ZEBRA

Платформа безопасности Zebra

Надёжная защита вашей организации

Стремительное распространение подключаемых устройств способствует развитию вашего бизнеса, но также приводит к возникновению потенциальных рисков нарушения безопасности. Использование межсетевых экранов – это не универсальное решение безопасности, но лишь начальный этап на пути обеспечения защиты перед лицом постоянно возрастающих и меняющихся угроз. Мы предлагаем вам ознакомиться с передовыми практиками и промышленными решениями, которые способны повысить защиту вашей организации и данных.

Как предотвратить угрозы безопасности, которые способны нарушить работу вашего предприятия

Безопасность – это действительно важно

Номера кредитных карт. Медицинские карты. Номера социального страхования. Пароли. Ваша организация предоставляет услуги клиентам, пациентам или гражданам? Вам необходимо, а иногда вы просто обязаны обеспечить конфиденциальность персональной информации людей.

Риски будут возрастать

Со временем обеспечение безопасности будет только усложняться. Например, интернет вещей и облачные технологии обеспечивают, как никогда прежде, взаимодействие людей и информации, предоставляя вашей организации невероятные возможности для контроля и прозрачности информации. Такие перспективы выглядят воодушевляющими, однако они таят в себе риски.

По прогнозам к 2022 году в мире будут использоваться 50 миллиардов[1] взаимодействующих устройств. Они смогут привести к бесчисленному количеству случаев уязвимости данных организаций и конфиденциальной информации. Возможности получения огромных материальных выгод и низкая вероятность ответственности за содеянное (уголовному преследованию были подвержены лишь пять процентов хакеров[2]) никак не способствуют снижению активности киберпреступников.

Какова цена бездействия?

Один несанкционированный доступ к системе может повлечь очень серьёзные последствия. Это крайне негативно скажется на уровне производительности и приведёт к финансовым потерям, а также может угрожать репутации вашей организации.

Что же можно сделать? К вопросам обеспечения безопасности необходимо относиться серьёзно. Даже если в вашей организации реализуется программа по обеспечению безопасности, существуют риски ошибочного восприятия безопасности, которые подрывают целостность защиты и приводят к возникновению нежелательных уязвимостей в защите систем.

3,9 миллиона долл. США
Средняя стоимость нарушения безопасности данных.[3]

25575 записей
Средний размер утечки данных в результате нарушения безопасности.[3]

12 часов
Среднее время, которое требуется 88% хакеров для проникновения в систему, минуя средства защиты.[4]

197 дней
Среднее время, в течение которого организации могут обнаружить проникновение в систему хакеров.[3]

Цели

Розничная торговля
80% информации, включающей данные и пароли пользователей интернет-магазинов, становится доступной хакерам, использующим украденные данные.[5]

Государственные учреждения и организации
Главные мотивы: шпионаж и получение финансовых выгод.[6]

Медицинское обслуживание
Вторая по важности для хакеров сфера деятельности, на которую приходится 15% кибератак.[6]

Производство
За последние несколько лет эта отрасль испытала самое большое количество взломов сетей с целью шпионажа данных.[6]

Ошибочное восприятие безопасности не должно позволить ослабить защиту вашей организации

Несмотря на массу публикаций о случаях нарушения безопасности многие организации по-прежнему не уделяют должного внимания своей защите. Не стоит успокаивать себя ложным ощущением защищённости. Если вы можете причислить себя к тем, кто делает нижеописанные утверждения, вы не защищены от угроз.

«Моя организация не такая большая, чтобы стать объектом кибератаки».

43% кибератак нацелены на малые предприятия.[6] Хакеры пользуются тем, что у малого бизнеса нет достаточных ресурсов и знаний в этой области. Они даже могут использовать вашу организацию для доступа к вашим связям с более крупными организациями.

«Наша сеть достаточно защищена».

Надёжная защита представлена многоуровневой системой, которая постоянно развивается. Вы закрыли входную дверь? Однако недоброжелатель сможет проникнуть в ваш дом через открытое окно. Результаты одного из исследований показали, что традиционные меры, такие как межсетевой экран и антивирусная защита, практически никогда не могли остановить хакеров. Действительно с задачей справляются лишь эффективные технологии, обеспечивающие безопасность оконечных устройств.[4]

«У нас не было нарушений безопасности, поэтому наша система защиты работает замечательно».

