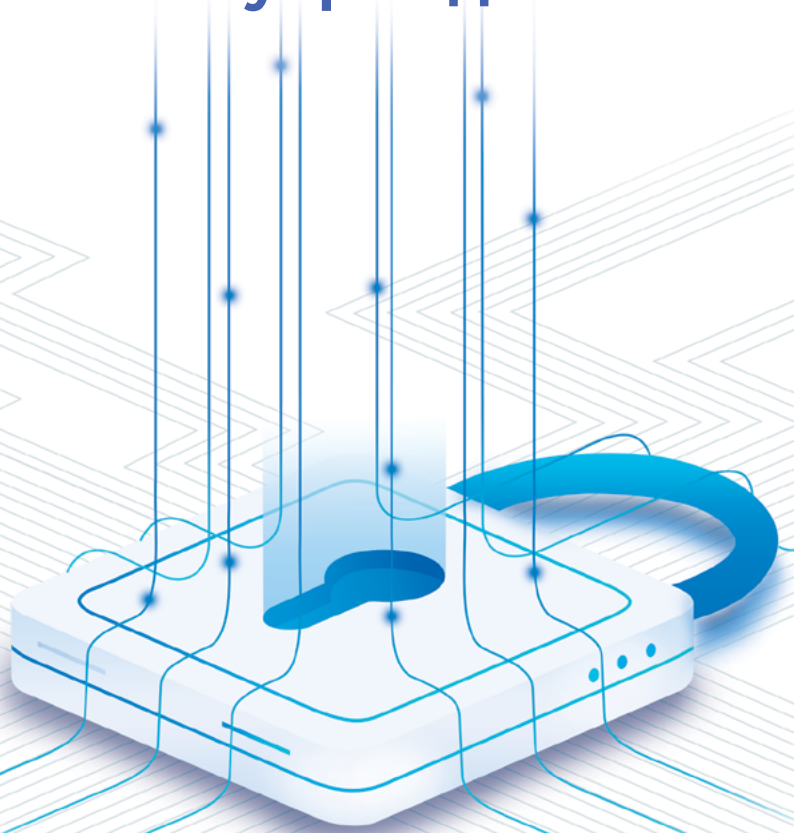
TRAFFIC INSPECTOR NEXT GENERATION®

Платформа цифрового благополучия

Информационная безопасность для государственных структур, образовательных и медицинских учреждений



В госорганах необходимо повысить защищенность информационных систем и сетей связи. Проведенные в 2021 году проверки показали, что большинство действующих там ресурсов уязвимы для массированных атак, для деструктивного внешнего воздействия, тем более при использовании зарубежных технологий последнего поколения. Нужно укреплять оборону отечественного цифрового пространства — здесь не должно быть слабых мест. Для этого будет создана госсистема защиты информации.

Чтобы эти системы работали бесперебойно и были защищены от любого потенциального негативного воздействия извне, страна должна перейти на отечественную технику, технологии, программы и продукты. Нужно разработать и внедрить для этого свое технологическое оборудование, в том числе необходимое для производства программно-аппаратных комплексов.

из выступления Президента РФ В.В. Путина
на заседании Совета безопасности России, 20.05.2022

Ситуация на рынке

более 170

зарубежных IT-компаний заявили о полном уходе с отечественного рынка и прекращении поставок и техподдержки после 24 февраля 2022 года.

50

IT-компаний сообщили об ограничениях в работе с российскими пользователями. В их числе Microsoft, HP, Dell, Cisco, SAP, Poly, Avaya, Oracle, IBM, TSMC, Nokia и Ericsson, Samsung, Apple.

Два фактора, которые трансформировали ИТ-отрасль РФ:

1. Западное оборудование и программное обеспечение, которое покупали отечественные компании, превратилось в кирпич. В сегменте кибербезопаности это гораздо более чувствительно, чем в IT-инфраструктуре или бизнес-приложениях.
2. Взрывной рост атак и инцидентов, связанных с кибербезопасностью. Весной 2022 года количество кибератак на инфраструктуру российских компаний увеличилось в 80 раз по сравнению с тем же периодом 2021 года.

Другие составляющие актуального ИТ-ландшафта:

- Прекратились поставки запасных частей для иностранного оборудования, купить их официально невозможно.
- Обновления для встроенного ПО и исправления уязвимостей недоступны российским компаниям, продлить подписки невозможно.
- Компании вынуждены срочно переходить на отечественные продукты или адаптироваться к работе в новых условиях.
- Появились сложности с использованием имеющегося парка защитных решений, возникла острая потребность в сохранении работоспособности.
- Сокращены сроки массового перехода на отечественное ПО.

Цена компрометации систем становится выше, а самое главное, ощутимее в реальном мире. Еще десять лет назад трудно было представить, что из-за кибератаки может быть остановлена работа сети АЗС, больницы или касс в магазине. Сейчас такой риск осознают все организации и по мере сил превентивно внедряют средства обнаружения и отражения атак.

> Иностранные вендоры, покинув рынок России и без предупреждения отрезав доступ к своим сервисам, дискредитировали себя в глазах российских пользователей. Даже если западные вендоры вернутся на российский рынок, они уже не смогут вернуть доверие клиентов. Если компания хлопает дверью и говорит, что больше не будет поддерживать продукты или, что еще хуже, отзывает оплаченные лицензии, то это крайне некорректно. Западные игроки бросили добросовестных заказчиков в один из самых непростых моментов. И заказчики этого не забудут.
>
> Председатель совета директоров
> «СерчИнформ» Лев Матвеев

