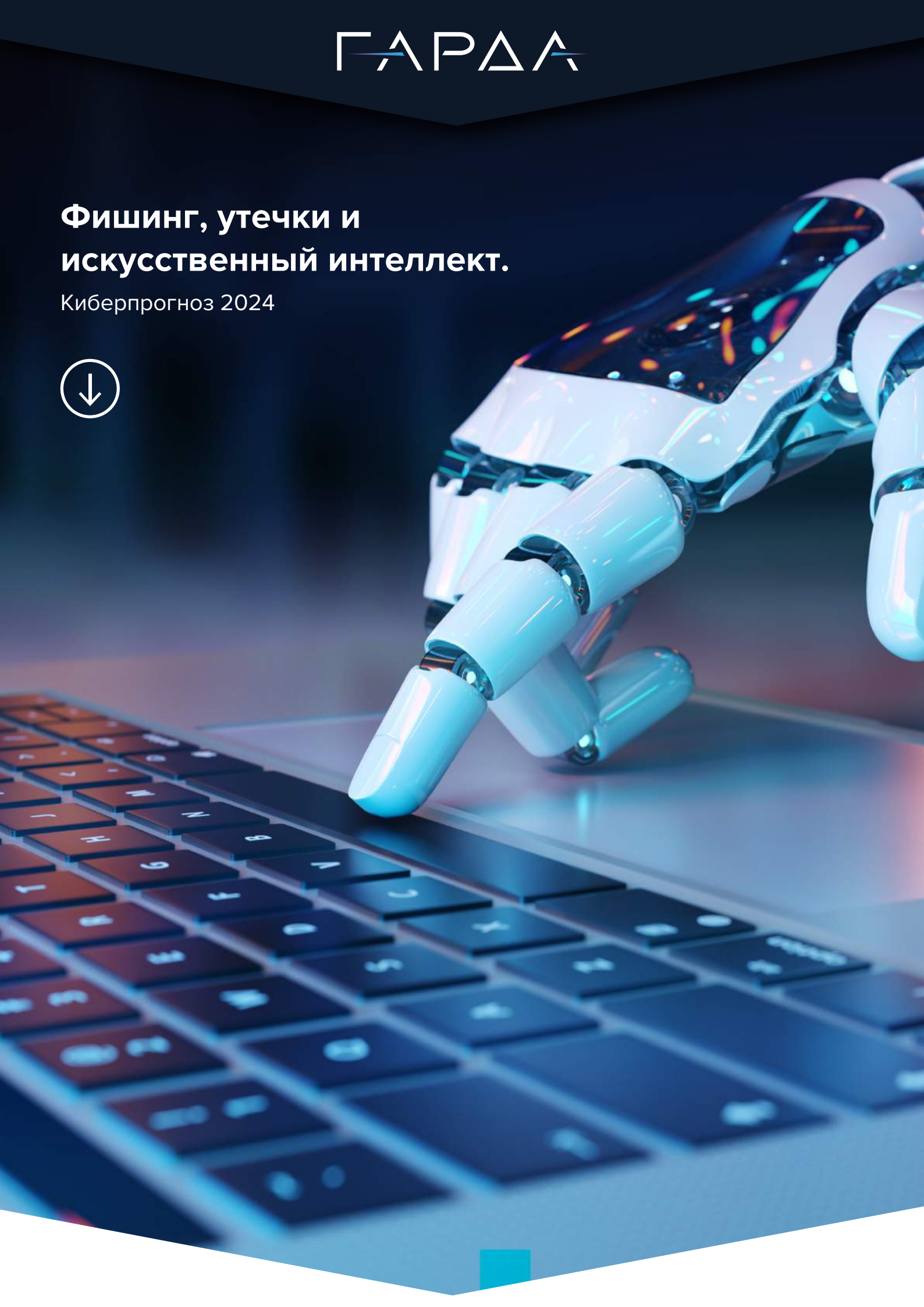
ГАРДА

Фишинг, утечки и искусственный интеллект.

