DOI 10.36622/VSTU.2022.25.4.008
УДК 004.056

ЭШЕЛОНИРОВАННАЯ ЗАЩИТА КОРПОРАТИВНОЙ РАСПРЕДЕЛЕННОЙ СЕТИ

Ю.Ю. Громов, П.И. Карасев, А.М. Тихонов

В статье рассматривается методика защиты корпоративной распределенной сети с помощью создания эшелонированной обороны. Объясняется основной принцип эшелонирования, проводится параллель между обычной обороной и эшелонированной. Приводится методика правильного построения эшелонированной обороны, и как на неё влияет избыточность. Проводится расчет достижения эффективности при использовании технологии. В Cisco Packet Tracer была построена модель корпоративной распределенной сети, для этой сети были проработаны разные варианты защиты, включая правильно настроенную эшелонированную оборону. Были проведены опыты, результаты которых отражены в статье, доказывающие эффективность использования правильно настроенной эшелонированной защиты. Приведены минусы и плюсы технологии. Описаны методы защиты, позволяющие построить комплекс мер безопасности вместе с эшелонированной обороной сети.

Ключевые слова: эшелонированная защита, информационная безопасность, корпоративная распределенная сеть, методы защиты информации.

Введение

В настоящее время, для того чтобы быть конкурентоспособными, все больше организаций вынуждены использовать технологии ИТ. Этот технологический прогресс влияет и на количество информации, которую эти организации должны внутри себя хранить, обрабатывать, анализировать и использовать. Зачастую утечка таких данных может повлечь за собой большие финансовые и репутационные убытки для компании. С каждым годом организации хранят все больше информации, а злоумышленников становится только больше. Растет и вариативность атак этих злоумышленников, направленных на получение несанкционированного доступа внутрь организации. Для того, чтобы справляться с наибольшим количеством возможных угроз, нужны универсальные методы защиты. Одним из таких методов является эшелонированная защита сети. С помощью такого типа защиты, организация способна построить внутри сети надежную, избыточную оборону, которая будет работать достаточно быстро. Она способна задерживать атаки на разных своих уровнях (эшелонах) обороны, благодаря чему данные внутри организации не будут потеряны, украдены, искажены или недоступны.

Основная часть

Злоумышленники, которые пытаются получить несанкционированный доступ к системе и реализовать угрозу безопасности данных, делятся на два типа [1-3]:

• Злоумышленники, которые находятся во внутренней сети (рабочий персонал организации). В качестве примера, можно привести администратора сети, который намеренно поменял политику безопасности, в результате которой система стала уязвимой.

• Злоумышленники, которые находятся во внешней сети и пытаются проникнуть во внутреннюю, используя специальные методики, программное и аппаратное обеспечение. Их цель – получить несанкционированный доступ к данным, хранящимся или передающимся внутри сети. Урон от такой атаки может быть ранжирован, в зависимости от того, какие данные требовались злоумышленнику и какой уровень доступа он смог получить.

Любая атака, независимо от того организована она извне или изнутри сети, под собой несет цель повлиять на целостность, доступность или конфиденциальность информации. Для того, чтобы не дать злоумышленнику это сделать, вводятся специальные меры и методики защиты. Одна из таких методик называется эшелонированная защита сети. В этой статье

рассматривается преимущество эшелонированной защиты в сравнении с обыкновенной защитой в рамках противодействия опасному трафику, поступающему снаружи сети от злоумышленников.

Эшелонированная защита

Термин Defense in depth дословно с английского переводится как «защита в глубину». По сути, такое название и олицетворяет саму методику защиты. Появилась она во время ведения боевых действий, когда нужно было построить непреступную оборону места. Идея заключается в том, чтобы разделить имеющиеся ресурсы на несколько рубежей. Каждый из этих рубежей должен сдерживать свою часть атакующих отрядов. Например, дальним эшелоном выставляются противотанковые ежи, ближним – колючая проволока. Во время атаки противника дальний рубеж танки проехать не смогут, до следующего рубежа смогут дойти только пехотинцы. Но и они не смогут преодолеть следующий эшелон – колючую проволоку [4].

