positive technologies

DEPHAZE

PT Dephaze

СОДЕРЖАНИЕ

ЕСТЬ ЛИ НЕОБХОДИМОСТЬ В АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ 4

КИБЕРАТАКИ В РОССИЙСКИХ ОРГАНИЗАЦИЯХ 9

ПОЧЕМУ КОМПАНИИ ВСЕ ЕЩЕ УЯЗВИМЫ ПЕРЕД КИБЕРПРЕСТУПНИКАМИ 15

ОЦЕНКА ЗАЩИЩЕННОСТИ 18

КАК ОБЕСПЕЧИТЬ РЕГУЛЯРНУЮ ПРОВЕРКУ БЕЗОПАСНОСТИ 27

ЕСТЬ ЛИ НЕОБХОДИМОСТЬ В АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Несмотря на постоянно растущий спрос 1 на решения для информационной безопасности, число успешных кибератак на организации по всему миру ежегодно увеличивается. Так, по данным Positive Technologies, в 2023 году этот показатель вырос 2 на 18%, и, судя по тенденциям 3 2024 года, продолжит расти. Одним из факторов роста, по данным исследования 4 о киберустойчивости организаций, является цифровизация. Компании автоматизируют процессы и внедряют новые информационные технологии, что ведет к увеличению числа цифровых активов, которые могут стать уязвимым местом в инфраструктуре без обеспечения их оперативной защиты.

1

2

3

4

Цели, методы и участники исследования

Цель исследования — оценить зрелость информационной безопасности в российских компаниях, узнать, хорошо ли они справляются с кибератаками, есть ли у них планы по развитию ИБ на ближайшие пять лет и готовы ли они переходить от ручного тестирования на проникновение (пентеста) к автоматизации этого процесса.

Исследование основано на результатах анонимного опроса, который проводился в третьем квартале 2024 года. В опросе приняли участие представители российских компаний среднего и крупного бизнеса, до 300 специалистов из числа директоров по информационной безопасности и информационным технологиям, руководителей SOC, а также другие сотрудники, принимающие решения, связанные с ИТ-инфраструктурой и информационной безопасностью компаний из сферы ИТ, транспорта, промышленности, финансового сектора, ритейла и других отраслей.

Размер компаний

Для получения объективной оценки в исследовании принимали участие компании разного размера:

от 1000 до 2000
сотрудников

с численностью сотрудников
более 2000

Во вторую категорию также вошли компании, в которых число сотрудников превышает 5000 человек (см. рис. 1).

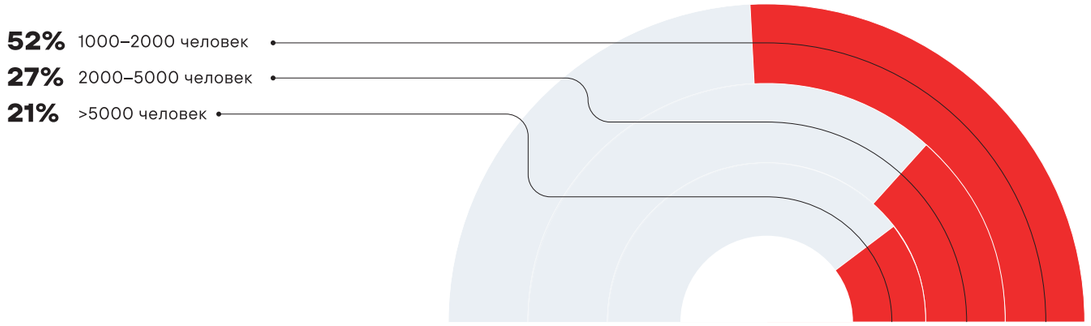


Рисунок 1. Размер компаний, участвовавших в исследовании (количество сотрудников)