Киберпрогноз 2024



Наступление нового года резонно заставляет задуматься о том, к чему готовиться бизнесу в части защиты информации. Опыт 2023 подтвердил необходимость фокусировки усилий производителей решений и провайдеров услуг кибербезопасности на защите данных ограниченного распространения, в том числе персональных. Обеспечить такую защиту возможно как с помощью специализированных продуктов, так и с помощью систем, покрывающих мониторингом и реагированием всю корпоративную сеть. Причём, в силу роста числа угроз для, в том числе, мобильных телефонов и иных устройств интернета вещей, наиболее эффективен мониторинг в первую очередь сетевого трафика, классический подход с анализом журналов при сравнении оказывается более реактивен.

К чему еще в области кибербезопасности в 2024 году готовиться бизнесу, рассказывает директор по стратегическим альянсам и взаимодействию с органами государственной власти группы компаний «Гарда» Павел Кузнецов.

01 Утечки данных

С учётом новой реальности стоит ожидать, к сожалению, роста, если не количества, то масштаба утечек данных. Поведение атакующих демонстрирует умение выжидать достаточно длительные сроки от получения первичного доступа в инфраструктуру до его реализации в виде конкретного ущерба атакованной организации. Необходимо помнить, что угроза может исходить как от внешних злоумышленников, так и от инсайдеров, которые могут быть мотивированы как чисто идеологически, так и финансово. При этом не стоит сбрасывать со счетов и классическую для злоумышленников схему, когда результаты нескольких старых утечек компилируются в большой массив, чтобы найти на него покупателя. В связи с этим реагировать на новости об утечках следует, предварительно критически оценив поступившую информацию.

Большинство именно новых атак, направленных на организацию утечек данных, при этом скорее будут нацелены на крупные компании и правительственные учреждения, в том числе потому, что атакующие преследуют цель нанесения репутационного ущерба всему государству, чего достичь при взломе небольшой организации проблематично.

02 Угрозы мира BYOD

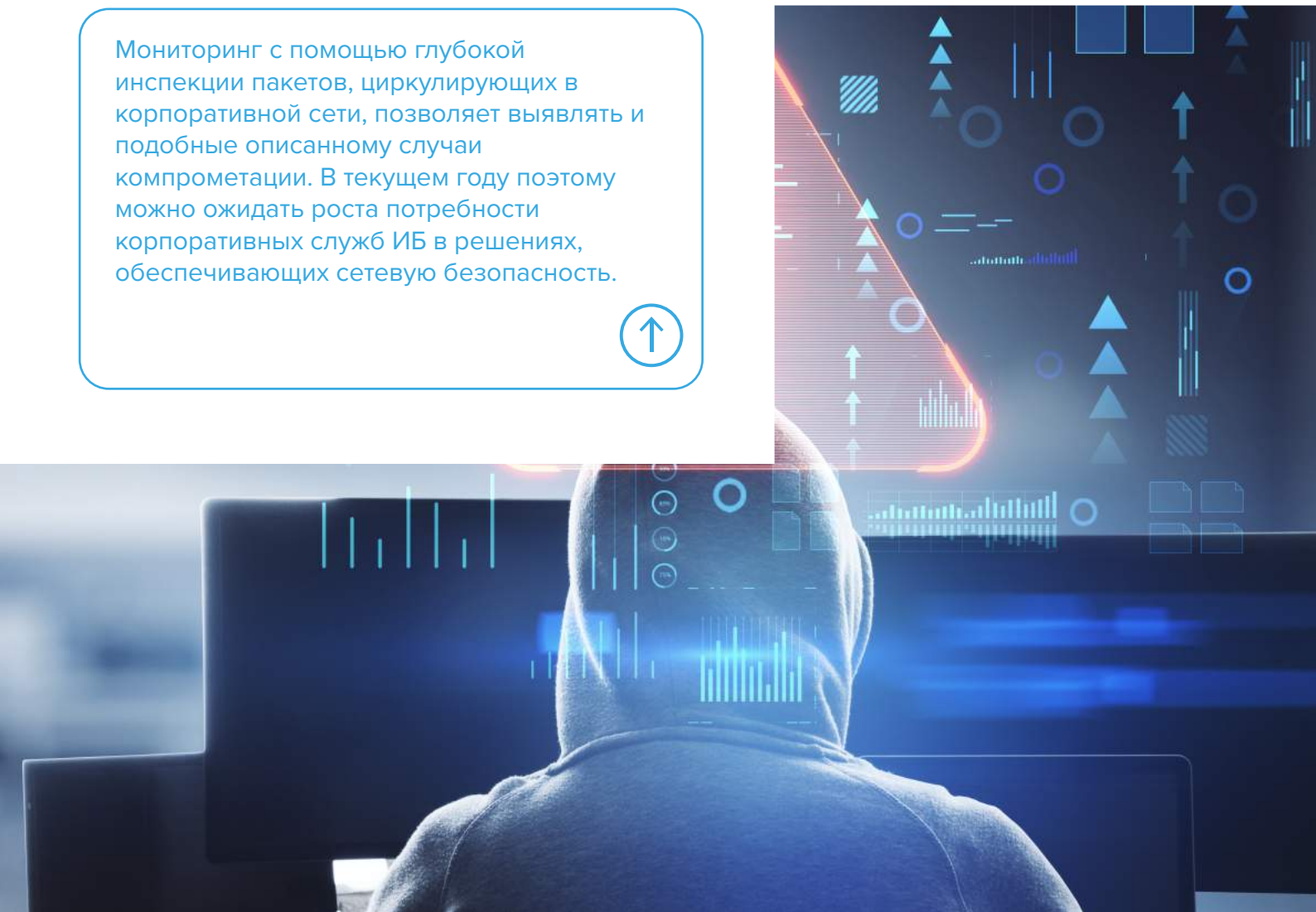
Предыдущий год ознаменовало появление IN-THE-WILD* образцов вредоносного программного обеспечения, эксплуатирующего крайне «тонкие» уязвимости глубоко в системном программном обеспечении мобильных устройств производства компании APPLE. Соответствующее предупреждение было выпущено и Федеральной службой безопасности Российской Федерации. При этом уязвимости имели характер, дающий возможность атаковать мобильное устройство без участия пользователя, скрытно от него. Учитывая закрытый характер операционной системы мобильных устройств, подверженных атаке, и трудность установки на них средств контроля, либо подключения журналов безопасности этих устройств к системам мониторинга и управления инцидентами, стал как никогда актуален вопрос непрерывного анализа сетевого трафика в организациях.

* ITW (IN-THE-WILD, от англ. дословно – в дикой среде) — употребляется в случаях, когда вредоносное ПО выявлено в реальных атаках и инцидентах, в отличие от, к примеру, эксплоитов, созданных в исследовательских целях и хранящихся в лабораторных условиях

ГАРДА

Фишинг, утечки и искусственный интеллект

Мониторинг с помощью глубокой инспекции пакетов, циркулирующих в корпоративной сети, позволяет выявлять и подобные описанному случаи компрометации. В текущем году поэтому можно ожидать роста потребности корпоративных служб ИБ в решениях, обеспечивающих сетевую безопасность.



03

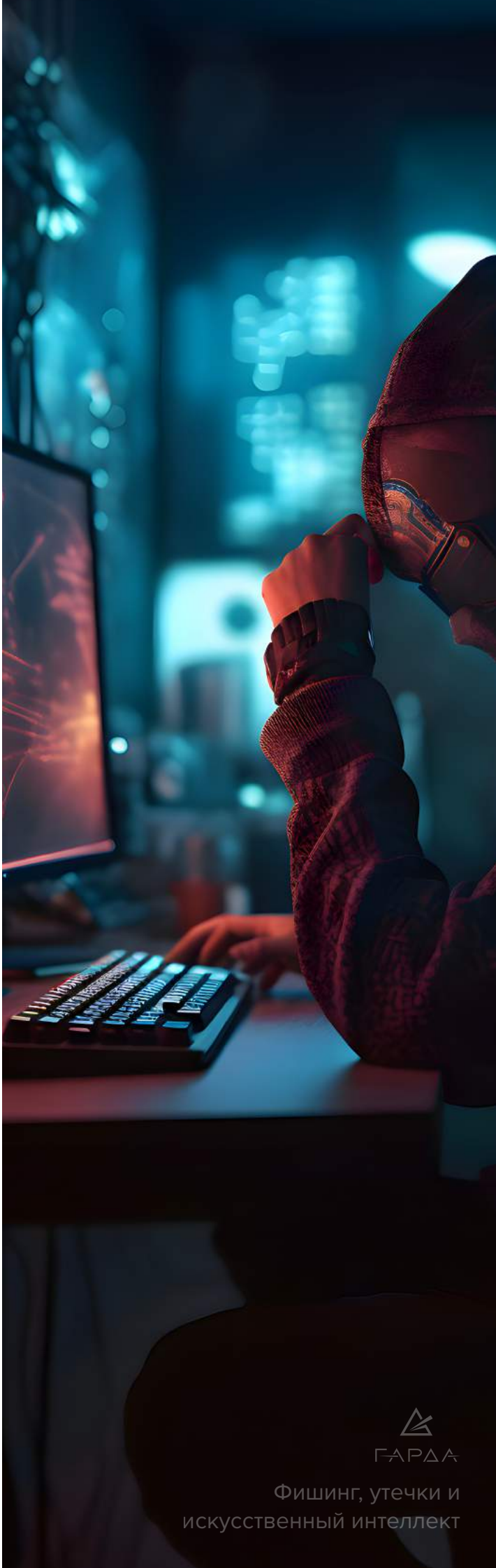
Киберпреступность как бизнес

В 2023 году сохранился тренд роста услуг «теневого рынка» киберпреступности. В наступившем 2024 этот тренд скорее продолжит свой рост. В условиях всплеска политически-мотивированного «хактивизма» и на фоне недостаточной квалификации основной массы подобных акторов актуальны становятся различные вредоносные сервисы.

Популярной, вероятно, будет схема организации кибератак, когда «хактивисты» коллективно определяют поверхность атаки, то есть перечень целей, а затем, посредством каналов «тёмного» интернета обращаются к услугам «профессионалов». Такими сервисами могут быть как организация DDoS-атак, так и продажа, к примеру, RANSOMWARE-AS-A-SERVICE*.

Более сложные инструменты в рамках массовых кампаний используются куда реже, в то время как «классические» попытки выведения сервисов из строя путём переполнения каналов связи «мусорными» пакетами и шифрование информации в целях как нарушения работы организаций, так и извлечения последующей финансовой выгоды, сохранят и преумножат свою популярность.

* RaaS (RANSOMWARE-AS-A-SERVICE, от англ. – программы-вымогатели как услуга) — бизнес-модель, по которой разработчики вредоносного ПО предоставляют по подписке программы-вымогатели и инфраструктуру для управления ими.

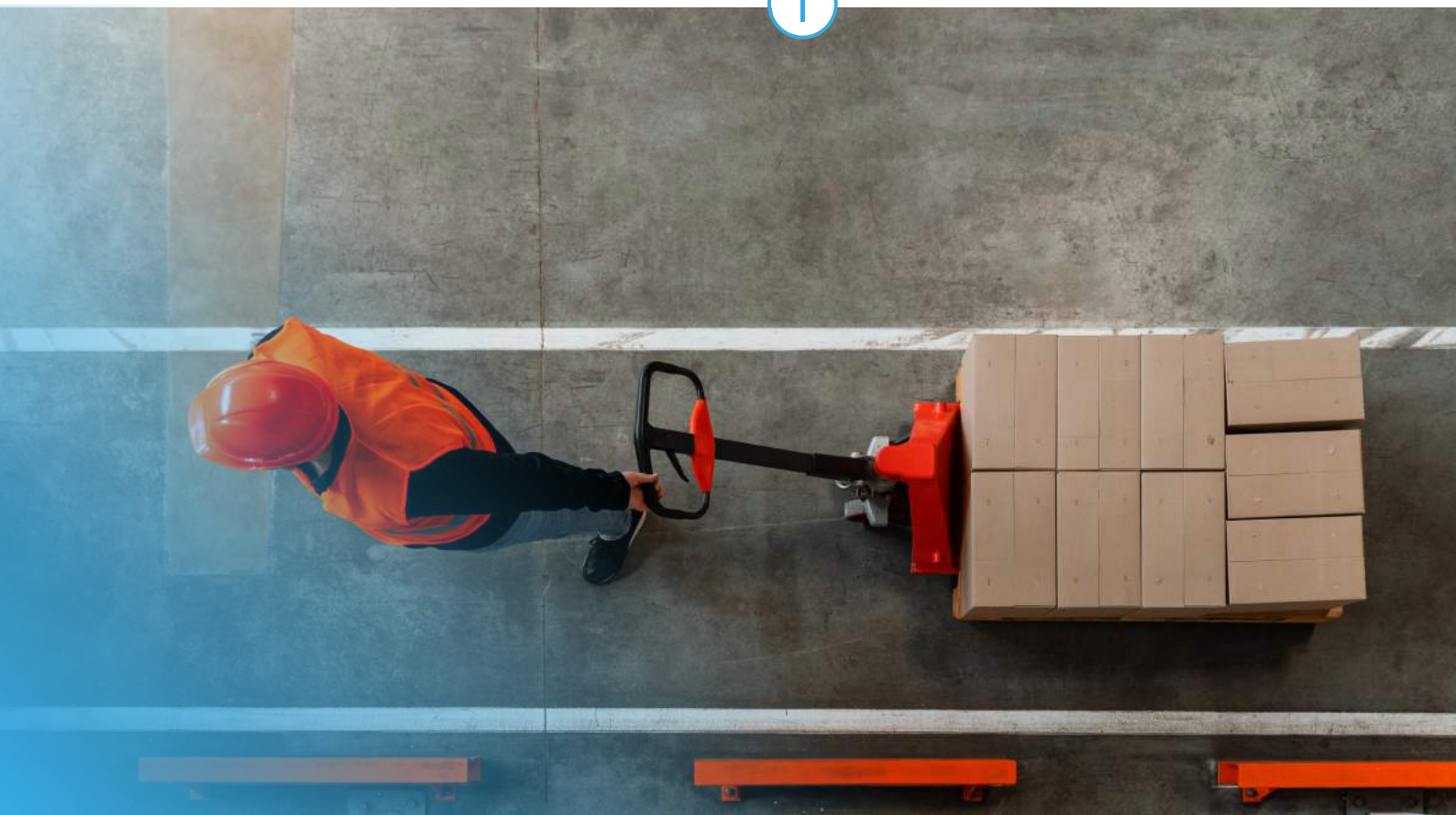


04 Импортозамещение

По результатам исследования, проведённого группой компаний «Гарда» в конце прошедшего года, рынок решений сегмента сетевой безопасности в России остаётся, по мнению респондентов, в известной степени импортозависимым. При этом, сравнимыми с иностранными по набору функций и качеству отечественные решения в сегменте многофункциональных межсетевых экранов (Next Generation Firewall, NGFW) назвали 44% опрошенных. В 2024 году, судя по декларируемым планам производителей, ситуация должна измениться в лучшую сторону. Традиционно сильные математическая и инженерная школы подготовки специалистов позволяют компаниям-производителям двигаться к реализации запланированного набора функций уверенными темпами.

Классификатор (собственной разработки) разбираемых решением Гарда NGFW протоколов, к примеру, позволяет разбирать содержимое проходящего трафика для более чем 100 различных сервисов и приложений, предоставляя гибкие инструменты обновления правил. Движение к достижению технологической независимости иных производителей также носит поступательный характер. В прочих сегментах с ещё более высоким уровнем зрелости, таких как NTA/NDR решения и решения по защите конечных точек, ситуация выглядит даже лучше.

Поэтому, несмотря на необходимость сохранения тонуса у производителей, к концу года стоит ожидать наличия на рынке набора продуктов, позволяющих обеспечить уровень киберзащищённости как минимум не ниже, чем до принятия отдельными зарубежными производителями решения об уходе с российского рынка.



05 Угрозы со стороны искусственного интеллекта

Технологии генеративных моделей искусственного интеллекта (ИИ) становятся все более распространёнными, отдельные производители защитных решений даже внедряют их в собственные разработки. Однако, повсеместный рост популярности ИИ также создаёт и новые угрозы для информационной и кибербезопасности. Компрометация публичных систем ИИ может создавать угрозы манипуляции общественным сознанием и позволять атакующим опосредованно массово атаковать граждан. Как правило, целью таких атак является создание информационно-психологических предпосылок для роста тревожности и неуверенности в завтрашнем дне, а также продвижения повестки дня в собственных интересах. А бесконтрольное внедрение генеративных моделей зарубежной разработки в отечественные решения создаёт предпосылки для их последующей компрометации либо вывода из строя по причине деятельного разрыва отношений компаний-разработчиков моделей с подсанкционными странами.

В части именно кибербезопасности уже отмечались в прошлом году и будут продолжаться с большей частотой случаи использования генеративных моделей ИИ в фишинговых кампаниях. Выражаться это будет как в генерации с помощью ИИ заинтересовывающих жертв текстов, так и для создания DEEPFAKE аудио- и видеоматериалов, позволяющих атакующим действовать от имени лиц, которым жертва доверяет. Также злоумышленники, вероятно, будут продолжать пытаться использовать ИИ в целях обфускации кода вредоносного программного обеспечения и изменения кода таким образом, чтобы избежать обнаружения новых экземпляров средствами защиты информации.

Заключение

Не стоит ждать от 2024 года появления каких-либо «прорывных» с точки зрения технологического стека новых угроз кибербезопасности, однако снижать бдительность точно не следует. Интенсивность давления на отечественную информационную инфраструктуру сохраняется, а спорадический характер мировых событий последнего времени подсказывает, что новый год может как минимум принести с собой достаточно инфоповодов, которыми злоумышленники могут воспользоваться в рамках подготовки и реализации массированных фишинговых атак. Подобными инфоповодами, к примеру, практически наверняка станут все крупные политические и экономические мероприятия года, такие как основные международные форумы. Поэтому к проведению подобных мероприятий следует подходить ответственно и подготавливать информационную инфраструктуру в соответствии с концепцией SECURE-BY-DESIGN*, то есть строить архитектуру обеспечения кибербезопасности уже встроенной в общую архитектуру ИТ-сервисов.

> * SECURE-BY-DESIGN (от англ. конструктивно безопасный) - это подход к разработке, который придерживается принципов безопасности на всех этапах производства и жизненного цикла продукта: от проектирования до обновлений.

Справка

Гарда (входит в ИКС Холдинг) – производитель семейства продуктов для защиты данных и сетевой безопасности. Решения «Гарда» применяют в крупнейших государственных организациях и корпорациях, используют для защиты 50% всего российского интернета от DDoS-атак и безопасности цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель группы компаний построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

Юлия Чурикова
PR-служба «Гарда»
Моб.: +7-926-371-36-50
e-mail: j.churikova@gardatech.ru