Кибербезопасность как задача анализа и управления рисками сложных цифровых систем

Кибербезопасность перестала быть задачей установки защитных программ и охраны сетевого периметра. Она превращается в междисциплинарную науку об анализе сложных цифровых систем и управлении рисками в условиях неопределенности. Такой вывод следует из исследования Kept о развитии российского рынка кибербезопасности.

Раньше цифровую систему организации можно было представить как здание с охраняемым входом: контроль периметра считался достаточным для защиты внутренних ресурсов. Облачные сервисы, удаленный доступ, внешние приложения и подключаемые устройства разрушают такую границу. По оценке Kept, рост российских рынков инфраструктуры как услуги, IaaS, на 23–25% и платформы как услуги, PaaS, на 25–26% в год увеличивает число объектов, которые необходимо защищать.

Цифровая инфраструктура стала слишком распределенной и изменчивой, чтобы защищать ее вручную и только по периметру. Нужны непрерывный контроль активов, автоматическое выявление уязвимостей и анализ связанных событий. Системы управления внешней

поверхностью атаки, EASM, автоматически находят доступные из интернета ресурсы организации, проверяют их на уязвимости и помогают оценить пути проникновения.

Как формально описать «поверхность атаки», как измерять ее изменения и как предсказывать наиболее опасные изменения инфраструктуры? Ответы лежат в области математического моделирования, теории графов, оптимизации и анализа больших данных.

Второе изменение — переход от реакции на отдельные тревожные сигналы к анализу связанных событий. Системы расширенного обнаружения и реагирования, XDR, собирают сведения с рабочих станций, из сетевого трафика, электронной почты и облачной инфраструктуры, чтобы восстановить логику атаки: как злоумышленник попал в систему, какие ресурсы использовал и куда движется дальше. Такой подход опирается на распознавание закономерностей во временных рядах, теорию графов, сетевой анализ, статистическое моделирование и теорию принятия решений.

Масштаб проблемы подтверждают данные исследования: в 2025 году число подтвержденных киберинцидентов превысило 33 тыс., а среднее число атак на одну компанию выросло на 51%. Ручной анализ такого объема событий невозможен, поэтому возрастает роль алгоритмов, выделяющих значимые сигналы из потока данных.

Искусственный интеллект — одновременно инструмент защиты и новый объект риска. Он помогает выявлять аномалии, связывать события, ранжировать инциденты по риску и восстанавливать сценарии атак. В антифрод-системах модели отличают законные операции от мошеннических, а в системах разведки киберугроз, Threat Intelligence, помогают обрабатывать отчеты, технические индикаторы и сведения об инфраструктуре злоумышленников. Качество результата зависит от полноты и достоверности исходных данных.

ИИ создает и новые риски. Модели подвержены отравлению обучающих данных, утечкам данных через запросы к модели, подмене входных данных и использованию для автоматической генерации фишинговых сообщений или вредоносного кода. Отсюда вырастает направление безопасности систем искусственного интеллекта: защита моделей, проверка надежности их выводов, прозрачность решений и контроль последствий автоматических действий.

Разведка киберугроз показывает, что защита требует не только алгоритмов, но и аналитической работы. Системы Threat Intelligence превращают разрозненные данные в контекст, позволяющий понять, связано ли событие с известной кампанией или группировкой. Без проверки гипотез, приоритизации угроз и перевода выводов в конкретные меры поток данных сам по себе не снижает риск.

Сходная логика прослеживается в антифроде и защите от цифровых рисков: антифрод-системы анализируют поведение людей и транзакции, а решения класса защиты от цифровых рисков, DRP, отслеживают фишинговые сайты, утечки и незаконное использование брендов. Здесь соединяются поведенческая психология, лингвистика, экономика доверия, право и компьютерные науки.

Это открывает исследовательскую программу: моделирование поверхности атаки, анализ связанных инцидентов, оценка неопределенности, безопасность и интерпретируемость алгоритмов, взаимодействие человека и автоматических систем защиты. Кибербезопасность становится наукой о сложных адаптивных системах, где взаимодействуют программы, люди, организации, данные и алгоритмы.

Кадровый дефицит усиливает этот запрос: о нехватке специалистов сообщили 71% коммерческих и 78% государственных организаций. Будущие решения должны не заменять экспертизу, а перераспределять ее: алгоритмы берут на себя рутинный мониторинг и первичный анализ, человек — проверку гипотез, интерпретацию и действия в нестандартных ситуациях.

Прогноз Kept предполагает, что к 2031 году наиболее быстро будут развиваться XDR и EASM — направления, основанные на непрерывном сборе данных и автоматизированном контроле инфраструктуры. Их развитие зависит от способности создавать проверяемые модели сложных систем, надежные методы анализа данных и понятные критерии доверия к автоматическим выводам.

Полный текст Обзора российского рынка кибербезопасности и прогноз его развития: