: https://www.globenewswire.com/en/news-release/2023/05/15/2669171/0/en/Global-Critical-Infrastructure-Protection-Market-Size-To-Surpass-USD-254–51-Billion-by-2032-CAGR-of-6–27.html#:~: text=The%20Global%20Critical%20Infrastructure%20Protection, published%20by%20Spherical%20Insights%20%26%20Consulting (дата обращения 07.09.2023). — Текст: электронный

7 Cybersecurity Market Size & Share Analysis — Growth Trends & Forecasts (2023–2028) / Mordor intelligence. URL: https://www.mordorintelligence.com/industry-reports/cyber-security-market (дата обращения 07.09.2023). — Текст: электронный

8 INFORMATION SECURITY SPEND GROWTH FROM 2017 TO 2023 / SAPPHIRE URL: https://www.sapphire.net/insights/information-security-spend/ (дата обращения 07.09.2023). — Текст: электронный

9 Cybersecurity outpaces wider tech market with 12.5% growth in challenging economy / Canalys. URL: https://canalys.com/newsroom/cybersecurity-market-Q1–2023 (дата обращения 19.09.2023). — Текст: электронный

10 Финансовая отчётность Palo Alto Networks / Finrange. URL: https://finrange.com/ru/company/NYSE/PANW/financial-statements (дата обращения 07.09.2023). — Текст: электронный

11 Cybersecurity outpaces wider tech market with 12.5% growth in challenging economy / Canalys. URL: https://canalys.com/newsroom/cybersecurity-market-Q1–2023 (дата обращения 19.09.2023). — Текст: электронный

12 Финансовая отчётность Fortinet / Finrange. URL: https://finrange.com/ru/company/NASDAQ/FTNT/financial-statements (дата обращения 07.09.2023). — Текст: электронный

13 Cybersecurity outpaces wider tech market with 12.5% growth in challenging economy / Canalys. URL: https://canalys.com/newsroom/cybersecurity-market-Q1–2023 (дата обращения 19.09.2023). — Текст: электронный

14 Там же

15 Там же

16 Актуальные киберугрозы: итоги 2022 года / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id9 (дата обращения 07.09.2023). Текст: электронный

17 Там же

18 Число кибератак в России и в мире / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#:~: text=%D0%92%D1%81%D0%B5%D0%B3%D0%BE%20%D0%B7%D0%B0%202022%20%D0%B3%D0%BE%D0%B4%20%D0%B1%D1%8B%D0%BB%D0%BE, Gamaredon%2C%20MuddyWater%2C%20Mustang%20Panda (дата обращения — 19.09.2023). Текст: электронный

19 Там же

20 Там же

21 Cost of a Data Breach Report 2023 / Отчет IBM Security. URL: https://www.ibm.com/downloads/cas/E3G5JMBP (дата обращения 07.09.2023). Текст: электронный

22 Там же

23 Там же

24 Там же

25 Актуальные киберугрозы: итоги 2022 года / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id9 (дата обращения 07.09.2023). Текст: электронный

26 Там же

27 Там же

28 В 2023 целью хакеров станет не только финансовая, но и политическая выгода / RG.RU Специальный проект Digital. URL: https://rg.ru/2023/02/28/v-2023-celiu-hakerov-stanet-ne-tolko-finansovaia-no-i-politicheskaia-vygoda.html (дата обращения 07.09.2023). Текст: электронный

29 Актуальные киберугрозы: итоги 2022 года / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id9 (дата обращения 07.09.2023). Текст: электронный

30 Turning Tides Navigating the Evolving World of Cybercrime / Отчет Arete Advisors. URL: https://areteir.com/static/cbad1568d2538e9a7d20c30ba038d0fc/Turning-Tides.pdf (дата обращения 07.09.2023). Текст: электронный

31 Ransomware Revenue Down As More Victims Refuse to Pay / Аналитический отчет Chainalysis. URL: https://www.chainalysis.com/blog/crypto-ransomware-revenue-down-as-victims-refuse-to-pay (дата обращения 07.09.2023). Текст: электронный

32 Improved Security and Backups Result in Record Low Number of Ransomware Payments / Coveware. URL: https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments (дата обращения 08.09.2023). Текст: электронный

33 Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы / Официальный сайт «Центра стратегических исследований» URL: https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf (дата обращения 19.09.2023). Текст: электронный

34 Там же

35 Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы / Официальный сайт «Центра стратегических исследований» URL: https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf (дата обращения 19.09.2023). Текст: электронный