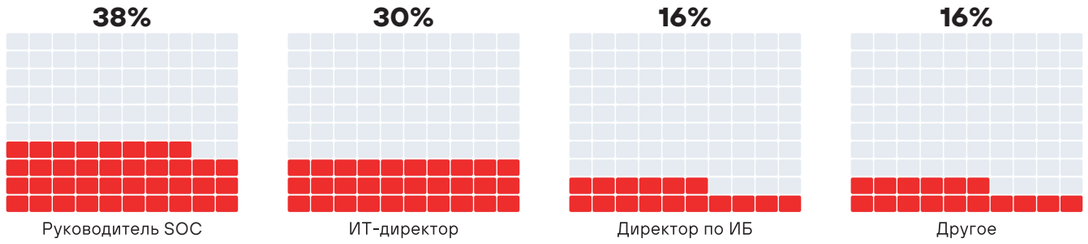


Рисунок 2. Специалисты, участвовавшие в исследовании

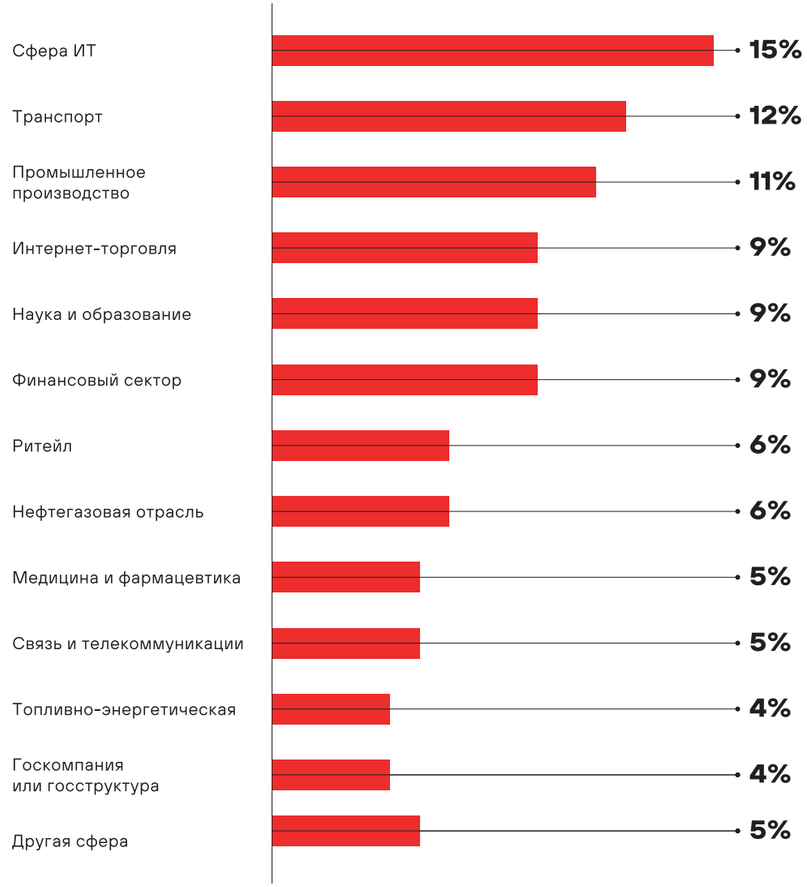


Рисунок 3. Сфера деятельности компаний — участников опроса

Основные результаты исследования

За последний год атакам подвергались **53%** опрошенных компаний, из них около 25% были атакованы меньше полугода назад. Чаще всего скомпрометированными оказывались удаленные устройства.

Среди опрошенных компаний **79%** указали, что изменения в их ИТ-среде происходят чаще, чем раз в квартал. При этом только **21%** опрошенных заказывают услуги по ручному тестированию на проникновение, из них регулярные пентесты делают только **64%**.

В среднем компании используют от 10 до 30 продуктов для ИБ. При этом планы на закупку новых решений в перспективе до 2 лет есть у 63% опрошенных компаний.

Согласно исследованию Positive Technologies «Итоги пентестов 2023» [5], в 96% случаев пентесты продемонстрировали потенциальную незащищенность компаний перед действиями внешних злоумышленников. В 100% проверенных компаний при проведении внутреннего пентеста специалисты смогли установить полный контроль над инфраструктурой, а в 63% было установлено, что совершить проникновение в сеть компании извне сможет даже злоумышленник с низкой квалификацией.

Можно сделать вывод, что несмотря на внедрение стратегий безопасности в компаниях разного размера, их уровень защищенности не позволяет обеспечить киберустойчивость. Это подтверждает исследование «Актуальные киберугрозы для организаций: итоги 2023 года» [6], в котором сказано, что количество успешных атак ежегодно растет по всему миру. В 2023 году их доля выросла на 18% по сравнению с 2022 годом, эти тенденции сохраняются [7] и в 2024 году.

В постоянно меняющемся ландшафте киберугроз важно не только выстраивать надежную систему защиты, но и регулярно проверять ее эффективность. Проверка защищенности инфраструктуры позволяет выявить и устранить слабые места в системе, снижая вероятность того, что злоумышленники используют их для проникновения. Есть ли такая практика в российских компаниях — покажет наше исследование.

5

6

7

КИБЕРАТАКИ В РОССИЙСКИХ ОРГАНИЗАЦИЯХ

Злоумышленники проникают в инфраструктуру предприятия, используя разные методы: от социальной инженерии и рассылок с вредоносными вложениями до эксплуатации уязвимостей. По нашим данным, количество успешных атак на организации ежегодно растет [8] по всему миру, чему способствует множество факторов, среди которых — сложная мировая геополитическая обстановка, массовая эксплуатация уязвимостей нулевого дня в популярном ПО, а также усложнение и изощренность атак.

8

Несмотря на значительные инвестиции в инфраструктуру безопасности, за последний год жертвами кибератак стали 55% опрошенных организаций, из которых каждая четвертая была атакована в последние полгода. Остальные участники опроса отметили, что сталкивались с инцидентами безопасности более полутора лет назад, и только небольшая часть компаний никогда не подвергалась кибератакам.

