ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛОКАЛЬНЫХ СЕТЕЙ

Курманов Талгат Нургалеевич

Академия ФСО России, РФ, г. Орел

Тезин Александр Васильевич

научный руководитель, сотрудник, Академия ФСО России, РФ, г. Орел

Кокорев Антон Владимирович

научный руководитель, сотрудник, Академия ФСО России, РФ, г. Орел

INFORMATION SECURITY OF LOCAL NETWORKS

Talgat Kurmanov

Academy of Federal Guard Service of Russian Federation, Russia, Orel

Aleksander Tezin

Scientific director, Employee, Academy of Federal Guard Service of Russian Federation, Russia, Orel

Anton Kokorev

Scientific director, Employee, Academy of Federal Guard Service of Russian Federation, Russia, Orel

Аннотация. В данной статье рассматриваются актуальные проблемы обеспечения безопасности локальных сетей, основные виды угроз, которым подвержены вычислительные сети, а также способы противодействия им.

Abstract. This article discusses current issues of local network security, the main types of threats to which computer networks are exposed, as well as ways to counter them.

Ключевые слова: локальная сеть, защита информации, система обнаружения вторжений, атака, антивирусное программное обеспечение.

Keywords: local network, information security, intrusion detection system, attack, anti-virus software.

В настоящее время локальная сеть являются неотъемлемой составляющей процесса

функционирования офисов, отделов и организаций. Благодаря своей гибкости, сеть может активно использоваться сотрудниками или не использоваться совсем. Локальная сеть имеет ряд преимуществ, позволяющих существенно упростить процесс взаимодействия между устройствами, а также обеспечить быстрый доступ к требуемой информации. Ввиду своей востребованности необходимо обеспечить защиту локальных сетей от совершения нелегитимных действий злоумышленниками.

Локальная сеть – это группа компьютеров и связанные с нею устройства, которые служат интересам определенного числа пользователей и осуществляют подключение по общей линии связи, использующая ресурсы выделенного сервера или процессора [1].

Локальные сети могут быть реализованы через проводное или беспроводное соединение. При реализации проводного соединения, на рисунке 1 используются кабели Ethernet, при этом необходимо сконфигурировать коммутатор (Switch) и маршрутизатор (Router).

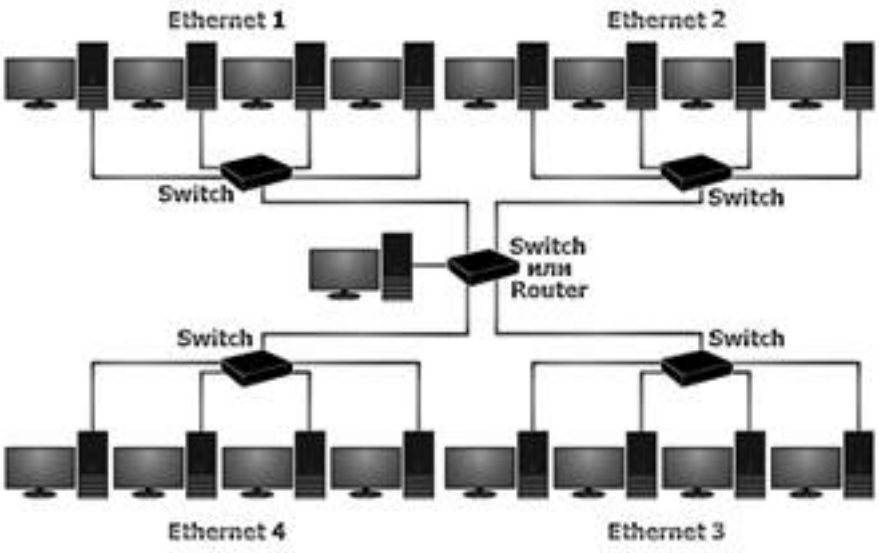

Рисунок 1. Проводная локальная сеть

Беспроводное соединение реализуется через точки беспроводного доступа – точки приёма сигнала и передачи радиоволн. Точки доступа представляют собой коммуникационные узлы, через которые пользователи локальной сети имеют возможность общаться с проводной сетью. На рисунке 2 показано взаимодействие проводных и беспроводной сетей с точкой доступа.