Вы можете даже не осознавать, что взлом вашей системы безопасности уже имел место. Исследование показывает, что компании может потребоваться 197 дней, чтобы просто обнаружить взлом системы безопасности.[3]

«У нас уже имеется соответствующая требованиям программа обеспечения безопасности».

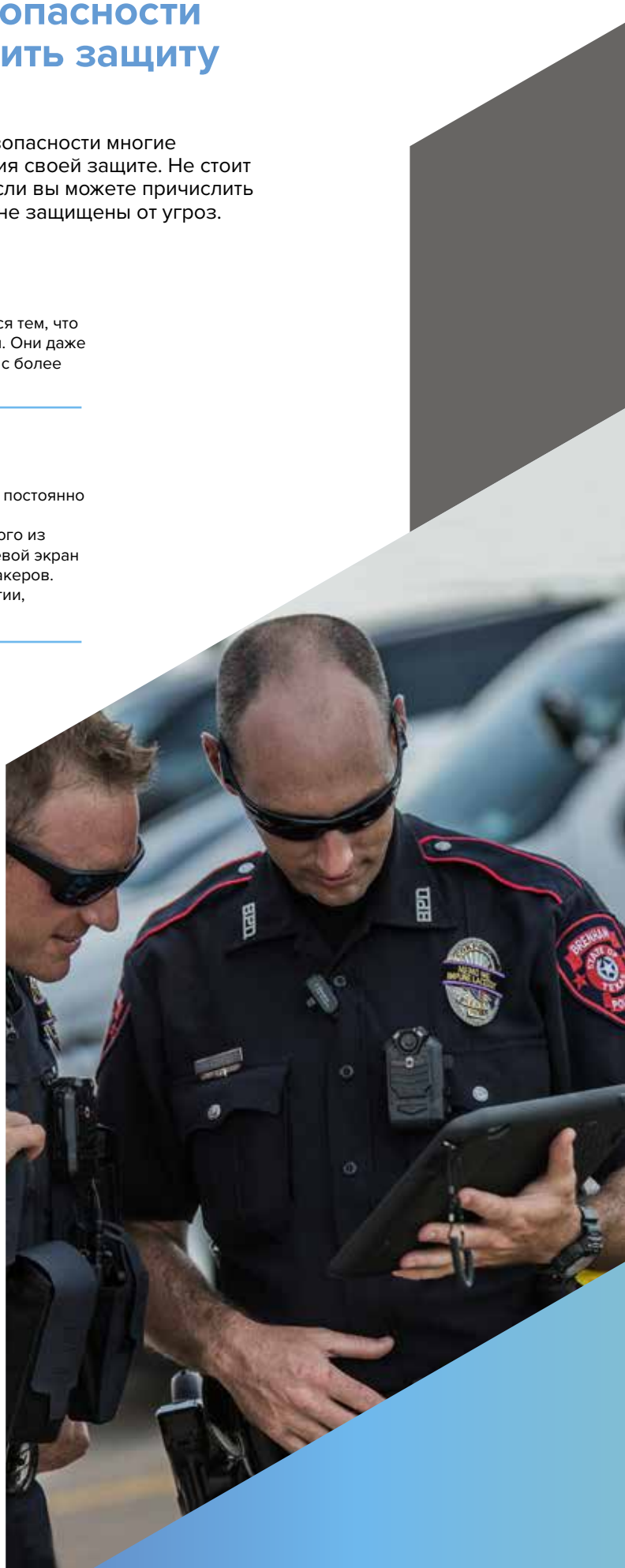
Замечательно. Ваша система безопасности постоянно совершенствуется с учётом возрастающих угроз? Она охватывает все технологические решения? Подход «однажды сделали и забыли» не обеспечит защиту от современных изощрённых киберпреступников.

«Технологии безопасности слишком сложны для нас».

Технологии безопасности хорошо продуманы, они интуитивно понятны в использовании и просты в реализации. Современные решения безопасности удобны для ваших пользователей и просты в управлении для ваших ИТ-специалистов.

«Безопасность негативно сказывается на производительности».

Существуют общие для многих опасения: системы безопасности считаются слишком сложными, их трудно интегрировать или они приводят к замедлению рабочих процессов. Однако атака недоброжелателей может вовсе привести к остановке работы предприятия. Каков же выход? Необходимо использовать технологии с уже встроенными средствами защиты. Именно тогда решения безопасности будут оказывать помощь, а не снижать производительность.



Защита вашей организации при помощи многоуровневой системы безопасности

Не все средства защиты могут соответствовать вашим нуждам. При выборе технологии обратите внимание на наиболее важные характеристики средств защиты, которые вам может предложить Zebra Technologies.