Отойдя от военной тематики, рассмотрим эшелонированную защиту корпоративной распределенной сети. Итак, в организацию поступает большое количество различного трафика. Причем траффик может быть как полезным, так и опасным для этой организации. Естественно, этот трафик необходимо фильтровать, в зависимости от его допустимости. В сети организации может стоять демилитаризованная зона (ДМЗ), в которую может поступать допустимый для нее и не допустимый для внутренней сети трафик. Таким образом, правила защиты должны быть разделены для внутренней сети и демилитаризованной зоны. Предположим, что у нас стоят два межсетевых экрана (МЭ) – между внутренней сетью и ДМЗ, и между ДМЗ и внешней сетью. Теперь предположим, что организации требуется обработка большого потока данных, поступающих из сети. При этом, в организации установлен крупный список запрещенных к использованию протоколов, чтобы фильтровать внешний трафик. Значительную часть этих протоколов должен отбивать МЭ, расположенный между ДМЗ и внешней сетью. Чем больше список правил, по которым проверяется каждый пакет, направленный из внешней сети, тем дольше он будет обрабатываться фаерволом. В таком случае, если направить внутрь сети значительный поток (на который не был рассчитан МЭ), состоящий из полезного и вредного трафика, то МЭ перестанет обрабатывать его с необходимой скоростью. В результате, очередь из пакетов для обработки будет увеличиваться до тех пор, пока не переполнится, что приведет к неработоспособности сети. Избежать такого переполнения или хотя бы улучшить ситуацию можно, если этот список правил разделить на несколько МЭ.

Основной идеей эшелонированной обороны корпоративной распределенной сети является разделение имеющихся правил на несколько межсетевых экранов. Чтобы правильно построить такую оборону, организация должна проанализировать свой сетевой трафик, который поступает внутрь сети. Из этого трафика необходимо вычленить наиболее часто встречающиеся протоколы, которые необходимо заблокировать. Из блокировок этих протоколов нужно будет выстраивать самые дальние рубежи защиты. Причем, самый дальний рубеж должен быть построен по следующему принципу – он должен содержать наименьший список правил с наиболее часто встречающимися угрозами для сети. Закон Парето, как правило, применим для построения эшелонированной защиты – около 80% всего опасного трафика будут отбиты на дальнем рубеже с наименьшим списком правил фильтрации. За счет короткого списка, пакеты будут обрабатываться быстро и передаваться следующему узлу внутри сети, либо блокироваться, такой межсетевой экран будет гораздо сложнее «повесить» избытком трафика [5].

Каждый следующий уровень эшелонированной защиты должен содержать больший набор правил. Чем ближе уровень защиты к внутренней сети, тем правила должны блокировать менее популярные протоколы для атак. Таким образом, самый ближний эшелон должен содержать самый

большой набор правил, который блокирует самые редкие типы атак.

В случае использования ДМЗ в организации, можно построить два эшелонированных защиты – до ДМЗ и после. Дело в том, что если не использовать МЭ между внутренней сетью и ДМЗ и блокировать все потенциально опасные для внутренней сети протоколы между ДМЗ и внешней сетью, то внешние пользователи, у которых должен быть доступ к ДМЗ (например, чтобы зайти на сайт организации), будут заблокированы. Есть и обратная сторона медали – пытаться блокировать все опасное после ДМЗ. В таком случае, злоумышленник сможет получить несанкционированный доступ к ДМЗ и оттуда попытаться войти во внутреннюю сеть, что тоже является плохим вариантом. Если отказаться от ДМЗ и сервера из этой зоны перевести во внутреннюю сеть, с возможностью доступа к ним извне, то внутренняя сеть перестанет быть защищенной, тоже плохой вариант. Поэтому надо тщательно прорабатывать список ограничивающих правил, которые будут располагаться до и после ДМЗ.