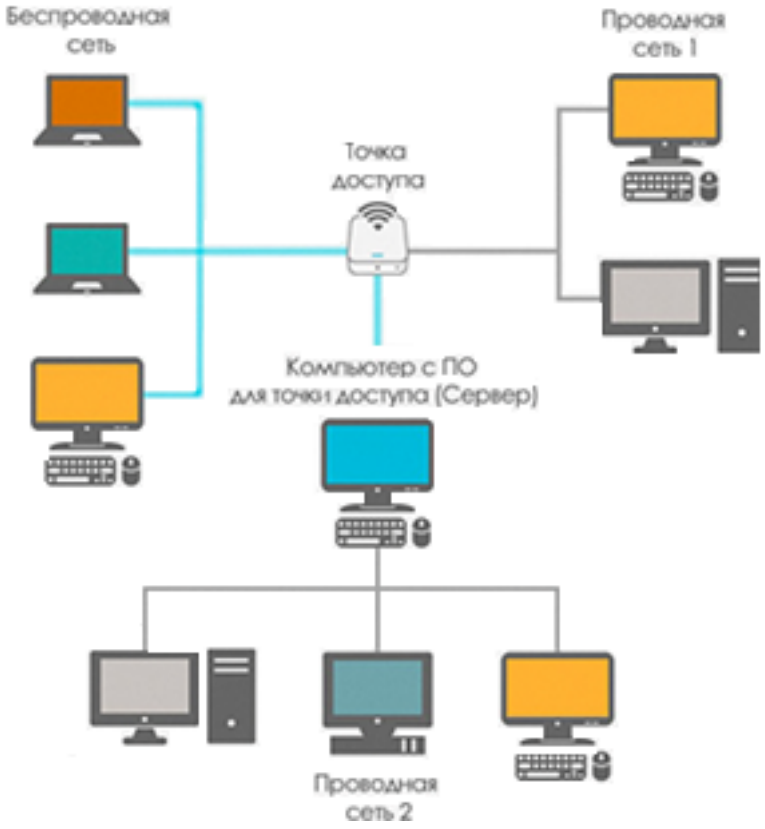

Рисунок 2. Схема и проводных и беспроводной сетей

Использование виртуальной частной сети. Локальная сеть имеет ряд преимуществ, обеспечивающих актуальность её применения: быстрота и экономичность использования; гибкость; наличие общей базы данных и программного обеспечения для всех пользователей сети; возможность изменения данных с сервера; высокая скорость передачи данных между устройствами; масштабируемость сетей; возможность использования глобальной сети Internet. Несмотря на обилие достоинств, локальная сеть имеет свои недостатки, связанные как с обеспечением безопасности, так и с её обслуживанием: высокая стоимость коммуникационного оборудования; необходимость установки программного обеспечения на сервер; невозможность создания локальной сети в глобальной; некорректная работа сервера приводит к сбоям во всей сети.

Для обеспечения безопасности локальных сетей необходимо использовать несколько уровней защиты [2]. На первом уровне таким средством служит межсетевой экран или брандмауэр, также именуемый фаерволом. Брандмауэр представляет собой программу, предотвращающую несанкционированный доступ к сети путем проверки трафика с помощью набора правил выявления угроз. Межсетевые экраны применяются в корпоративных и персональных сетях и являются неотъемлемым компонентом безопасности сети.

В случае необходимости удаленного доступа к ресурсам компании таким средством защиты служат виртуальные частные сети, так называемые VPN (Virtual Private Network) [2]. VPN – обеспечивает защищенное сетевое соединение через публичные сети. На рисунке 3 изображена архитектура VPN, принцип работы которой заключается в сокрытии IP-адреса и перенаправлении его через удаленный сервер.

Рисунок 3. Архитектура VPN

Применение систем предотвращения вторжений. Несмотря на наличие вышеупомянутых средств, в сеть могут получить доступ неавторизованные пользователи. Для выявления данных фактов используются системы обнаружения и предотвращения вторжений, или IDS/IPS (Intrusion Detection System и Intrusion Prevention System). При установке IDS/IPS необходимо выяснить в каком месте данная система должна быть расположена. Выбор места расположения зависит от типа выбранной системы.

Система обнаружения вторжений может быть установлена перед файрволлом. В таком случае IDS будет анализировать только незаблокированный межсетевым экраном трафик, так как анализ блокируемых данных нецелесообразен.

С этой целью IDS устанавливают на внешней границе сети, после межсетевого экрана. Пример такого расположения изображен на рисунке 4. Данный вид построения системы защиты обеспечивает фильтрацию излишних шумов глобальной сети и защиту от возможности картирования сети. Такое расположение обеспечивает контроль 4 – 7 уровней сети. Данная архитектура обеспечивает сокращение числа ложных срабатываний. Расположение IDS следует выбирать в зависимости от требований к ней, а также средств и размеров сети.