Встроенные средства защиты и обеспечения производительности

Выбирайте такого поставщика, который сразу интегрирует в свою продукцию средства защиты и обеспечения производительности. Вы обнаружите, что наши решения включают всё, что необходимо для повышения производительности, при этом одновременно они предлагают высокоэффективные протоколы и средства защиты.

Автоматизированные средства защиты

Если прежде вашим ИТ-специалистам приходилось тратить недели на обеспечение сертификации Wi-Fi®, теперь эти процессы осуществляются автоматически, обеспечивая вам и вашим сотрудникам надёжно защищенное сетевое подключение.

Адаптация в соответствии с вашими требованиями

Вы хотите задать особые пороговые значения для ваших систем безопасности? Решения Zebra упрощают эту задачу: вы можете задать требуемую конфигурацию с учётом особых уровней защиты, что будет соответствовать нуждам вашей компании или департаментов.

Простое управление и обслуживание

Вы можете быть уверены в том, что наши инструменты, программы и оборудование безопасности были разработаны и прошли испытания с целью обеспечения минимального обслуживания и максимального времени безотказной работы. Более того, наша служба поддержки работает 24 часа в сутки и готова оказать вам требуемую помощь.

Простая интеграция

Продукция Zebra обеспечивает лёгкий и надёжный процесс интеграции. Мы располагаем всесторонними знаниями о нуждах вашей отрасли и видах применения продукции, поэтому мы разработали наши решения с учётом ваших требований и обеспечили вам удобную интеграцию.

Постоянный контроль защиты и поддержка

Мы предоставляем обновления ОС и встроенного ПО в течение многих лет использования устройств, а также предлагаем услуги поиска и устранения неисправностей, оценку уязвимостей и сотрудничество со специалистами по безопасности наших клиентов.

Использование мирового опыта

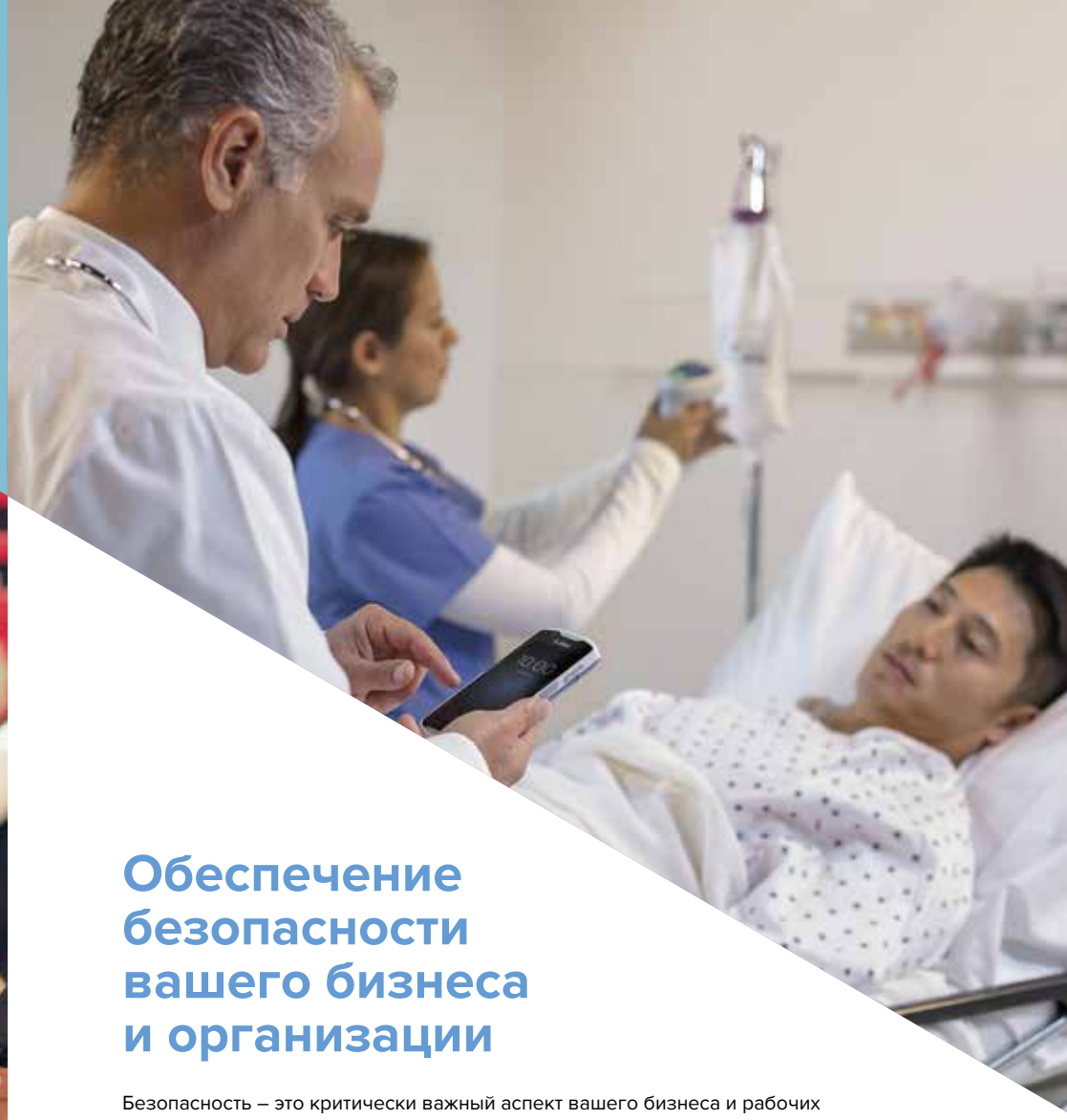
Вы можете быть уверены в вашей безопасности, потому что Zebra руководствуется признанными в мире практиками и методами. Мы сотрудничаем с ISO, Национальным институтом стандартов и технологий (NIST) и Центром интернет-безопасности (CIS). Наши продукты и решения используются организациями, которые обязаны выполнять требования законов и стандартов HIPAA, PCI-DSS и GDPR.