Статистика по оборудованию и ПО

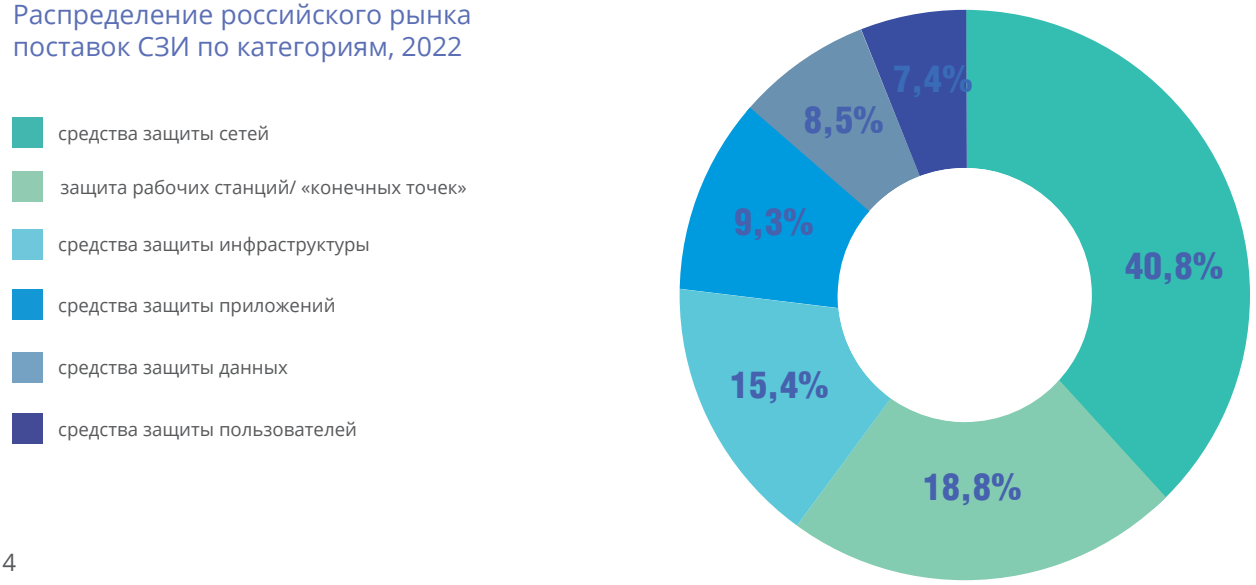
Объем рынка информационной безопасности в России (за исключением сегмента B2C)

По данным исследования Фонда «Центр стратегических разработок», объем рынка информационной безопасности России по итогам 2022 года составил 193,3 млрд руб. На услуги пришлось 26%, а на поставки СЗИ – 74% рынка — 142,5 млрд руб.

Совокупная доля услуг и поставок средств защиты информации по результатам 2022 года

Самым крупным сегментом рынка стала сетевая безопасность. На него приходится 58 млрд руб. — 40,8% от всего объема поставок СЗИ в России.

Распределение российского рынка поставок СЗИ по категориям, 2022



Доля российских вендоров на рынке

Российские вендоры в 2022 году поставили 70% всех СЗИ.

Доля российских и зарубежных вендоров средств защиты по результатам 2022 года

Российские вендоры

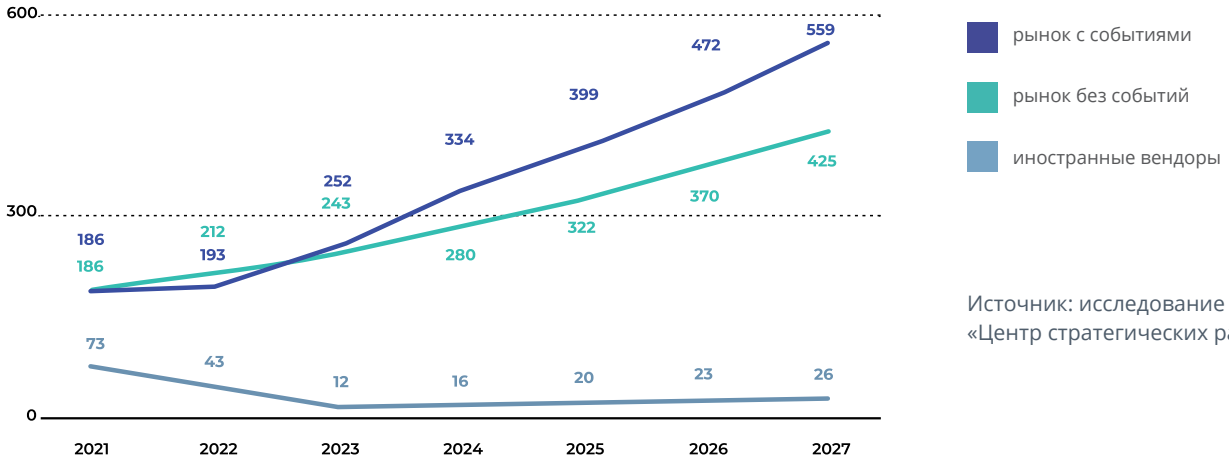
Зарубежные вендоры

Стремительный уход зарубежных вендоров в 2022 году не привел к ожидаемому сокращению общего объема рынка — отечественные компании смогли оперативно заместить большинство решений, также были реализованы схемы параллельного импорта. Падение выручки зарубежных вендоров в 2022 году составило более 70%, по итогам года их доля на рынке сократилась до 30%.

Российские вендоры имеют солидный портфель продуктов и сервисов и быстро занимают освободившийся рынок. Основная часть освобождаемой доли рынка (порядка 60 млрд руб.) будет освоена в течение ближайших 2 лет на существующих наработках и решениях. Разработка недостающих решений может занять до 5 лет.

Прогноз темпов роста российского рынка кибербезопасности защиты сетей

Прогноз развития рынка кибербезопасности России, млрд руб.



Источник: исследование Фонда «Центр стратегических разработок»

Российский рынок кибербезопасности продолжает расти. Ожидаемый спад 2022 года фактически был достаточно мягким и не привел к падению объемов рынка относительно 2021 года. Совокупный среднегодовой темп роста объема рынка за период 2022–2027 года ожидается в районе 24%, к 2027 году объем рынка составит 559 млрд руб. На долю российских вендоров придется 531 млрд руб. или 95% всего объема этой части рынка.

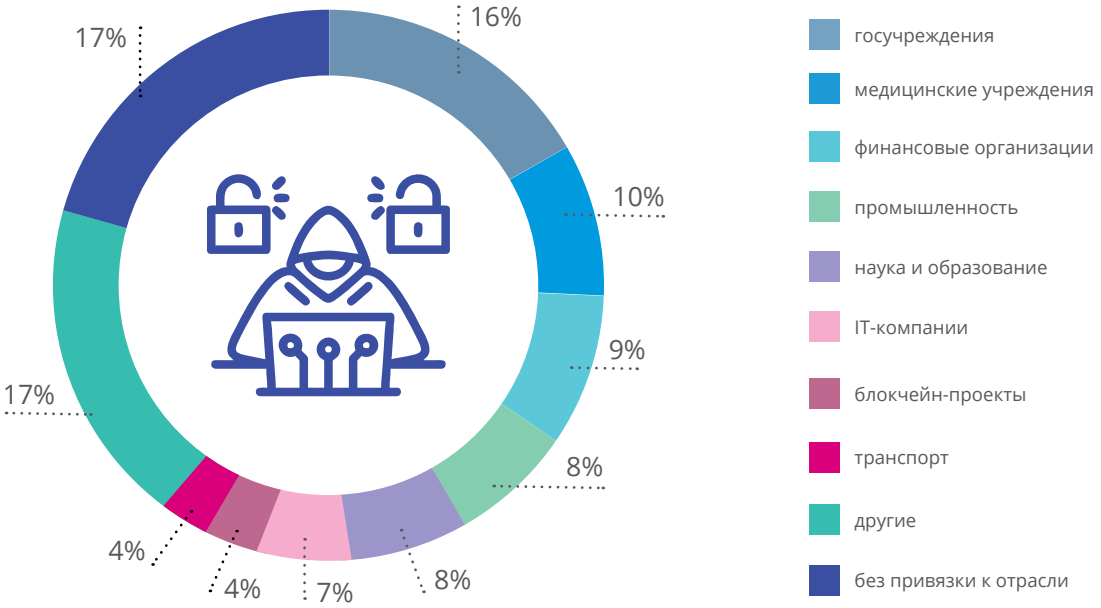
В целом по рынку ожидается бурный рост в следующие 5 лет с постепенным снижением темпов роста, но сохранение динамики роста существенно выше среднемировых. Сегмент средств защиты сетей ожидает активная конкурентная борьба за лидерство.