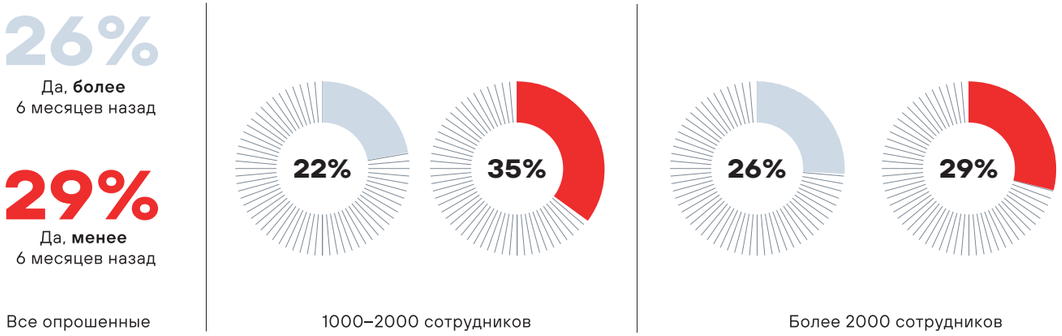


Рисунок 4. Подвергалась ли компания атакам за последний год

Последствия кибератак

Восемь из десяти опрошенных компаний столкнулись с серьезными последствиями кибератак в 2024 году, и лишь 13% компаний отметили, что не получили значительного урона от взлома. Четверть организаций сообщили о финансовых потерях — это говорит о том, что одной из главных целей для злоумышленников остаются деньги. Такое же количество компаний (чуть более 25%) сообщили о репутационных потерях. Однако самые большие риски связаны с непрерывностью бизнеса: 48% опрошенных отметили, что атака привела к незапланированным простоям, из-за которых компании были вынуждены приостановить ключевые процессы или потеряли контроль над оборудованием. Влияние атаки на конфиденциальные данные отметили 34% респондентов, а для 18% компаний инцидент привел к юридическим проблемам.

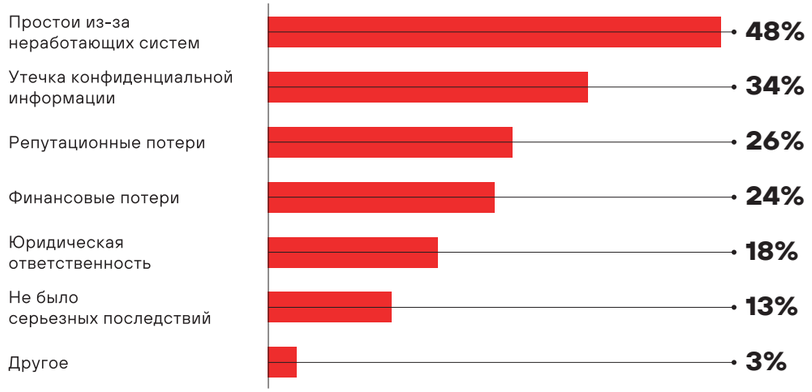


Рисунок 5. Негативные последствия кибератак

Скомпрометированные сегменты

Злоумышленники атакуют по всем направлениям, не ограничиваясь конкретными векторами или инфраструктурной средой. Периметр организации сильно размыт, и хакеры вынуждены тщательно готовиться — изучать инфраструктуру и собирать данные, — прежде чем начать кибератаку. Исследование показывает, что под угрозой находятся не только удаленные или локальные устройства, но и облачная инфраструктура, которой требуются специальные средства защиты. Можно предположить, что с ростом использования облачных решений число атак на них будет только расти.

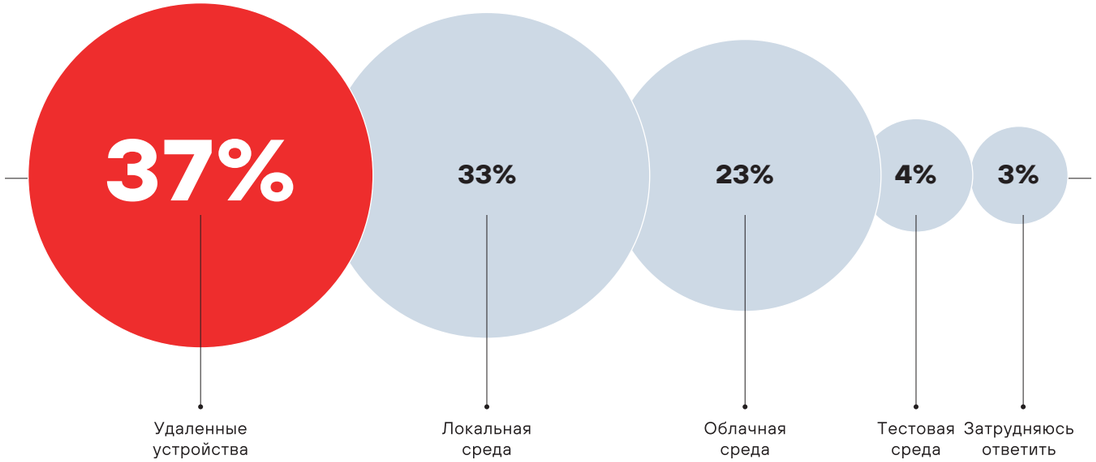


Рисунок 6. Какой сегмент был скомпрометирован в последней кибератаке

Используемые продукты для ИБ

Большинство организаций, участвовавших в опросе, используют от 10 до 30 решений для ИБ, и только 20% компаний используют менее 10 автоматизированных средств защиты. Несмотря на преимущества многоуровневого обеспечения безопасности, на практике такое количество систем не решают проблемы. При неправильной настройке решения производят много уведомлений о потенциальных проблемах и инцидентах, что затрудняет мониторинг и управление инфраструктурой, ограничивая способность организации обнаруживать угрозы и реагировать на них. Кроме того, поддержка работоспособности множества систем и их интеграции между собой требует дополнительных ресурсов, которые не все компании могут себе позволить.

Количество используемых продуктов для ИБ зависит от размера компании: в крупных компаниях в 2,5 раза чаще используется более 30 продуктов. Менее 10 систем чаще используют компании, в которых работает менее 2000 сотрудников. Среди крупных компаний встречаются и такие, которые используют для защиты инфраструктуры более 50 решений.