Чтобы эшелонированная защита была надежна – нужно составить полный список правил, которые способны защитить сеть от атак, а также правильно распределить этот список по МЭ. Для того, чтобы защита была избыточна, нужно использовать каждое правило по одному разу. Повторение правил не повлияет на качество защиты, но замедлит работу сети [6-7].

Нужно учитывать, что внутренние пользователи могут иметь ограниченный набор протоколов для использования. Поэтому на межсетевых экранах можно настроить набор правил, ограничивающий исходящий из внутренней сети трафик. Этот набор правил можно распределить по тому же принципу, по которому был распределен набор правил для внешнего трафика.

С помощью приведенной выше методики можно защитить сеть от внешних атак и ограничить трафик, исходящий из внутренней сети. Но эта методика не защитит саму внутреннюю сеть от вторжений, не предоставит мониторинг и активный анализ инцидентов сети. Поэтому методику эшелонированной системы защиты необходимо объединять с другим комплексом мер по информационной безопасности. Например, на каждом компьютере внутри сети должны стоять антивирусы и использоваться только актуальное проверенное ПО, которое не содержит в себе опасностей для работы организации. Все специалисты организации должны быть проинформированы о различных вариантах атак (например, фишинговые письма) и понимать, как действовать в случае опасности. Внутри организации должны стоять надежные средства для мониторинга и анализа трафика, с которыми должны работать квалифицированные специалисты. Доступ к данным должен быть предоставлен только тем лицам, которые имеют на это право, остальные не должны иметь доступа. Представители информационной безопасности компании должны ввести комплекс мер, чтобы гости организации не могли получить доступ к внутренней сети. Чтобы сохранить важную информацию, должны быть правильно спроектированы ханипоты. И прочие меры безопасности.

Основным принципом безопасности является то, что информация, которую необходимо защитить, должна стоить дороже, чем её защита. В противном случае её защита не имеет смысла. Построение эшелонированной защиты – не дешевая история. Для защиты сети используется больше аппаратных устройств, каждое из которых нужно отдельно настраивать и поддерживать, причем сделать это сможет только квалифицированный персонал. Помимо затрат на поддержку и закупку, нужно учитывать, что разработка самой концепции защиты и начальный анализ трафика также будут стоить денег и времени. Поэтому, если речь идет об эшелонированной защите, то её применение подойдет скорее для организаций среднего и крупного размеров.

Опытная часть

Для того, чтобы доказать эффективность технологии эшелонированной защиты, в программе Cisco Packet Tracer была создана модель корпоративной распределенной сети

для организации, у которой есть три офисных здания, расположенных близко друг от друга.

Все офисы соединены в единую внутреннюю распределенную сеть (рис. 1). В каждом офисе стоит маршрутизатор, маршрутизаторы офисов соединены друг с другом и с маршрутизатором-ядром. Этот маршрутизатор соединен двойной связью с коммутатором зоны ДМЗ (рис. 2). Также он может выступать в роли межсетевого экрана, чтобы фильтровать поток данных, который поступает внутрь сети. Коммутатор соединен с роутером – эшелоном, на котором выставлен список правил для фильтрации. По счету это последний рубеж защиты перед зоной ДМЗ, этот маршрутизатор представляет собой также межсетевой экран, который содержит наибольший список правил фильтрации (рис. 3). С этим роутером соединен следующий эшелон защиты – такой же роутер/МЭ, но уже с меньшим списком правил. Следующие рубежи идут друг за другом, на каждом из них установлен свой список правил. Самый дальний эшелон соединен с провайдером, который предоставляет доступ в интернет. К провайдеру подключены компьютеры и сервер внешней сети. Один из компьютеров является для внутренней сети доверительным, чтобы можно было проверить скорость её работы [8].