Рост российского рынка кибербезопасности связан со следующими факторами:

- массовый уход зарубежных вендоров с российского рынка, а также ограничение поставок их продуктов в Россию;
- значительный рост числа кибератак на органы власти, бизнес и промышленные объекты экономики РФ;
- ввод персональной ответственности руководителей организаций за обеспечение их информационной безопасности (см. Указ Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ»);
- запрет на закупку зарубежного программного обеспечения для использования на значимых объектах КИИ, а с 1 января 2025 года полный запрет использования зарубежного ПО на таких объектах (см. Указ Президента от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ»);
- поддержка ИТ-отрасли со стороны государства (субсидии, льготы, дополнительные учебные программы, снижение регуляторной нагрузки);
- ужесточение требований отраслевых регуляторов, предъявляемых к заказчикам ИБ-решений.

Статистика по кибератакам

Категории жертв среди организаций

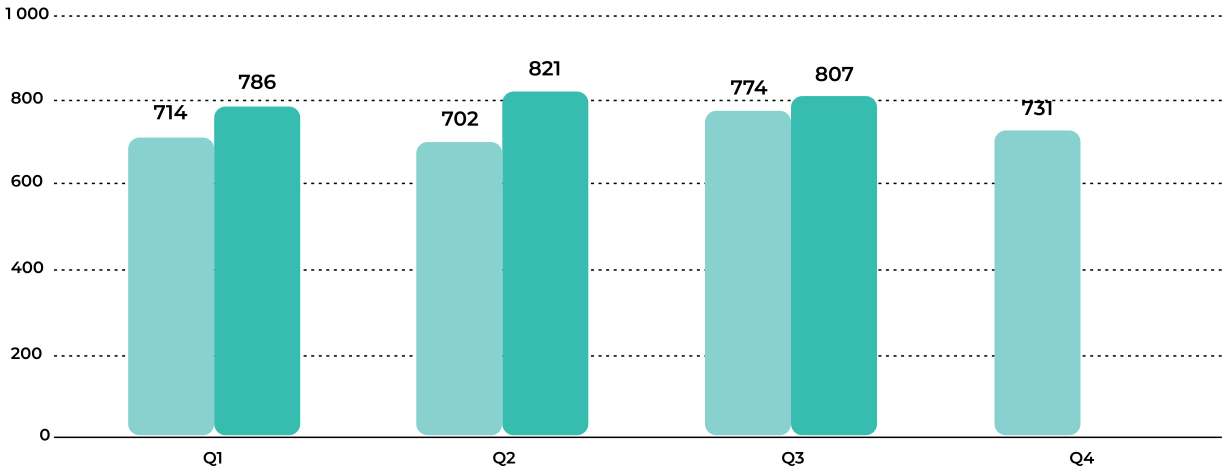


Источник: Positive Technologies

Массовые утечки данных в 2022-2023 годах коснулись многих организаций и частных лиц как в России, так и во всем мире. Пострадали такие известные компании и сервисы как Гемотест, СДЭК, Яндекс.Еда, Delivery Club, DNS.

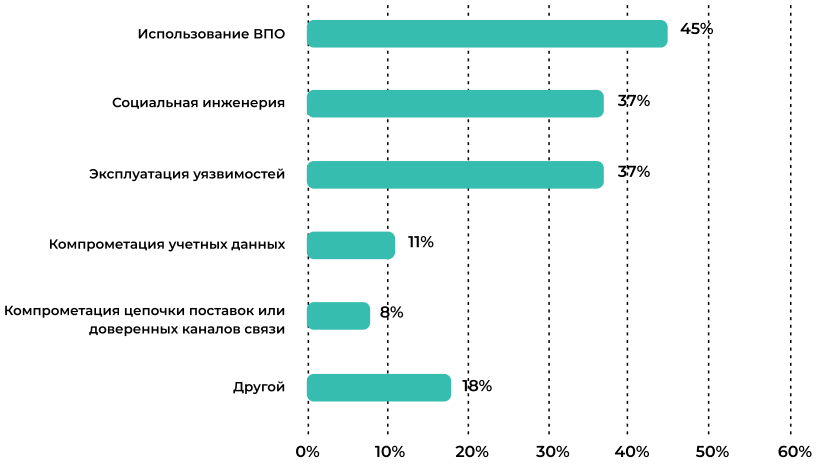
Ущерб от утечек во всем мире растет: согласно отчету IBM, в 2022 году средняя стоимость утечки данных достигла рекордно высокого уровня — 4,35 млн долларов, что на 2,6% больше, чем в 2021 году.

Количество атак в 2022 и 2023 годах (по кварталам)



Источник: Positive Technologies

Методы атак (доля успешных атак) в организациях



Источник: Positive Technologies

Законодательство

Указ Президента РФ 01.05.2022 № 250

«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» запрещает государственным органам использовать средства защиты из недружественных стран с 1 января 2025 года.

К каким организациям относится: госорганы и госкомпании

Указ Президента РФ от 30.03.2022 № 166

«О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» усиливает требования к инфраструктуре и информационной безопасности. В соответствии с документом, с 1 января 2025 г. органам государственной власти запрещается использовать иностранное ПО на принадлежащих им значимых объектах критической информационной инфраструктуры.

К каким организациям относится: госорганы и госкомпании

Федеральный закон от 27.07.2006 № 149-ФЗ

«Об информации, информационных технологиях и о защите информации»

Закон вводит понятие реестра сайтов, содержащих запрещенную в РФ информацию. Согласно закону, доступ к сайтам, включенным в реестр, должен быть ограничен. За нарушение этих требований предусмотрена дисциплинарная, гражданско-правовая, административная и уголовная ответственность. Чтобы избежать наказания, организации обязаны соблюдать требования законодательства и блокировать доступ пользователей к сайтам из реестра.

К запрещенной информации относится детская порнография, сведения о наркотиках, самоубийствах, азартных играх и несчастных случаях с несовершеннолетними, фильмы, книги, фотографии, музыка и другая информация, защищенная авторским правом, призывы к насилию, экстремизму и массовым беспорядкам.

К каким организациям относится: госорганы и госкомпании, образовательные и медицинские учреждения

Федеральный закон от 27.07.2006 № 152-ФЗ

«О персональных данных»

Закон № 152-ФЗ определяет порядок работы с информацией, прямо или косвенно относящейся к физическому лицу. Одно из требований закона — защита персональных данных физических лиц (сотрудников, клиентов, посетителей и т. д.)Защита персональных данных включена в раздел охраны труда на предприятии (государство гарантирует их защиту всем работникам).

Средство защиты информации должно пройти процедуру оценки соответствия, обнаруживать и предотвращать вторжения, регистрировать события безопасности и защищать информационную систему, устанавливая правила доступа к персональным данным.

К каким организациям относится: госорганы и госкомпании, образовательные и медицинские учреждения

Федеральный закон от 29.12.2010 № 436-ФЗ

«О защите детей от информации, причиняющей вред их здоровью и развитию»

В соответствии с законодательным актом в местах, доступных для детей, организатор доступа в интернет обязан обеспечить информационную безопасность детей, применяя административные и организационные меры, технические и программно-аппаратные средства защиты детей от информации, причиняющей вред их здоровью и развитию. В частности, должен быть заблокирован доступ к информации, провоцирующей на суицид, употребление наркотических средств, побуждающей к жестокости, пропагандирующей нетрадиционные сексуальные отношения, содержащей нецензурную брань, порнографию и др.

Нарушение 436-ФЗ, связанное с неприменением лицом, организующим доступ к распространяемой посредством информационно-телекоммуникационных сетей информации в местах, доступных для детей, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и развитию, наказывается административным штрафом. Для индивидуальных предпринимателей в размере от 5 тысяч до 10 тыс. рублей, для юридических лиц — от 20 тыс. до 50 тыс. рублей (статья 6.17 КоАП РФ).

К каким организациям относится: госорганы и госкомпании, образовательные и медицинские учреждения

Федеральный закон от 26.07.2017 № 187-ФЗ

«О безопасности критической информационной инфраструктуры РФ»

Согласно Федеральному закону от 26.07.2017 года № 187-ФЗ, критическая информационная инфраструктура (КИИ)представляет собой совокупность объектов КИИ, информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия таких объектов.

Закон накладывает ряд обязанностей на организации и компании, относящиеся к субъектам КИИ, в числе которых:

- соблюдение требований по обеспечению безопасности;
- незамедлительная реакция на компьютерные инциденты;
- оповещение уполномоченных организаций.

К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ, относятся в том числе средства защиты информации от несанкционированного доступа, межсетевые экраны, средства обнаружения и предотвращения вторжений, средства антивирусной защиты, средства контроля защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.

Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться сертифицированные средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки.

К каким организациям относится: госорганы и госкомпании, субъекты КИИ

Задачи и решения в сфере ИБ

Задача: Защита от кибератак

Основание: Федеральные законы №№ 152-ФЗ и 187-ФЗ

Суть проблемы: Киберпреступники непрерывно атакуют сети организаций с помощью вредоносного ПО, пытаются эксплуатировать уязвимости и вызвать отказ в обслуживании, чтобы нарушить доступность сервисов, проникнуть внутрь периметра и получить доступ к конфиденциальной информации. Нужно защитить инфраструктуру, чтобы она продолжала работать, несмотря на действия хакеров.

К каким организациям относится: госструктуры и госкорпорации, образовательные и медицинские учреждения, операторы ПДн.

Решение: использование функционала Универсального шлюза безопасности Traffic Inspector Next Generation — межсетевого экрана для защиты от кибератак и системы IDS/IPS для своевременного обнаружения и предотвращения кибернападений.

Задача: Переход на российское ПО и средства защиты

Основание: Указы Президента РФ №№ 166 и 250

Суть проблемы: в соответствии с Указами 166 и 250 госструктуры, госкорпорации и объекты КИИ обязаны до 1 января 2025 года полностью перейти на использование российского ПО и средств защиты.

К каким организациям относится: госструктуры и госкорпорации, субъекты КИИ.

Решение: внедрение Универсального шлюза безопасности Traffic Inspector Next Generation – российского продукта, входящего в Единый реестр российского программного обеспечения для ЭВМ и баз данных Мицифры России.

Задача: Использование сертифицированных защитных решений

Основание: Федеральный закон № 187-ФЗ

Суть проблемы: для обеспечения защиты информации, не составляющей гостайну, в государственных информационных системах должны применяться средства защиты, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации (т.е. имеющие соответствующий сертификат ФСТЭК).

К каким организациям относится: госструктуры и госкорпорации, субъекты КИИ.

Решение: переход на Traffic Inspector Next Generation FSTEC – сертифицированный ФСТЭК продукт, входящий в Единый реестр российского программного обеспечения для ЭВМ и баз данных Минцифры России.

Задача: Обязательная авторизация для общедоступных Wi-Fi сетей

Основание: Постановление Правительства РФ № 758

Суть проблемы: доступ к публичному беспроводному интернету в пунктах коллективного доступа может предоставляться только после идентификации пользователей.

К каким организациям относится: госструктуры и госкорпорации, образовательные и медицинские учреждения, операторы ПДн.

Решение: использование функции SMS-идентификации в составе Traffic Inspector Next Generation. Для авторизации посетителей используется SMS-идентификация по номеру телефона его владельца. После того как пользователь подключается к Wi-Fi, он попадает на специальную страницу, вводит номер своего телефона, получает сообщение с кодом доступа, вводит его на следующей странице и получает доступ в сеть.

Задача: Соблюдение законодательства о ПДн

Основание: Федеральный закон № 152-ФЗ

Суть проблемы: исключить несанкционированный доступ, утечки или перехват персональных данных во время их передачи и обработки.

К каким организациям относится: госструктуры и госкорпорации, образовательные и медицинские учреждения, операторы ПДн.

Решение: использование VPN для защищенного обмена информацией, межсетевого экрана для защиты от кибератак и системы IDS/IPS для своевременного обнаружения и предотвращения вторжений. Все эти компоненты входят в состав Универсального шлюза безопасности Traffic Inspector Next Generation.

Задача: Защита от нецелевого использования интернета

Суть проблемы: необходимо запретить сотрудникам посещать развлекательные и потенциально вредоносные ресурсы, чтобы устранить риски проникновения в сеть опасного контента и исключить потери рабочего времени.

К каким организациям относится: госструктуры и госкорпорации, образовательные и медицинские учреждения.

Решение: использование средств контроля трафика и блокировки по спискам и ключевым словам в составе Traffic Inspector Next Generation. С их помощью можно блокировать рекламу, сайты по URL и содержимому страниц, торренты и мессенджеры и т. п., вести учет посещений интернет-ресурсов.