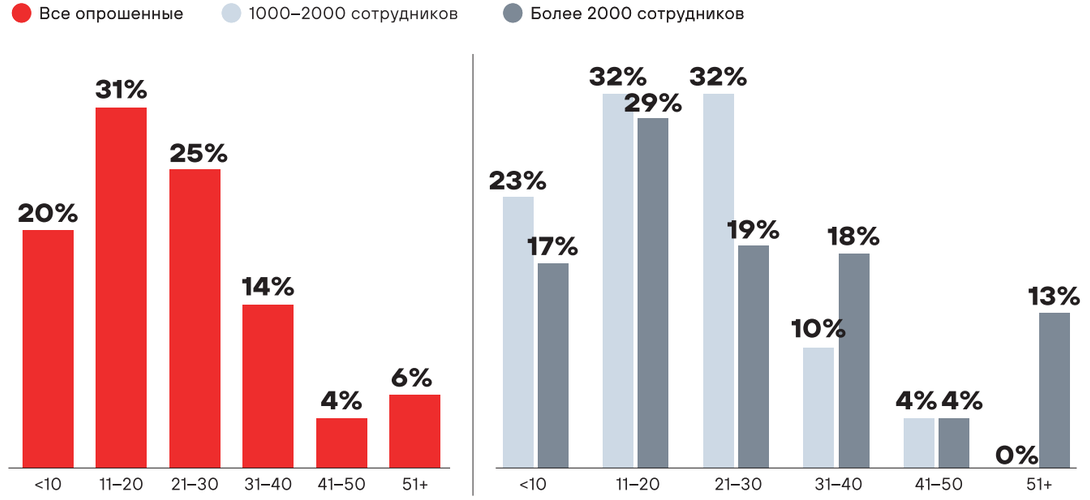


Рисунок 7. Количество используемых продуктов для ИБ

Стратегии информационной безопасности

Центр стратегических разработок в исследовании «Прогноз развития рынка кибербезопасности в Российской Федерации на 2024–2028 годы»[9] отмечает, что объем российского рынка ИБ в следующие пять лет будет расти со среднегодовым темпом прироста в 23,6% и к 2028 году достигнет 715 млрд рублей. Мы уточнили у компаний, планируют ли они закупки решений для информационной безопасности в краткосрочной или долгосрочной перспективе.

Результат опроса показывает, что для крупных компаний более характерно долгосрочное планирование: планы на 5 и более лет имеют 13% очень крупных компаний, тогда как среди организаций размером 1000–2000 сотрудников такие планы имеют только 3% компаний. При этом подавляющее большинство компаний (63%) имеет планы по закупкам систем для ИБ только в перспективе ближайших 1–2 лет, что говорит о тактическом уровне планирования. Возможно, для стратегического планирования компаниям не хватает информации о том, на каком уровне безопасности они находятся в данный момент.

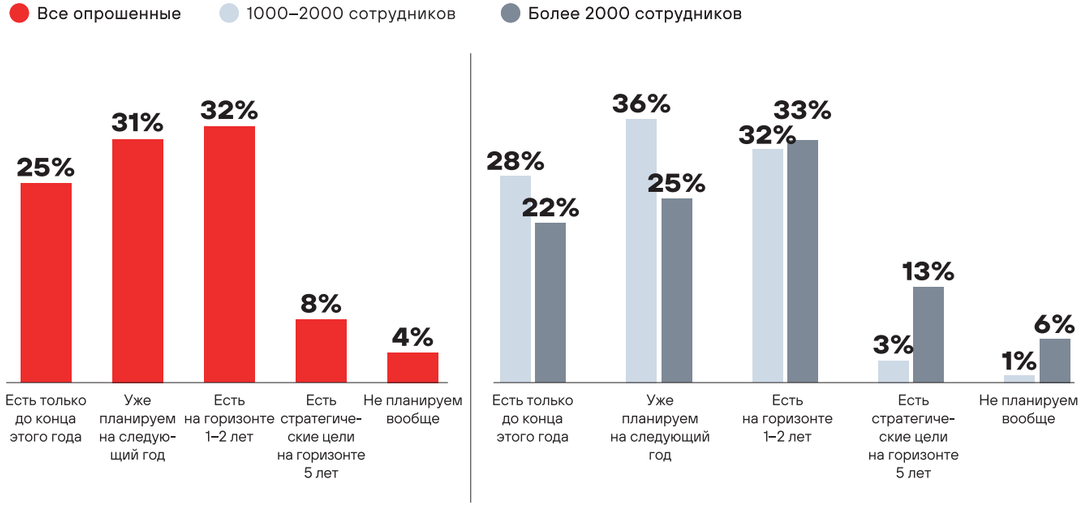


Рисунок 8. Планы по закупкам систем и продуктов для ИБ на ближайшее время

ПРОБЛЕМА № 1

Несмотря на инвестиции в ИБ, компании все еще недостаточно защищены и постоянно сталкиваются с кибератаками, что вынуждает их закупать новые средства защиты. С одной стороны, это говорит о том, что компании выстраивают эшелонированную защиту и многоступенчатую безопасность. С другой стороны — большое количество СЗИ создает много событий безопасности, которые требуют внимательного изучения службой ИБ, затрудняя определение приоритетных инцидентов и потенциальных угроз.