36 Исследование рынка информационной безопасности в России по клиентским сегментам / Официальный сайт «РТК Солар». URL: https://rt-solar.ru/upload/iblock/962/b7wyn7498evdp1jf8t7iccj5239ug4i9/Issledovanie-rynka-IB-RF-2022.pdf (дата обращения 19.09.2023). Текст: электронный

37 Там же

38 ЦСР представил доклад о потенциале российских решений в области кибербезопасности / Официальный веб-ресурс «Центра стратегических разработок» (ЦСР). URL: https://www.csr.ru/ru/events/tssr-predstavil-doklad-o-potentsiale-rossiyskikh-resheniy-v-oblasti-kiberbezopasnosti/ (дата обращения 19.09.2023). Текст: электронный

39 Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы / Официальный сайт «Центра стратегических разработок» URL: https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf (дата обращения 19.09.2023). Текст: электронный

40 Около четверти кибератак в России в 2022 году приходилось на сферу промышленности / Российское государственное федеральное информационное агентство. URL: https://tass.ru/ekonomika/17622093 (дата обращения 18.09.2023). Текст: электронный

41 Число кибератак на госучреждения увеличилось в 2022 году / Российское государственное федеральное информационное агентство. URL: https://ria.ru/20230207/ataki-1850280231.html (дата обращения 18.09.2023). Текст: электронный

42 Около четверти кибератак в России в 2022 году приходилось на сферу промышленности / Российское государственное федеральное информационное агентство. URL: https://tass.ru/ekonomika/17622093 (дата обращения 18.09.2023). Текст: электронный

43 Отчет «Кибератаки на российские компании в 2022 году» / Официальный сайт «РТК Солар». — Москва, 2023. — 13 с. URL: https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf (дата обращения 18.09.2023). — Текст: электронный

44 Атаки на российские компании во втором квартале 2023 года / Официальный сайт «РТК Солар». URL: https://rt-solar.ru/upload/iblock/956/s6a6rc6gs9usip5xdp8vq27419khu4hx/Otchet_Ataki_na_rossiyskie_kompanii_vo_II_kvartale_2023_g.pdf (дата обращения 19.09.2023). Текст: электронный

45 Там же

46 Solar JSOC Security Report. Итоги 2019 года / Официальный сайт «РТК Солар». URL: https://rt-solar.ru/upload/iblock/faf/Solar-JSOC-Security-Report-2019.pdf (дата обращения 20.09.2023). Текст: электронный

47 Атаки на российские компании во втором квартале 2023 года / Официальный сайт «РТК Солар». URL: https://rt-solar.ru/upload/iblock/956/s6a6rc6gs9usip5xdp8vq27419khu4hx/Otchet_Ataki_na_rossiyskie_kompanii_vo_II_kvartale_2023_g.pdf (дата обращения 19.09.2023). Текст: электронный

48 Там же

49 Атаки на российские компании во втором квартале 2023 года / Официальный сайт «РТК Солар». URL: https://rt-solar.ru/upload/iblock/956/s6a6rc6gs9usip5xdp8vq27419khu4hx/Otchet_Ataki_na_rossiyskie_kompanii_vo_II_kvartale_2023_g.pdf (дата обращения 19.09.2023). Текст: электронный

50 Актуальные киберугрозы: I квартал 2023 года / Официальный сайт Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q1/ (дата обращения: 07.08.2023). — Текст: электронный

51 MITRE ATT&CK / Официальный сайт. URL: https://attack.mitre.org/ (дата обращения: 07.08.2023). — Текст: электронный

52 Реестр сертифицированных СЗИ ФСБ / Электронный ресурс «Госзакупки ИТ». URL: https://www.goszakupki-it.ru/knowledge/articles/reestry_importozameshcheniya/1505 (дата обращения 29.08.2023). — Текст: электронный

53 Сертификация ФСТЭК / Официальный сайт «РТК Солар». URL: https://rt-solar.ru/products/solar_dozor/blog/2713/ (дата обращения 29.08.2023). — Текст: электронный

54 Постановление правительства Российской Федерации № 1236 от 16.11.2016 г. / Справочно-правовая система по законодательству Российской Федерации. URL: https://base.garant.ru/71252170/ (дата обращения 28.08.2023). — Текст: электронный

55 Число кибератак в России и в мире / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#:~: text=%D0%92%D1%81%D0%B5%D0%B3%D0%BE%20%D0%B7%D0%B0%202022%20%D0%B3%D0%BE%D0%B4%20%D0%B1%D1%8B%D0%BB%D0%BE,Gamaredon%2C%20MuddyWater%2C%20Mustang%20Panda (дата обращения 19.09.2023). — Текст: электронный

56 Цифровизаиця банков / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9E%D0%B1%D0%B7%D0%BE%D1%80_TAdviser:_%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D0%B1%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2_2022 (дата обращения 18.09.2023). — Текст: электронный