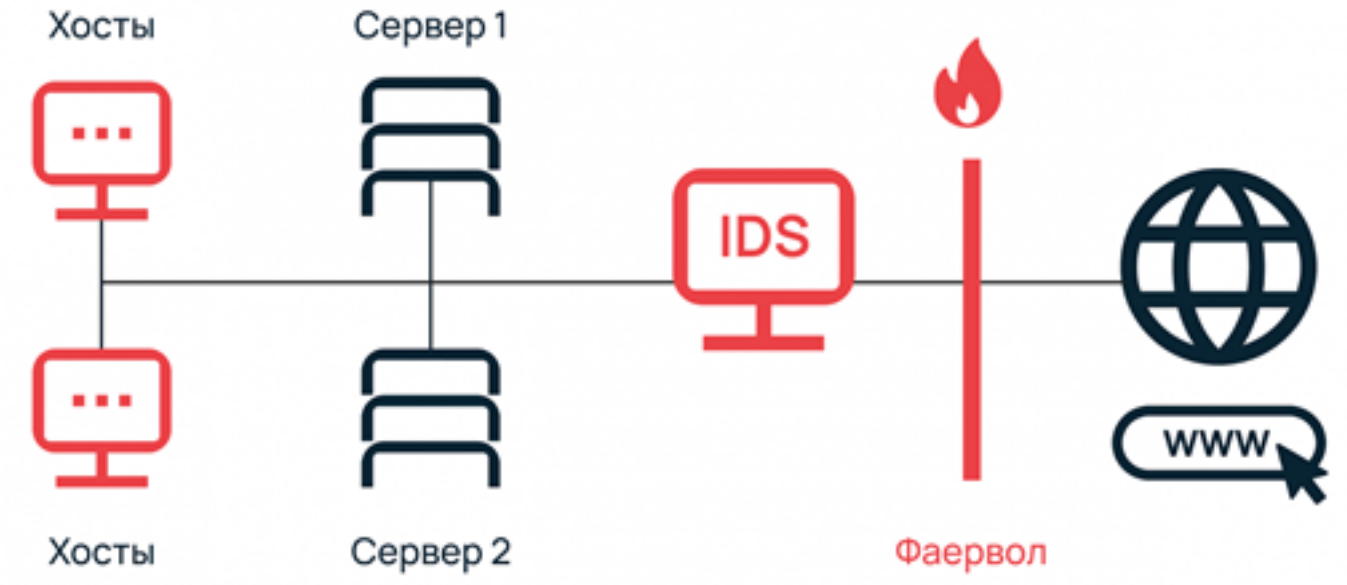

Рисунок 4. Пример расположения IDS

В случае необходимости возможно использование нескольких копий IDS в критически важных местах [3]. На рисунке 5, IDS расположены за сетевым экраном, непосредственно перед серверами. Также возможно размещение IDS внутри сети для обнаружения подозрительной активности.