ПОЧЕМУ КОМПАНИИ ВСЕ ЕЩЕ УЯЗВИМЫ ПЕРЕД КИБЕРПРЕСТУПНИКАМИ

Знание собственной инфраструктуры

По данным опроса, каждая третья компания (30%), независимо от числа сотрудников, не уверена, что обладает точной информацией об аппаратном и программном обеспечении, которое формирует основу операционной деятельности. При этом практически любой ИТ-актив компании может стать входной точкой для злоумышленников, и специалисты, отвечающие за безопасность, должны знать, что именно нужно защищать.

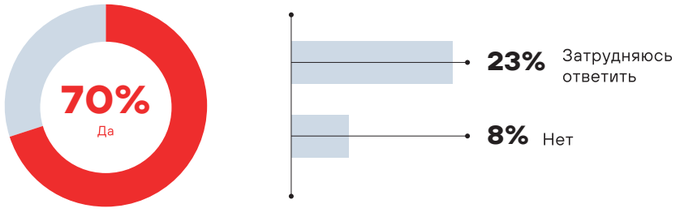


Рисунок 9. Знаете ли вы или ваша служба ИБ, сколько узлов есть в вашей компании в любой момент времени

Сложность ИТ-инфраструктуры растет во всех компаниях, и они вынуждены внедрять новые решения для управления безопасностью и поддержания киберустойчивости. Развертывание нового ПО, добавление или удаление рабочих станций неизбежно меняют инфраструктуру. Каждое изменение создает новые потенциальные бреши, которые могут использовать злоумышленники. Компании имеют сложную инфраструктуру, состоящую из дата-центров, ДМЗ, сегментов рабочих станций, географически распределенных офисов с разными часовыми поясами, тестовых сегментов и т. д. Все эти сегменты имеют различный уровень и особые требования к защите ИБ, контролировать которые в моменте очень сложно.

Изменение активов в инфраструктуре

Около 80% опрошенных компаний, независимо от размера, добавляют или отключают активы как минимум раз в квартал, что сильно меняет инфраструктуру и может оказать влияние на уровень защищенности. Добавление и отключение активов (серверов, сетевых устройств, ПО, систем управления БД, а также различных видов конфиденциальных данных) может спровоцировать появление дополнительных уязвимостей и незащищенных мест, которые могут быть использованы для проведения атак.

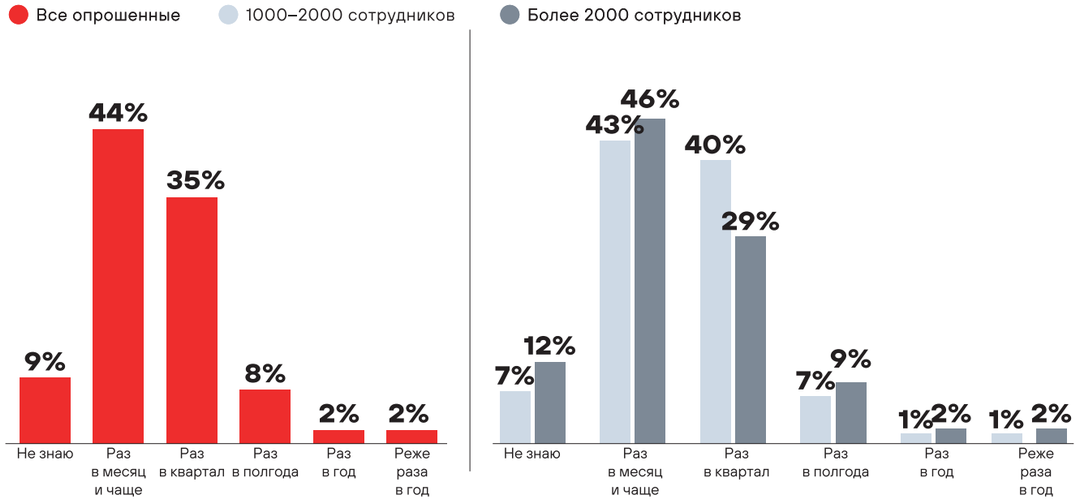


Рисунок 10. Как часто изменяется количество активов в вашей инфраструктуре

ПРОБЛЕМА № 2

Сложность инфраструктуры компаний непрерывно растет: постоянно меняется количество активов, увеличивается количество средств защиты — это требует постоянной проверки настроек и состояния СЗИ, источников событий и процессов ИБ (мониторинг, реагирование, харденинг, treat hunting и т. д.). Из-за динамичных изменений инфраструктуры компании не всегда точно знают о состоянии ИТ-активов и том, как настроена их безопасность, что создает дополнительные уязвимые места, которыми могут воспользоваться злоумышленники.

ОЦЕНКА ЗАЩИЩЕННОСТИ

Оценка защищенности инфраструктуры может выявить узкие места и неэффективные процессы, которые необходимо оптимизировать для улучшения киберустойчивости компании. Разнообразие методов анализа защищенности позволяет выбрать наиболее подходящие, в зависимости от ресурсов и уровня зрелости ИБ в компании. По данным исследования «Готовы ли российские компании противостоять кибератакам?» [10], наиболее объективную оценку уровня защищенности можно получить, если проводить анализ, действия которого имеют максимальное сходство с действиями реальных злоумышленников.

[10]

Регулярная оценка состояния безопасности

Более 90% компаний проводят оценку безопасности и защищенности, 61% из них делают это регулярно.

Рисунок 11. Проводите ли вы регулярную оценку состояния безопасности

Это связано с тем, что многим компаниям необходимо соблюдать требования регуляторов в области защиты информации, несоответствие которым может привести к серьезным штрафам. Кроме того, регулярная оценка инфраструктуры помогает выявлять и устранять слабые места, которые могут быть использованы для проникновения в систему и кражи данных, менять процессы, плейбуки и сценарии реагирования на угрозы, а также сфокусироваться на самых вероятных векторах атак.