Задача: Защита детей от информации, причиняющей вред их здоровью и развитию

Основание: Федеральный закон № 436-ФЗ, Приказ Минкомсвязи России № 161 от 16.06.2014

Суть проблемы: в местах, доступных для детей, организатор доступа в интернет обязан обеспечить информационную безопасность детей, применяя административные и организационные меры, технические и программно-аппаратные средства защиты детей от информации, причиняющей вред их здоровью и развитию.

В частности, должен быть заблокирован доступ к информации, провоцирующей на суицид, употребление наркотических средств, побуждающей к жестокости, пропагандирующей нетрадиционные сексуальные отношения, содержащей нецензурную брань, порнографию и др.

За несоблюдение этих требований как руководитель, так и сама образовательная организация могут быть оштрафованы контролирующими органами.

К каким организациям относится: образование, включая дистанционное.

Решение: в настройках межсетевого экрана, входящего в состав Traffic Inspector Next Generation, есть опция блокировки отдельных групп в соцсетях и разделов сайтов. Вместе с тем, разрешенный контент порталов остается доступным, если это необходимо для учебного процесса (например, в «Википедии» можно заблокировать статьи о том, как создавать запрещенные вещества в домашних условиях, но оставить доступ к полезным статьям).

Подключение к порталу Роскомнадзора позволяет скачивать реестр сайтов из черного списка в режиме реального времени. Модуль контентной фильтрации определяет и блокирует «плохие» страницы по содержащимся на них словам. Администратор может использовать уже готовые списки, дополнять их или составлять свои.

Задача: Защищенное управляемое взаимодействие между подразделениями, в том числе территориально распределенными.

Основание: Федеральный закон № 152-ФЗ

Суть проблемы: крупные организации имеют обширную сеть подразделений и филиалов, которые активно взаимодействуют друг с другом. Передача по открытым интернет-каналам конфиденциальной информации о пациентах, историях болезни, персональной информации сотрудников госкомпаний, студентах и школьниках может привести к утечке и нарушению закона «О защите персональных данных» (№ 152-ФЗ).

К каким организациям относится: госструктуры и госкорпорации, образовательные и медицинские учреждения, операторы ПДн.

Решение: технология шифрования данных VPN (Virtual Private Network) полностью исключает возможность перехвата информации, передаваемой между подразделениями. Система IDS/IPS для обнаружения и предотвращения неавторизованного доступа и другие современные средства защиты отражают различные типы атак. Для защиты географически распределенных подразделений удобно использовать несколько устройств Traffic Inspector Next Generation с единым центром управления Central Management System.

Задача: Разграничение трафика по категориям пользователей

Суть проблемы: во многих организациях существуют категории пользователей с разными задачами и различной потребностью в доступе к интернет-ресурсам. Например, в образовательных учреждениях есть преподаватели, которым требуется доступ с минимальными ограничениями, и учащиеся, для которых должна выполняться фильтрация в соответствии с требованиями законодательства. В госкомпаниях это могут быть сотрудники отдела маркетинга или закупок, которым требуется доступ к соцсетям и различным СМИ, и сотрудники бухгалтерии, которым для работы необходим только доступ к бухгалтерскому порталу.

Невозможность разграничить трафик по категориям может повысить риски заражения компьютеров вредоносным ПО, а также создаст возможности для нецелевого использования интернета в рабочее время.

К каким организациям относится: госструктуры и госкорпорации, образовательные и медицинские учреждения.

Решение: создать группы доступа на веб-прокси, использовать средства контроля трафика и блокировки по спискам и ключевым словам в составе Traffic Inspector Next Generation. С их помощью можно блокировать рекламу, сайты по URL и содержимому страниц, торренты и мессенджеры и т. п., вести учет посещений интернет-ресурсов.

Traffic Inspector Next Generation FSTEC

универсальный шлюз безопасности, сертифицированный для использования госучреждениями и операторами персональных данных

Traffic Inspector Next Generation (TING) – сетевой шлюз (UTM на основе NGFW) для организации контролируемого доступа в интернет корпоративных компьютерных сетей и их защиты от внешних угроз, разрабатываемый российской компанией «Смарт-Софт».

Решение разворачивается в роли шлюза на границе корпоративной сети и позволяет контролировать информационные потоки между локальной сетью и интернетом.

TING содержит более 80 различных функций, среди которых:

средства защиты сети от киберугроз:

- межсетевой экран,
- система обнаружения и предотвращения вторжений (IDS/IPS),
- контроль приложений (L7-фильтрация).

система контроля доступа в интернет:

- фильтрующий веб-прокси,
- различные методы аутентификации,
- контентная фильтрация,
- декодирование HTTPS-трафика,
- Captive Portal.

средства управления каналом и трафиком:

- VPN (в т.ч. ГОСТ-VPN, Site-to-Site IPSec),
- шейпирование трафика,
- балансировка канала,
- Connection Failover,
- кластер высокой доступности,
- централизованная система управления (CMS).

мониторинг и отчеты:

- мониторинг трафика,
- отчеты по веб-прокси,
- системный журнал,
- журнал межсетевого экрана.

Сертификат соответствия ФСТЭК № 4692

Действителен до 13.07.2028 г.

Универсальный шлюз безопасности (UTM) Traffic Inspector Next Generation сертифицирован ФСТЭК России. Сертификат соответствия № 4692 от 13.07.2023 удостоверяет, что Traffic Inspector Next Generation является средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям следующих документов:

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия;
- «Требования к межсетевым экранам» (ФСТЭК России, 2016);
- «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016);
- «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016);
- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011);
- «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Сертифицированный универсальный шлюз безопасности Traffic Inspector Next Generation FSTEC может применяться в следующих информационных системах:

- в значимых объектах критической информационной инфраструктуры (КИИ) 1 категории;
- в государственных информационных системах (ГИС) до 1 класса защищенности включительно;
- в автоматизированных системах (АС) управления производственными и технологическими процессами до 1 класса защищенности включительно;
- в информационных системах персональных данных (ИСПДн) до 1 уровня защищенности включительно;
- в информационных системах общего пользования II класса.