В нашем случае, правила между эшелонами были распределены в соответствии с моделью OSI, то есть каждый уровень отвечал за охрану протоколов, работающих на том или ином уровне. С учетом уровней защиты модели OSI, ограничивающие правила были распределены следующим образом:

- 1 эшелон (сетевой уровень): ICMP и IP для 200.200.51.2 и для 200.200.51.3;
- 2 эшелон (транспортный уровень): TELNET TCP, FTP TCP, SSH TCP, SNMP UDP, TFTP UDP;
- 3 эшелон (уровень приложений): POP3 TCP, SMTP TCP, DOMAIN TCP/UDP;
- 4 эшелон (сеансовый уровень): isakmp, non500-isakmp, 1701, 1723, 1194, 1721, 135, 593, 445;
- 5 эшелон (различные порты): whoami 565/TCP+UDP, dhcp 546-7/TCP+UDP, syslog 514/UDP, shell 514/TCP, who 513/UDP, dcp 93/TCP+UDP, whoispp 63/TCP+UDP, rap 56/TCP+UDP, route access protocol 38/TCP+UDP, rlp 39/TCP+UDP, systat 11/TCP+UDP, discard 9/TCP+UDP, daytime 13/TCP+UDP, whois 43/TCP+UDP, chargen 19/TCP+UDP.

Для организации приоритезация угроз может меняться, поэтому необходимо провести изначальный анализ угроз извне и далее дорабатывать систему защиты в соответствии с изменениями приоритетов угроз. Например, эшелонов может быть не пять, а три, список ограничений может быть разделен не по уровням модели OSI, а смешано, чтобы достичь наибольшего КПД работы сети, список правил может использоваться больший или меньший.

Комплекс мер защиты, предполагаемый в данной модели, не ограничивается эшелонами на межсетевом экране. Были применены и другие подходы к организации защиты, в том числе и описанные выше, а именно:

- Защита на коммутаторах. Чтобы к коммутаторам не могли подключиться нежелательные пользователи, были отключены неиспользуемые порты. В случае появления нового участника сети, сетевой администратор открывает порт для него.
- Защита на маршрутизаторах. Аналогично, отключение неиспользуемых портов.
- Защита от перегрузки сети. Все маршрутизаторы связаны друг с другом с помощью Gigabit Ethernet, что позволит быстро передавать информацию.
- Защита от долгого восстановления после сбоя. Метод работы коммутатора был изменен на RSTP для быстрой перезагрузки портов, что позволяет быстро подключать новые порты и возобновлять имеющиеся подключения.
- Защита от вирусов. Каждый пользователь в сети имеет надежное антивирусное ПО, работающее в режиме реального времени.
- Защита от уязвимостей. Все программное обеспечение должно иметь актуальные версии.

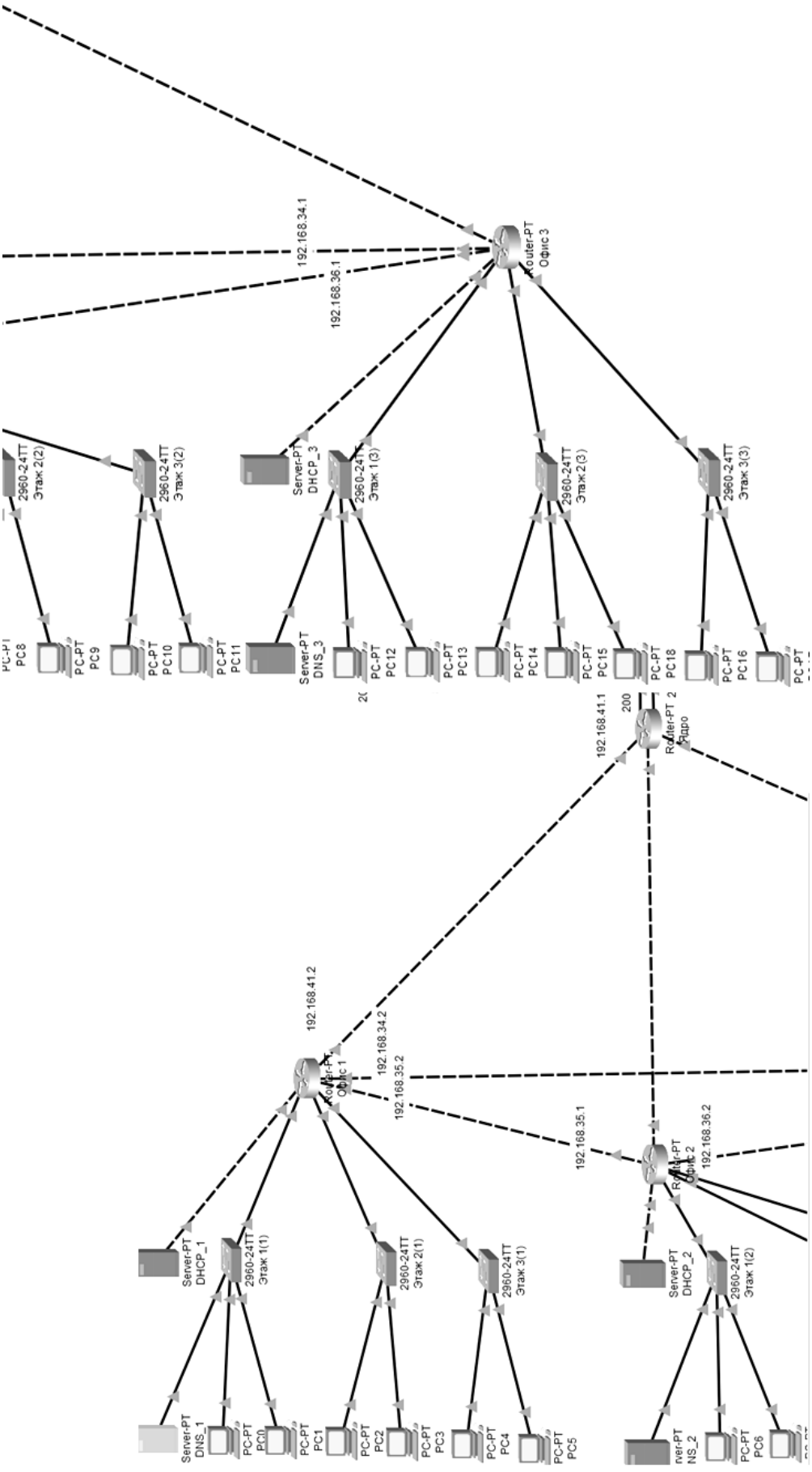

Рис. 1. Внутренняя корпоративная распределенная сеть

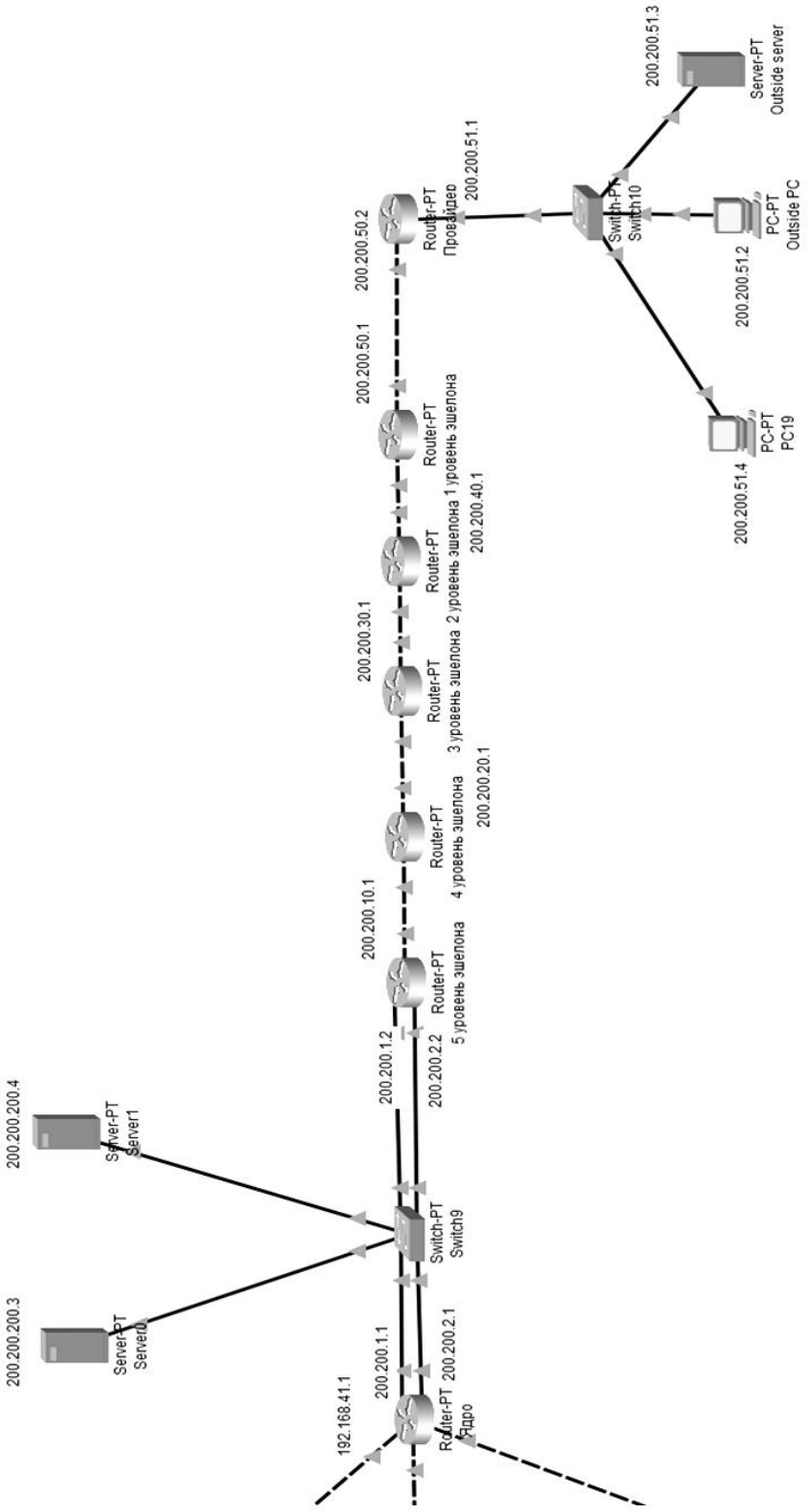

Рис. 2. Зона ДМЗ, эшелоны, внешняя сеть

• Защита от превышения полномочий сотрудниками. Разграничены доступы внутри сети. Пользователи, которые не должны иметь права доступа к закрытым для них данным и сегментам сети, его не имеют. Доступ ограничен с помощью сетевых администраторов.

• Защита от уязвимостей, возникших в результате действий пользователей. Сотрудникам проведено обучение по безопасности, проведены контрольные тесты, подтверждающие их готовность противодействовать атакам.

• Защита на провайдере. Провайдер фильтрует весь опасный трафик, который передает в организацию, список опасных IP адресов был согласован сотрудниками организации и провайдером.

• Защита от несанкционированных действий. Внедрен комплекс программных и аппаратных мер, позволяющий отслеживать работу сети в режиме онлайн, находить, анализировать и блокировать опасный трафик.

• Защита ДМЗ. ДМЗ выделена в качестве отдельной сети. Все сервисы, которые подключаются из внешней сети – подключаются к ДМЗ. До и после ДМЗ стоят межсетевые экраны.

Чтобы провести сравнение правильно настроенной эшелонированной системы защиты, были дополнительно настроены еще три модели:

• с защитой в виде одного эшелона, на которой присутствует весь список правил;

• с защитой в виде пяти эшелонов, на каждом из которых присутствует весь список правил;

• без защиты.