Бюджет на тестирование безопасности

Компании, которые инвестируют не только в системы для информационной защиты, но и в их тестирование, имеют меньше шансов столкнуться с кибератаками, утечками данных и другими киберугрозами, что способствует стабильному и успешному развитию бизнеса.

В среднем на оценку защищенности тратится около 10–30% бюджета, в более крупных компаниях затраты несколько выше. Некоторые компании могут неправильно оценивать важность тестирования защищенности, не придавать ему значения и направлять основную часть бюджета на выстраивание процессов защиты инфраструктуры.

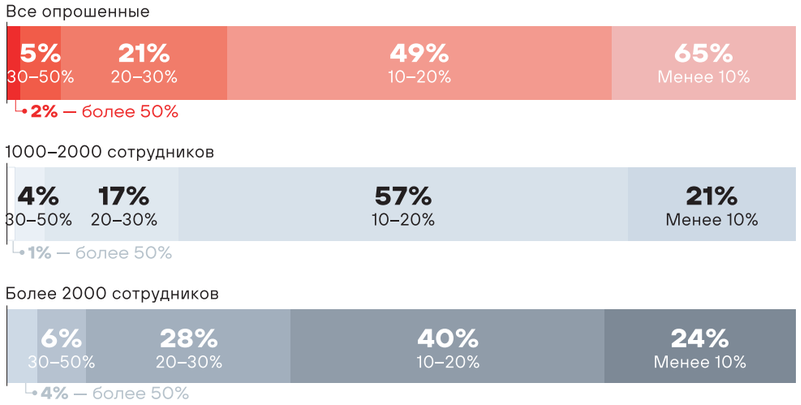


Рисунок 12. Какой процент бюджета на кибербезопасность выделен на тестирование защитных мер

Методы проверки безопасности

Мы опросили компании, которые регулярно тестируют защищенность, и выяснили, что самые популярные способы проверки — аудит безопасности и использование сканеров уязвимостей. Почти в два раза реже используются киберучения и специализированные программы. При этом ручной пентест заказывают только 21% компаний, хотя в мире наблюдается устойчивый рост интереса к подобным услугам.

Рисунок 13. Какие методы проверки безопасности используют компании

Результаты тестирования

Традиционно во многих отраслях проверка защищенности возникла как необходимость соответствовать требованиям регуляторов. Нет сомнений в том, что эти требования, даже если они навязаны регулирующими органами, по-прежнему в некоторой степени стимулируют компании проводить тестирование на безопасность.

Однако основной причиной для проверки защищенности является необходимость приоритизации закупок и выбора действительно нужных решений. Кроме того, немаловажным фактором называют демонстрацию результатов топ-менеджменту для информирования о рисках кибербезопасности как внутри компании, так и за ее пределами. Из опрошенных специалистов по ИБ 48% сообщили, что делятся результатами с высшим руководством, так как с увеличением числа громких нарушений приходит осознание важности кибербезопасности, понимание бизнес-рисков и возможного финансового ущерба от последствий атак. Экспертные знания в области ИБ становятся все более распространенными среди топ-менеджмента. Вполне вероятно, что управленцы все чаще будут запрашивать отчеты для оценки состояния безопасности, поэтому важно, чтобы эти отчеты были исчерпывающими и понятными. Результаты проверки также выходят за пределы организаций. В связи с ростом рисков от третьих лиц и возможности компрометации через цепочку поставок 20% опрошенных компаний делятся результатами со своими клиентами.

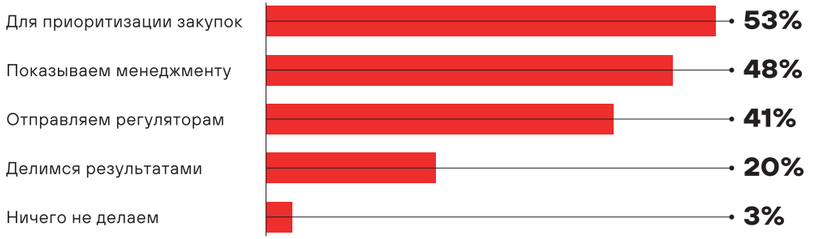


Рисунок 14. Как используются результаты тестирования

Частота заказа ручного пентеста

Среди всех опрошенных компаний 79% сообщают, что их инфраструктура меняется не реже одного раза в квартал (см. рис. 10), однако услуги по ручному тестированию на проникновение заказывают только 21% (см. рис. 13). Периодичность проведения регулярных пентестов очень важна, так как чем меньше интервал между проверками, тем более актуальную информацию о наличии уязвимостей и потенциальных действиях злоумышленника будет получать отдел ИБ. Каждый день хакеры совершенствуют тактики и техники атак, появляется информация о ранее неизвестных уязвимостях, динамично изменяется инфраструктура — все это значительно влияет на состояние защищенности. Для оперативного реагирования на угрозы необходимо регулярно проверять безопасность критически важных узлов и ключевых систем.