Варианты поставки
Traffic Inspector Next Generation FSTEC

Программное обеспечение – от 5 до 7000 учетных записей

Программно-аппаратные комплексы

Аппаратные платформы	Характеристики	Производитель
Traffic Inspector Next Generation S100 FSTEC-NP	NP-1002i CPU C3538 (4 core) / RAM 16 Gb / 512 Gb / без VGA	New Platforms
Traffic Inspector Next Generation S300 FSTEC-AQ	Аквариус T30 S001DC CPU Intel Atom C3758 2.2GHz, 8C/8T, 16MB, 25W/ CPU cooler/ RAM DIMM DDR4 16GB 2666MHz ECC/ SSD SATA 480GB 2.5» 7mm RI/ трансивер 1000BASE-T RJ-45 Copper SFP Optical Transceiver/ PSU 2x200W Hot-Swap, 80Plus/ кабель питания C13-C14, 1.8m	AQUARIUS
Traffic Inspector Next Generation M700 FSTEC-AQ	Аквариус T50 D110CF CPU Intel Xeon Silver 4216 2.1GHz, 16C/32T, 22MB, 100W/ CPU cooler/ RAM RDIMM DDR4 16GB 3200MHz ECC/ SSD SATA 960GB 2.5» 7mm RI/ кабель HDminiSAS, SFF8643 - SFF8643, 0.7m/ кабель HDminiSAS, SFF8643 - SFF8643, 0.8m/ NIC PHY OCP mezz 10GbE, Dual port, 2xSFP+/ NIC PCI-E x4, 1GbE, Quad port, 4xRJ-45, HHHL (Intel i350)/ PSU 550W Hot-Swap, 80Plus Platinum, CRPS/кабель питания C13-C14, 3m	AQUARIUS
Traffic Inspector Next Generation L1500 FSTEC-AQ	Аквариус T50 D202FW CPU Intel Xeon Gold 5218R 2.1GHz, 20C/40T, 27.5MB, 125W/ CPU cooler/ RAM RDIMM DDR4 32GB 3200MHz ECC/ SSD SATA 960GB 2.5» 7mm RI/ кабель HDminiSAS - 4xSATA, SFF8643 - 4xSATA, 0.8-1m для серверов CF/FW/BJ/ NIC PCI-E x8, 10GbE, Quad port, 4xSFP+, HHHL (Intel X710)/ NIC PCI-E x8, 40GbE, Dual port, 2xQSFP+ (Intel XL710)/ PSU 800W Hot-Swap, 80Plus Platinum, reversed airflow, CRPS/ кабель питания C13-C14, 1.8m	AQUARIUS

Почему выбирают Traffic Inspector Next Generation от Смарт-Софт

С ростом объемов и значимости цифровой информации растут и риски несанкционированного доступа в корпоративную сеть и утечки данных. Поэтому важно принимать защитные меры, направленные на обеспечение сетевой безопасности. Использование универсальных шлюзов безопасности (UTM) – одна из мер, ставшая стандартом обеспечения безопасности внутренних сетей и данных. Все чаще она становится обязательной на законодательном уровне.

Например, с начала 2018 года установка систем обеспечения безопасности инфраструктуры и обнаружения вторжений стала обязанностью всех госкомпаний, юридических лиц и индивидуальных предпринимателей, являющихся субъектами КИИ. Владельцы объектов КИИ должны информировать власти о компьютерных инцидентах и предотвращать попытки несанкционированного доступа к информации.

Нарушение законов ведет к негативным последствиям, вплоть до штрафов и персонального взыскания с руководителя организации. Избежать этого можно с помощью UTM-системы, отвечающей требованиям законодательства. Внедрив такое решение, руководитель получает уверенность в том, что в его организации не нарушается ни один федеральный закон.

Смарт-Софт — российская ИТ-компания, обладающая широкими компетенциями и продуктами собственной разработки в сфере информационной безопасности.

Смарт-Софт лицензирован Федеральной службой по техническому и экспортному контролю (ФСТЭК) на деятельность по разработке и производству средств защиты конфиденциальной информации.

Флагманская разработка компании — универсальный шлюз безопасности (UTM) Traffic Inspector Next Generation.

Решения Смарт-Софт входят в Единый реестр российских программ для ЭВМ и баз данных Минцифры России, Traffic Inspector Next Generation сертифицирован ФСТЭК России.

Бесплатное тестирование

Выбор решения по обеспечению информационной безопасности — ответственный процесс, требующий серьезного подхода. Как правило, компания-заказчик составляет перечень требований к решению в форме технического задания, в соответствии с которым выбирает оптимальный по параметрам продукт. Самый надежный способ убедиться в том, что выбранный вариант решит поставленные задачи — протестировать работу всех необходимых функций в боевых условиях.

Понимая потребности клиентов, «Смарт-Софт» предлагает в течение **30** дней бесплатно протестировать Traffic Inspector Next Generation.

Заказать бесплатное тестирование **Traffic Inspector Next Generation:**

info@smart-soft.ru

+7 (495) 775-59-91

www.smart-soft.ru

Особые условия покупки Traffic Inspector Next Generation для образовательных учреждений и НКО

Льготные категории организаций могут приобретать как коммерческую, так и сертифицированную ФСТЭК версию программного обеспечения Traffic Inspector Next Generation цене на **15%** ниже текущей стоимости соответствующей базовой лицензии.

Смарт-Софт предоставляет особые условия покупки
для следующих организаций:

Российские учреждения образования: дошкольные, общеобразовательные, профессиональные, высшего образования, дополнительного профессионального образования.

Российские некоммерческие организации и благотворительные фонды (исключая политические партии, религиозные организации, жилищно-строительные кооперативы, адвокатские образования).

Для получения скидки организация, относящаяся к перечню льготных категорий, должна будет подтвердить свой статус, предоставив в Смарт-Софт документы, удостоверяющие ее сферу деятельности и организационно-правовую форму.

Узнать больше:
info@smart-soft.ru
+7 (495) 775-59-91

Миграция на Traffic Inspector Next Generation

Для пользователей многофункционального межсетевого экрана Traffic Inspector, а также для пользователей USG, UTM и NGFW других производителей действует скидка **30**% на программное обеспечение **Traffic Inspector Next Generation** (кроме Traffic Inspector Next Generation SaaS).