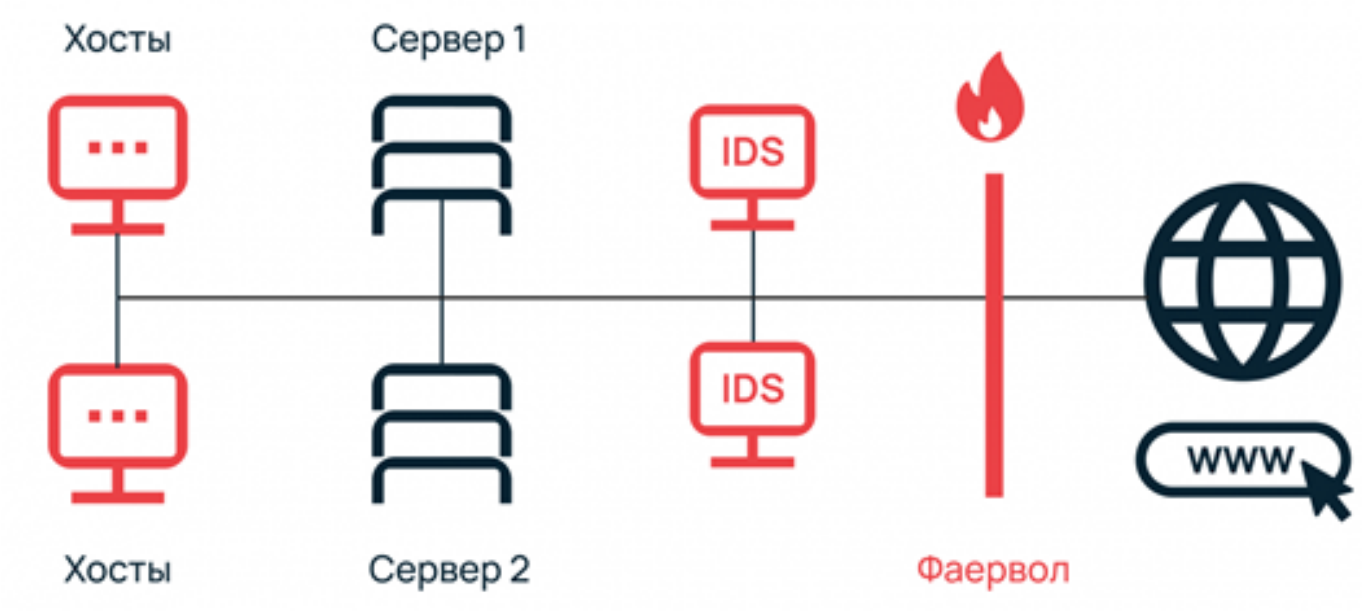

Рисунок 5. Размещение нескольких IDS

Сетевая система обнаружения вторжений. Технология сетевого обнаружения вторжений NIDS (Network Intrusion Detection System) – технология, которая позволяет устанавливать систему в стратегически важных местах сети, а также осуществлять анализ входящего и исходящего трафика на всех устройствах, находящихся в сети [3]. NIDS позволяет анализировать трафик в каждом пакете, начиная с канального уровня, заканчивая прикладным. В отличие от межсетевого экрана, технология NIDS способна обнаружить как внешние, так и внутренние угрозы, в то время как межсетевой экран идентифицирует только атаки вне сети. Сетевые системы обнаружения вторжений являются более экономичными ввиду способности контролировать всю сеть. Недостатком NIDS является большое потребление ресурсов, возникающее из-за отслеживания всего сетевого трафика. Большой объем трафика приводит к высокой потребности в ресурсах CPU и RAM, что приводит к задержкам в обмене данными, а также к снижению скорости работы сети.

Примером работы системы NIDS является ПО Suricata, изображенная на рисунке 6. Suricata – система сетевого обнаружения и предотвращения вторжений, представленная в 2010 году. Выявление угроз в Suricata происходит по сигнатурам. Небольшое количество legacy-кода позволяет Suricata работать гораздо быстрее, нежели ее аналогам.

Рисунок 6. Интерфейс Suricata

Антивирусные программы. Антивирусные программы и программы защиты от вредоносного ПО – это специализированные программы, необходимые для обнаружения вирусов и нежелательного ПО, обеспечивающие предотвращение, профилактику и восстановление модифицированных программ. Антивирусные программы и программы защиты от вредоносного ПО имеют сходство, однако в них присутствует и ряд отличий.

Антивирус основывается на профилактике, он защищает сеть, активно предотвращая заражение конечных устройств. Антивирусные программы – лечат и защищают сеть путем обнаружения и уничтожения вредоносного ПО, проникшего в сеть.

При попытке собственной защиты, вредоносные программы используют комплекс методов, позволяющих избежать обнаружения и уничтожения. Целью антивирусных программ служит защита систем и сетей от различных методов самосохранения. Вредоносное ПО имеют возможность мутировать, что обеспечивает затруднение в создании сигнатур. Помимо этого, существует вредоносное ПО, активно атакующее антивирусные ПО и брандмауэры, с целью завершения их процессов и предотвращения их запуска.

Обнаружение вредоносного ПО является чрезвычайно важным, причем своевременное обнаружение, позволяет предотвратить распространение вирусов и червей, а также ограничить их уничтожение до его начала. Антивирусная программа может защитить устройства от различных видов угроз, таких как: вирусы, черви, троянские кони, рекламное и запасное ПО, программы-выкупы, объекты-помощники браузера, кейлоггеры, бэкдоры и руткиты.

Для этого они используют различные уровни защиты обнаружения возможных вирусов, которые включают в себя комплекс мер - от проверенных и испытанных определений вирусов и эвристики до более новых технологий, таких как обнаружение в песочнице, обнаружение поведения, искусственный интеллект, машинное обучение и облачная детонация файлов.

Поскольку природа вредоносных программ постоянно меняется, применение обоих вариантов защиты сети в сочетании является наилучшим методом обеспечения безопасности сети. На рисунке 7 представлен результат длительного тестирования антивирусного ПО. В результате

тестирования антивирус Kaspersky занял первое место в 51 из 93 испытаний.