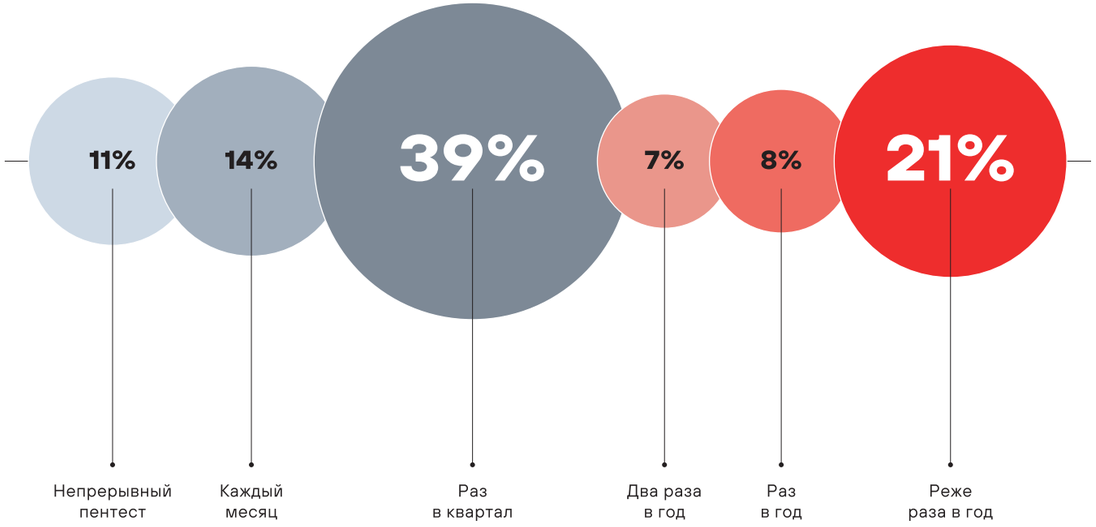


Рисунок 15. Как часто компании заказывают тестирование на проникновение

Частота проведения пентеста зависит от множества факторов, включая тип организации, характеристики информационной системы и изменение ландшафта угроз. Не всегда есть возможность проводить тестирование при внесении изменений в цифровые активы, например при внедрении новых технологий, обновлении ПО или изменении бизнес-процессов. Зачастую компании проводят пентест для соблюдения отраслевых стандартов и требований регуляторов. Например, согласно положению 683-П Центрального банка РФ [11], банки и НКО обязаны проводить тестирование на проникновение ежегодно.

По результатам исследования, только 11% компаний проводят непрерывный пентест, а 14% заказывают пентест ежемесячно. Проверяют защищенность тестированием на проникновение раз в квартал 39% компаний. Остальные заказывают такие услуги гораздо реже и делают это нерегулярно либо по запросу.

Причины заказа услуг ручного пентеста

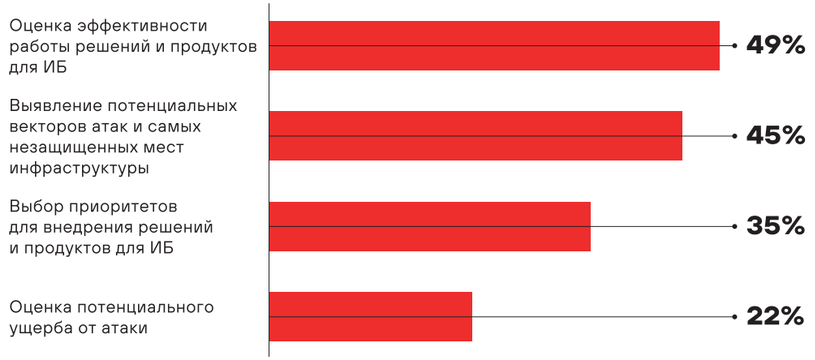


Рисунок 16. Причины заказа пентеста

Контроль и проверка кибербезопасности, а также оценка эффективности работы средств защиты информации — две основные мотивации для проведения тестирования на проникновение, кроме выполнения требований регуляторов.

Пентест также используется для оценки потенциального ущерба от атак и для выбора стратегии инвестирования в обеспечение безопасности. Это говорит о том, что компании начинают использовать пентест не только для выполнения требований регулирующих органов, но и для оценки реального состояния киберустойчивости инфраструктуры.

Барьеры для пентеста

Двумя главными препятствиями для заказа регулярного тестирования на проникновение являются отсутствие бюджета, а также угроза нарушения непрерывности бизнес-процессов. Прежде всего, перед службой ИБ стоит задача обеспечить безопасность ИТ-среды и бесперебойность бизнес-операций. Руководители ИТ и ИБ с осторожностью относятся к пентестам, поскольку многие сталкивались с простоями в работе. Это говорит о том, что компаниям необходимо работать только с самыми опытными командами, которые имеют хорошую репутацию и многолетний опыт работы по оказанию таких услуг и могут обеспечить высокий уровень проверки безопасности с минимальным риском для процессов. Немало компаний, особенно представители небольшого бизнеса, также озадачены необходимостью принятия мер по исправлению обнаруженных проблем безопасности.

Рисунок 17. Барьеры для заказа услуг ручного пентеста

Кто отвечает за проверку безопасности

Только в 10% крупных компаний есть своя команда пентестеров (red team). Примерно в половине опрошенных компаний есть специалисты, которые отвечают исключительно за организацию оценки безопасности, а у 41% опрошенных этой задачей занимаются специалисты со смежными обязанностями.

Очевидно, есть определенная нехватка квалифицированных кадров, которые отвечали бы за выстраивание процессов тестирования безопасности и были поглощены только этими задачами.