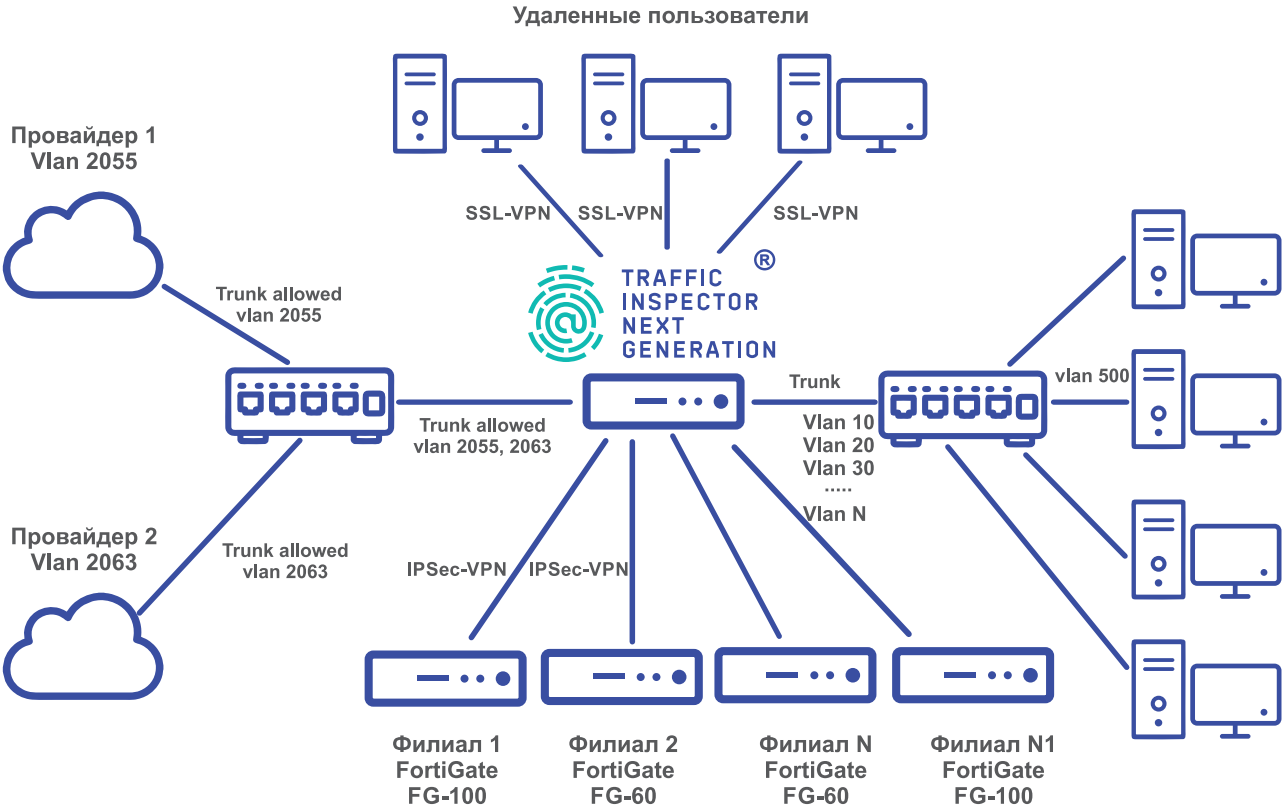
Скидка предоставляется при переходе на Traffic Inspector Next Generation с таким же количеством пользователей, как у продукта другого производителя, в соответствии с данными лицензионного соглашения.

Чтобы узнать подробности, свяжитесь со Смарт-Софт:

info@smart-soft.ru

+7 (495) 775-59-91

Кейс мягкой миграции на Traffic Inspector Next Generation с зарубежного решения



В начале марта 2022 года многие западные компании прекратили или приостановили работу на территории России. Среди них была американская компания Fortinet, производитель оборудования FortiGate, популярного среди отечественных компаний. Следствием такого решения стала невозможность купить новое оборудование, а также получить техническую поддержку и обновления для используемого ПО FortiGate.

Применение необновленных устройств для защиты интернет-подключений увеличивает риски проникновения злоумышленников в корпоративную сеть, поэтому многие пользователи FortiGate стали искать пути решения этой проблемы.

Одному из наших заказчиков мы предложили простой вариант с минимальными рисками и отличным результатом.

Исходная конфигурация

Компания использовала оборудование Fortinet в качестве интернет-шлюзов и для организации подключения удаленных пользователей.

Подключений к интернету было два:

- основной канал с одним внешним IP-адресом;
- резервный канал, 8 IP-адресов с маской /29.

Оба канала подключались к коммутатору, на котором был создан специальный VLAN Allowed. Этот же VLAN приходил на WAN-порт маршрутизатора FortiGate FG-100.

Удаленные и локальные пользователи подключались к этому же маршрутизатору. Для них был создан отдельный VLAN Vlan500. Удаленные пользователи использовали при подключении SSL VPN.

К этому же маршрутизатору через VPN с использованием IPSec были подключены филиалы. Имеющиеся там устройства FortiGate выполняли маршрутизацию трафика в сеть центрального офиса.

Решение

Оказалось достаточно добавить всего один новый компонент — Traffic Inspector Next Generation (TING) — в сетевую топологию компании. Все остальные задачи были решены путем настройки конфигурации на устройствах TING и FortiGate.

TING установили между интернетом и сетью компании. Затем настроили туннель между TING и FortiGate и включили протокол динамической маршрутизации, для которого воспользовались плагином os-zerotier в составе TING.

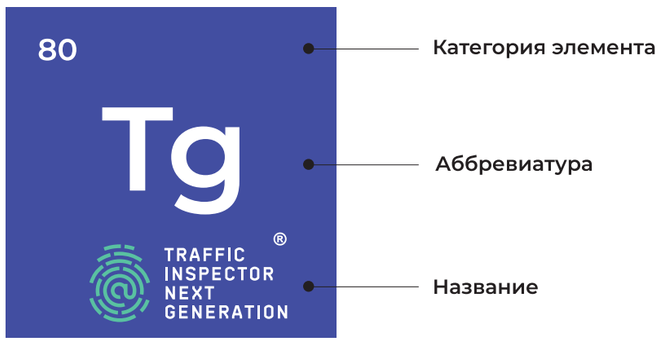
В результате весь внешний трафик стал транслироваться через универсальный шлюз безопасности Traffic Inspector Next Generation, а администраторы компании получили возможность выполнить фильтрацию этого трафика, выполнять его антивирусную проверку, а также блокировать доступ пользователей к определенным интернет-ресурсам.

При этом не пришлось менять настройки удаленных пользователей, подключающихся к сети с использованием SSL VPN, а также филиалов, использующих IPSec. Зато благодаря фильтрации входящего трафика на шлюзе, снизилась опасность заражения пользовательских устройств вредоносным ПО, которое кто-то из локальных пользователей мог, например, сохранить в общих папках.

Более подробно о выполненных настройках
читайте в нашей статье.