57 Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы / Официальный сайт «Центра стратегических исследований». URL: https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf (дата обращения 19.09.2023). — Текст: электронный

58 2023 ATARC Zero Trust Summit / Онлайн-ресурс. URL: https://www.govevents.com/details/61075/2023-atarc-zero-trust-summit (дата обращения 18.09.2023). — Текст: электронный

59 Утечки данных в России / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#:~: text=%D0%9E%D0%B1%D1%8A%D0%B5%D0%BC%20%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA%20%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85%20%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85%20%D0%B2,%D1%80%D0%B0%D0%B7%D0%B0%20%D0%B1%D0%BE%D0%BB%D1%8C%D1%88%D0%B5%2C%20%D1%87%D0%B5%D0%BC%20%D0%B3%-D0%BE%D0%B4%D0%BE%D0%BC%20%D1%80%D0%B0%D0%BD%D0%B5%D0%B5 (дата обращения 11.09.2023). — Текст: электронный

60 Что такое Zero Trust? Модель безопасности / веб-сайт в формате блогов. URL: https://habr.com/ru/companies/varonis/articles/472934/ (дата обращения 12.09.2023). — Текст: электронный

61 What Is Zero Trust? / Официальный сайт «Zscaler». URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trus (дата обращения 12.09.2023). — Текст: электронный

62 Gartner Unveils Top Eight Cybersecurity Predictions for 2023–2024 / Press Release Newsroom. URL: https://www.gartner.com/en/newsroom/press-releases/2023–03–28-gartner-unveils-top-8-cybersecurity-predictions-for-2023–2024 (дата обращения 12.09.2023). — Текст: электронный

63 Яковлева Анна Валерьевна. КИБЕРБЕЗОПАСНОСТЬ И ЕЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ (ЗАРУБЕЖНЫЙ И РОССИЙСКИЙ ОПЫТ) // Социально-политические науки. 2021. № 4. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-i-ee-pravovoe-regulirovanie-zarubezhnyy-i-rossiyskiy-opyt (дата обращения: 19.09.2023). — Текст: электронный

64 Число кибератак в России и в мире / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#.2A_.D0.A7.D0.B8.D1.81.D0.BB.D0.BE_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B0.D1.82.D0.B0.D0.BA_.D0.BD.D0.B0_.D1.80.D0.BE.D1.81.D1.81.D0.B8.D0.B9.D1.81.D0.BA.D0.B8.D0.B5_.D0.98.D0.A2-.D0.BA.D0.BE.D0.BC.D0.BF.D0.B0.D0.BD.D0.B8.D0.B8_.D0.B2.D1.8B.D1.80.D0.BE.D1.81.D0.BB.D0.BE_.D0.B2_4_.D1.80.D0.B0.D0.B7.D0.B0 (дата обращения 19.09.2023). — Текст: электронный

65 Cost of a Data Breach Report 2023 / Отчет IBM Security. URL: https://www.ibm.com/downloads/cas/E3G5JMBP (дата обращения 07.09.2023). — Текст: электронный

66 Глобальный индекс кибербезопасности / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D0%B4%D0%B5%D0%BA%D1%81_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_Global_Cybersecurity_Index_(GCI)#.D0.A0.D0.BE.D1.81.D1.81.D0.B8.D1.8F_.D0.BD.D0.B0_28-.D0.BC_.D0.BC.D0.B5.D1.81.D1.82.D0.B5 (дата обращения 19.09.2023). — Текст: электронный

67 Рейтинг стран по уровню кибербезопасности / NoNews. URL: https://nonews.co/directory/lists/countries/cybersecurity-index (дата обращения 19.09.2023). — Текст: электронный

68 Нормативных актов в сфере ИБ за 2022 год принято на 25% больше / InfoWatch. URL: https://www.infowatch.ru/company/presscenter/news/normativnykh-aktov-v-sfere-ib-za-2022-god-prinyato-na-25-bolshe (дата обращения 19.09.2023). — Текст: электронный

69 Минобороны получило полномочия для определения госполитики в области международной ИБ — указ президента / Онлайн-издание D-russia.ru. URL: https://d-russia.ru/minoborony-poluchilo-polnomochija-dlja-opredelenija-gospolitiki-v-oblasti-mezhdunarodnoj-ib-ukaz-prezidenta.html (дата обращения 19.09.2023). — Текст: электронный

70 Нормативных актов в сфере ИБ за 2022 год принято на 25% больше / InfoWatch. URL: https://www.infowatch.ru/company/presscenter/news/normativnykh-aktov-v-sfere-ib-za-2022-god-prinyato-na-25-bolshe (дата обращения 19.09.2023). — Текст: электронный