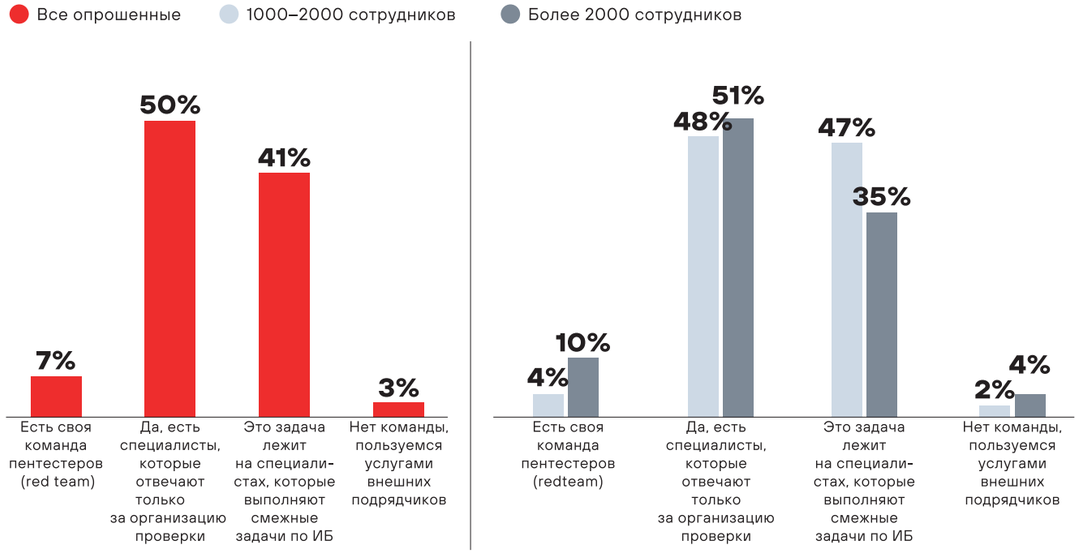


Рисунок 18. Есть ли внутри компании специалисты, отвечающие за проверку безопасности

ПРОБЛЕМА № 3

С одной стороны, компании хотели бы проверять киберустойчивость не только для выполнения требований регулятора, но и для понимания реальной ситуации с безопасностью в своих инфраструктурах. С другой — на рынке есть дефицит квалифицированных команд для проведения качественного пентеста, а внутри компаний недостаточно собственных ресурсов для выстраивания процесса тестирования. Кроме того, российские компании испытывают недостаток бюджета на проведение регулярных проверок и опасаются нарушения бизнес-процессов.

КАК ОБЕСПЕЧИТЬ РЕГУЛЯРНУЮ ПРОВЕРКУ БЕЗОПАСНОСТИ

Российские компании вынуждены работать в условиях изменений IT-инфраструктуры и постоянно меняющегося ландшафта киберугроз. Возможность проводить регулярный ручной пентест есть не у всех компаний, но есть потребность минимизировать риски безопасности, выявлять проблемы защиты и тщательно планировать закупки решений для ИБ с учетом возможностей и потребностей ИТ-инфраструктуры.

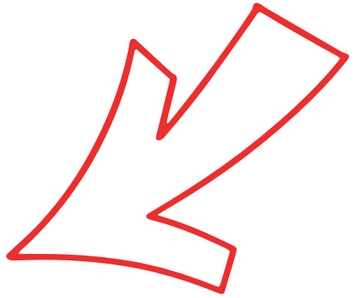
Обеспечить регулярное тестирование защищенности могут инструменты, которые проводят автоматические пентесты так, как это делают настоящие хакеры. Positive Technologies разработала продукт PT Dephaze, который позволит решить все проблемы, выявленные в ходе исследования. PT Dephaze [12] — система для безопасной симуляции атак, которая проверяет защищенность инфраструктуры через эмуляцию техник и тактик злоумышленников.

[12]

Продукт позволяет непрерывно проверять инфраструктуру любой сложности на наличие уязвимостей и потенциальной возможности для хакеров получить привилегированный доступ к системе. PT Dephaze подсветит небезопасные места информационной системы и поможет приоритизировать инвестиции в закупку средств защиты. Система расширяет область тестирования, не фокусируясь на каком-то отдельном сегменте, оптимизирует и масштабирует пентест в условиях, когда непрерывное ручное тестирование на проникновение невозможно.

МЫ ПРОВЕЛИ КОММЕРЧЕСКИЙ ЗАПУСК PT DEPHAZE 27 ФЕВРАЛЯ 2025 ГОДА И ПОКАЗАЛИ ЕГО В ДЕЙСТВИИ — ЗАПУСТИЛИ АВТОМАТИЧЕСКУЮ ПРОВЕРКУ В ПРЯМОМ ЭФИРЕ И РАССКАЗАЛИ, КАКОЙ ЭКСПЕРТИЗОЙ НАПОЛНЯЕМ ПРОДУКТ, ЧТОБЫ ОН НАХОДИЛ ВСЕ УЯЗВИМЫЕ МЕСТА В РАЗНЫХ ИНФРАСТРУКТУРАХ.

ДЛЯ ТОГО, ЧТОБЫ ПОСМОТРЕТЬ ЗАПИСЬ ИЛИ ОСТАВИТЬ ЗАЯВКУ НА «ПИЛОТ», ЗАРЕГИСТРИРУЙТЕСЬ НА НАШЕМ САЙТЕ 13.



13

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

Узнать больше
о PT Dephaze