Лидер в сфере технологий безопасности для предприятий

Мы смогли усилить защиту операционной системы Google Android™ и сделать её платформой корпоративного класса, для которой доступны обновления защиты на период до десяти лет. Высокая производительность и защищённость лежат в основе всей нашей продукции, включая наши мобильные компьютеры корпоративного класса, надёжные принтеры и передовые технологии.

Продукты, решения и услуги Zebra
Реализация каждого этапа стратегии кибербезопасности NIST

ИДЕНТИФИКАЦИЯ	Мониторинг управления рисками Программа-мастер для оценки защищённости принтеров Профессиональные услуги	Управление рисками в системах поставок Комитет по безопасности
ЗАЩИТА	LifeGuard™ for Android Защищённый режим работы принтера Управление устройствами	Обновления PrintSecure Управление автоматической сертификацией Wi-Fi Стратегия управления рисками
ОБНАРУЖЕНИЕ	Printer Profile Manager Enterprise Мониторинг средств безопасности	Обнаружение в режиме реального времени
РЕАГИРОВАНИЕ	Управление устройствами Меры противодействия обнаруженным угрозам	Реагирование на событие Оповещение клиентов
ВОССТАНОВЛЕНИЕ	Профессиональные услуги Меры по оптимизации	Восстановление до уровня штатного состояния



Обеспечение безопасности вашего бизнеса и организации

Безопасность – это критически важный аспект вашего бизнеса и рабочих процессов. Поэтому Zebra в упреждающем режиме отслеживает уязвимости безопасности и встраивает в свои решения многоуровневые средства защиты. Устройства, технологии и услуги Zebra созданы с учётом требований безопасности, не нарушая производительность ваших рабочих процессов. Вы обнаружите, что наши инструменты защиты просты в интеграции и удобны для ваших сотрудников. Наши передовые технологии предусматривают возможности настройки требуемой конфигурации и обеспечивают надёжную защиту в реальном времени в условиях реального применения. С продукцией и услугами Zebra вы сможете уверенно выполнять поставленные бизнес-задачи и выстраивать необходимые вам стратегии для внедрения технологий.

ZEBRA

Вы можете узнать, как наши стандарты безопасности способны обеспечить вам оптимальную защиту

Узнайте подробнее на веб-сайте **www.zebra.com/product-security**

Источники:

1. Juniper Research, 2018 г. **2.** «Отчёт о реагировании на угрозы», Carbon Black, ноябрь 2018 г. **3.** «Стоимость нарушения безопасности данных», исследование Ponemon Institute, 2018/2019 г. **4.** «Black Report», исследование Nuix, 2017 г. **5.** Отчет «Credential Spill Report», Shape Security, 2018 г. **6.** «Расследование нарушений безопасности данных», Verizon, 2019 г.