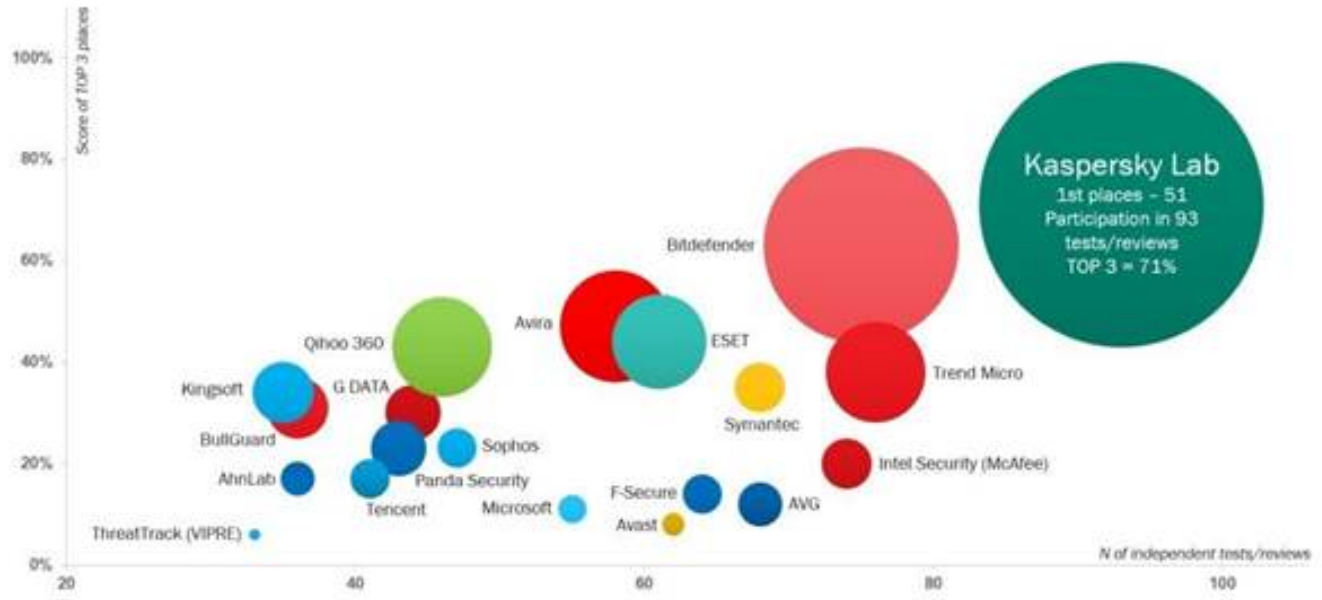

Рисунок 7. Результаты независимого тестирования антивирусного ПО

Белые списки. Использование белых списков также обеспечивает безопасность локальной сети. Белый список – это список субъектов, которым разрешен авторизованный или привилегированный доступ. Эти субъекты могут включать электронные группы или организации, привилегированные веб-сайты или даже адреса электронной почты. Белый список может также означать продвижение или признание организации, группы или отдельного лица. Иногда интернет-провайдеры используют белые списки для защиты своих клиентов. Существуют различные типы белых списков, включая коммерческие, некоммерческие, списки локальной сети (LAN), списки программ и приложений. Вместо внесения вредных веб-сайтов в черный список, белые списки считаются проактивной мерой. Белые списки используются для разрешения доступа к соответствующим и безопасным веб-сайтам, что может рассматриваться как альтернатива использованию антивирусного программного обеспечения.

Черный список является противоположностью белого списка и относится к списку организаций, которым отказано в доступе к компьютерному миру, которые подвергаются остракизму или не признаются.

Рассмотренные методы противодействия уязвимостям локальных сетей являются необходимыми мерами защиты информации. Появление новых механизмов борьбы с угрозами способствует качественному их выявлению, однако постоянно появляющиеся уязвимости требуют появления все более качественных решений.

Список литературы:

1. Защита информации в локальных сетях – [Электронный ресурс] – Режим доступа. – https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-setyakh/v-lokalnykh-vychislitelnykh-setyakh/.

2. Как защитить локальную сеть – [Электронный ресурс] – Режим доступа. – https://hd01.ru/info/kak-zashhitit-lokalnuju-set/.

3. Системы обнаружения и предотвращения вторжений – [Электронный ресурс] – Режим доступа. – https://selectel.ru/blog/ips-and-ids/.