Периодическая система элементов Traffic Inspector Next Generation

	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV	XVI
1	1 Pf Packet Filter	2 Sa Suricata			Pf Firewall		Ia Аутентификация		Ks Службы			Ig Протоколы				3 Bd BFD
2	4 Nt NAT	5 Ne NETMAP			Sa IDS/IPS		Is VPN/Туннели		Nf Отчеты			Ss Управление				6 Rp RIP
					Br Интерфейсы		Lf Фильтрация		Cf Отказоустойчивость			Of Маршрутизация				
3	7 Gi GeoIP	8 Ld Local DataBase	9 Lp LDAP	10 Is Ipsec	11 Dh DHCP	12 Dn DNS	13 Si Squid	14 Nf NetFlow	15 Db Dashboard	16 Sl Squid log	17 Fl Firewall log	18 Rt RRDtool	19 Ap Active-Passive	20 Sh SSH	21 Wi Web-интерфейс	22 Of OSPF
4	23 Lb Load Balancer	24 Sp SMS Portal	25 Ia IP-адреса	26 Kb Kerberos	27 Ov OpenVPN	28 Wg Wireguard	29 Ks Kaspersky	30 Rs Rspamd	31 Sm SMTP	32 Ip IP	33 Gg GGP	34 Sg Syslog	35 Cf Connection Failover	36 Ss Secure Source	37 Cm CMS	38 Bp BGP
5	39 Vl VLAN	40 Gi GIF	41 Ma MAC-адреса	42 Nm NTLM	43 Fi FreeIPA	44 Lt L2TP	45 Gr GRE	46 Ft FTP	47 Mo Monit	48 Dd Dnsmasq DNS	49 Ud UDP	50 Tc TCP	51 Ic ICMP	52 Hp HTTP	53 Ei Экспорт/импорт настроек	54 Bu Backup
6	55 La LAN	56 Wa WAN	57 Ru RADIUS	58 Cp Captive Portal	59 Tf 2FA	60 Pt PPTP	61 Tv Ting VPN	62 Gv ГОСТ VPN	63 Pe PPPOE	64 Tl Telnet	65 Sq SQL	66 Ra RAP	67 Qo QoS	68 Ig IGMP	69 Eg EGP	70 Hs HTTPS
7	71 Lg LAGG	72 Br Bridge	73 Vx VXLAN	74 So SSO	75 Lf Layer 7 Filter	76 Sh Shaper	77 As Antispam	78 Ac ACL								



SMART-SOFT®

ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РУКОВОДИТЕЛЮ

Изучайте новости законодательства и официальные документы

Регуляторы и вышестоящие организации выпускают указания, положения по обеспечению информационной безопасности, регламенты и другие нормативные акты. Как правило, это малопонятные тексты, написанные канцелярским языком. Поручите юристам совместно с ИТ-службой выделить из них главное, а затем обсудите с ними реализацию поставленных задач.

Доведите до персонала опасность раскрытия их паролей

Неважно, как сотрудник передаст свой пароль преступнику, напишет на стикере и приклеит снизу клавиатуры или введет на фишинговом сайте. Люди должны осознать, что, получив этот пароль, хакер сможет взломать всю сеть. Добейтесь, чтобы по возможности для всех учетных записей была включена двухфакторная аутентификация. Дайте указание ИТ-службе включить обязательную смену паролей раз в квартал.

Проконтролируйте резервное копирование важной информации

Резервное копирование — это периодическая запись всех цифровых данных организации на внешний накопитель информации. Если в результате кибератаки данные будут зашифрованы и недоступны для использования, работу можно будет продолжить, восстановив их с резервной копии.

Оптимальный вариант — делать полную резервную копию раз в неделю или месяц, а ежедневно делать только копии изменившихся файлов. Тогда при необходимости можно будет восстановить полную копию, а затем быстро довести ее до актуального состояния, «накатывая» ежедневные изменения.

Организуйте обучение и тренировку сотрудников навыкам безопасного поведения

Хакеры активно используют социальную инженерию, чтобы заставить сотрудников компаний выполнить нужное им действие. Если ваши сотрудники научатся распознавать подозрительные ситуации во время работы, вы получите дополнительный рубеж обороны.

Приобретите для компании специальные курсы или даже платформу для обучения и тренировки навыков безопасного поведения. Назначайте обучение новым сотрудникам, проводите регулярные проверки с помощью учебных кибератак, а по их результатам выявляйте «слабых» коллег, чтобы обучить их повторно.

Smart-Soft®

ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМНОМУ АДМИНИСТРАТОРУ

Используйте антивирусы на уровне шлюза

Главный источник вирусов и вредоносных программ других типов — интернет. Установив антивирус на уровне шлюза, вы защитите сразу все компьютеры локальной сети, так как он проверяет проходящий через прокси-сервер трафик. Не забудьте прописать каждому пользователю в качестве прокси-сервера шлюз с антивирусом.

Госкомпаниям необходимо использовать решения, сертифицированные ФСТЭК.

Используйте систему обнаружения/предотвращения вторжений (IDS/IPS)

Атаки на компьютерные сети организаций исходят в основном извне. Целью хакеров может стать как внешний ресурс (например, веб-сайт), так и внутренний (скажем, база данных). Решение — система обнаружения/предотвращения атак (IDS/IPS), которая распознает источники атак и атакуемые машины по сигнатурам сетевого трафика и защищает сеть предприятия от подобных негативных воздействий. Кроме того, система оповещает администратора о происходящем и составляет отчеты действий, чтобы впоследствии по ним можно было расследовать вторжения.

Одна из самых популярных IDS — Suricata. Ее база сигнатур содержит актуальный список компьютерных атак. При этом можно подключить базы еще одной популярной системы обнаружения атак — Snort. Как правило, функция IDS/IPS входит в состав универсальных UTM-систем информационной безопасности, причем не только дорогих западных, но и более доступных отечественных.

Используйте прокси-сервер для фильтрации сетевого трафика

Часто перед системным администратором ставят задачу заблокировать нерегламентированные действия пользователей рабочих станций. Например, сделать так, чтобы те не смотрели видеоролики, не сидели в соцсетях, не скачивали пиратский контент. Эти действия не только съедают рабочее время сотрудников, но и могут привести к заражению машин. Чтобы избежать опасности, на прокси-сервере необходимо установить правила блокировки доступа к тем веб-ресурсам, посещение которых нежелательно.

Прокси-сервер Squid позволяет настроить правила как для входящего, так и для исходящего трафика. Кроме того, в состав прокси-сервера входят средства SSL-bump, которые умеют расшифровывать защищенный трафик (HTTPS).

Полную версию инструкции читайте:

www.smart-soft.ru

TRAFFIC INSPECTOR NEXT GENERATION®

Smart-Soft®

Настоящая безопасность

Смарт-Софт — многопрофильная российская ИТ-компания с широкими компетенциями и продуктами собственной разработки в сфере информационной безопасности. Мы придерживаемся концепции эшелонированной обороны от киберугроз и практикуем многоуровневую модель защиты информационных систем заказчиков.

С 2003 года команда Смарт-Софт занимается разработкой комплексных решений по защите компьютерных сетей от внешних угроз и оказывает услуги и сервисное сопровождение проектов в области информационной безопасности.

Строим эффективные системы многоуровневой защиты информации

- Разработка модели угроз и возможных рисков
- Разработка политики безопасности и организационно-распорядительной документации
- Выбор методов и программно-технических средств защиты информации

КОНТАКТЫ

тел.: +7 (495) 775-59-91,
8 (800) 600-17-90

info@smart-soft.ru

www.smart-soft.ru