71 Распоряжение Правительства Российской Федерации от 22.12.2022 № 4088-р / Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202212230035 (дата обращения 19.09.2023). — Текст: электронный

72 Финансовые киберугрозы в 2022 году / ЛАБОРАТОРИЯ КАСПЕРСКОГО. URL: https://securelist.ru/financial-cyberthreats-in-2022/107223/#:~: text=%D0%A1%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0%20%D0%B7%D0%B0%202022%20%D0%B3%D0%BE%D0%B4%20%D1%81%D0%B2%D0%B8%D0%B4%D0%B5%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D1%83%D0%B5%D1%82,2%25 (дата обращения 19.09.2023). — Текст: электронный

73 Бизнес предложили штрафовать до 500 млн долл. за утечку данных россиян / РБК. URL: https://www.rbc.ru/technology_and_media/27/07/2023/64c15e069a79474102dac8b0 (дата обращения 19.09.2023). — Текст: электронный

74 Актуальные киберугрозы: итоги 2022 года / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 07.09.2023). — Текст: электронный

75 Какие тренды кибербезопасности нас ждут в 2023 году / SecurityLab от Positive Research. URL: https://www.securitylab.ru/news/535499.php (дата обращения 07.09.2023). — Текст: электронный

76 В России резко выросло число угроз критической и информационной инфраструктуры страны / Обозрение. URL: https://oboz.info/v-rossii-rezko-vyroslo-chislo-ugroz-kriticheskoj-i-informatsionnoj-infrastruktury-strany/ (дата обращения 07.09.2023). — Текст: электронный

77 РЫНОК МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ: РОСТ, ТЕНДЕНЦИИ, ВЛИЯНИЕ COVID-19 И ПРОГНОЗЫ (2023–2028 ГГ.) / Mordor intelligence. URL: https://www.mordorintelligence.com/ru/industry-reports/multifactor-authentication-market (дата обращения 07.09.2023). — Текст: электронный

78 Кибербезопасность в 2022–2023. Тренды и прогнозы / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id17 (дата обращения 07.09.2023). — Текст: электронный

79 Positive Technologies — о технологических трендах в России и мире / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-o-tekhnologicheskih-trendah-v-rossii-i-mire/ (дата обращения 07.09.2023). — Текст: электронный

80 Кибербезопасность в 2022–2023. Тренды и прогнозы / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id1 (дата обращения 07.09.2023). — Текст: электронный

81 Основы контейнеризации (обзор Docker и Podman) / веб-сайт в формате блогов. URL: https://habr.com/ru/articles/659049/ (дата обращения 12.09.2023). — Текст: электронный

82 Кто, как и зачем должен защищать контейнерную инфраструктуру? / Издание Anti-Malware.ru https://www.anti-malware.ru/analytics/Technology_Analysis/Container-Security (дата обращения 12.09.2023). — Текст: электронный

83 Phishing-as-a-Service (PhaaS) Explained / PowerDMAR C. URL: https://powerdmarc.com/ru/phishing-as-a-service-phaas/ (дата обращения 12.09.2023). — Текст: электронный

84 Там же

85 Программа-вымогатель как услуга (RaaS) — растущая угроза кибербезопасности / CISOCLUB. URL: https://cisoclub.ru/programma-vymogatel-kak-usluga-raas-rastushhaya-ugroza-kiberbezopasnosti/ (дата обращения 12.09.2023). — Текст: электронный

86 Актуальные киберугрозы: итоги 2022 года / Официальный веб-ресурс компании Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id9 (дата обращения 07.09.2023). — Текст: электронный

87 Мировой рынок ИБ-услуг к 2025 году достигнет объема в $94 млрд / ИКС–МЕДИА. URL: https://www.iksmedia.ru/news/5873383-Mirovoj-rynok-IBuslug-k-2025-godu.html (дата обращения 07.09.2023). — Текст: электронный

88 Там же

89 Информационная безопасность (тренды) / TADVISER. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%93%D0%BB%D0%B0%D0%B2%D0%BD%D1%8B%D0%B5_%D1%82%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B8_%D0%B2_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8 (дата обращения 07.09.2023). — Текст: электронный

90 Gartner Places Generative AI on the Peak of Inflated Expectations on the 2023 Hype Cycle for Emerging Technologies / Press Release Newsroom. URL: https://www.gartner.com/en/newsroom/press-releases/2023–08–16-gartner-places-generative-ai-on-the-peak-of-inflated-expectations-on-the-2023-hype-cycle-for-emerging-technologies (дата обращения 12.09.2023). — Текст: электронный

Университет Иннополис
2023