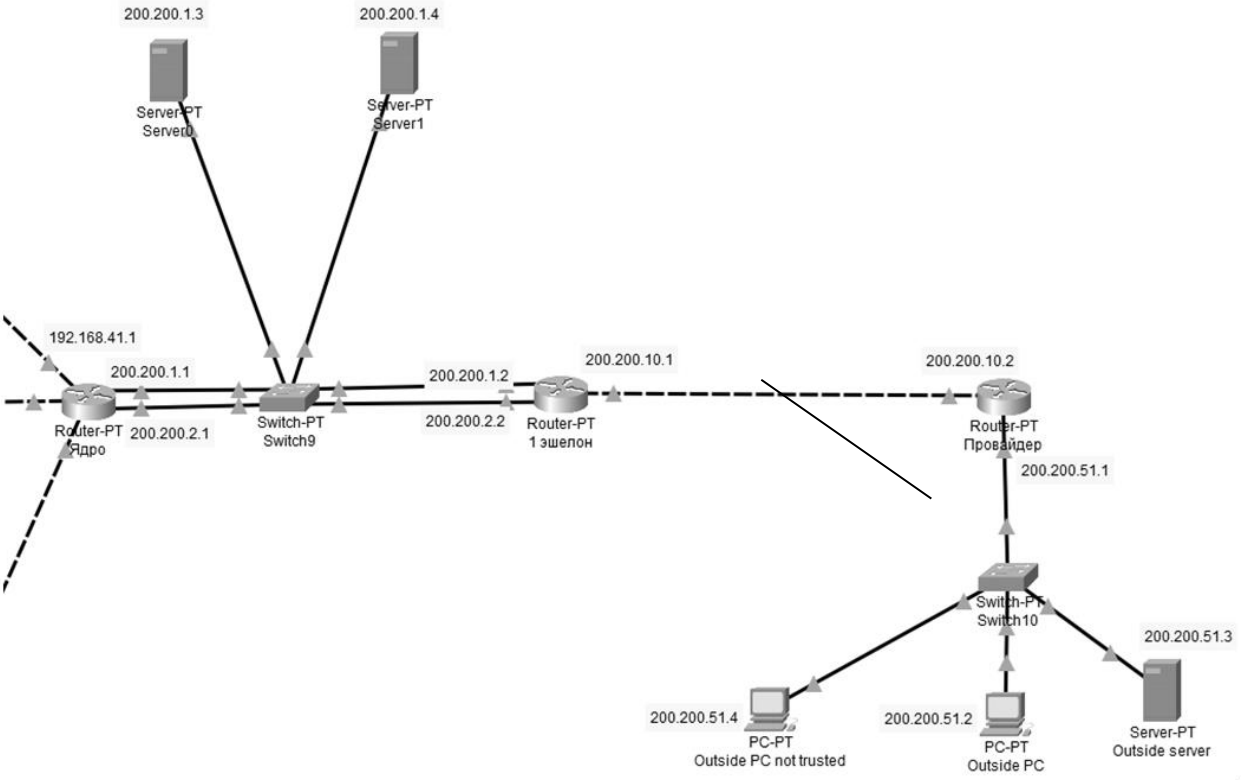

Рис. 3. Защита с одним МЭ

Были проведены следующие опыты. Из доверительного компьютера, который находится во внешней сети, были отправлены пакеты типа ICMP во внутреннюю сеть, на компьютер PC6 во втором офисе. Во время каждого опыта было отправлено по 100 пакетов, которые имели одинаковый размер. Компьютер из внешней сети знал путь до компьютера во внутренней сети, обмен ARP был проведен заранее. Для каждой модели проводился один опыт.

По результатам (табл. 1), быстрее всех работает незащищенная сеть. На следующем месте сеть с эшелонированной правильно настроенной защитой. Далее сеть с одним межсетевым экраном, а хуже всех отработала сеть с пятью эшелонами и неправильной, дублирующей настройкой.

Если проводить такой же тест в полевых условиях, добавив еще одну модель – эшелонированная сеть с неправильно распределенными (но не дублирующими) правилами, то результат будет следующим. Быстрее всех будет работать сеть без защиты, на следующем месте либо сеть с одним межсетевым экраном, либо сеть с пятью эшелонами (в зависимости от нагрузки на сеть), далее сеть с неправильно распределенным списком правил на эшелонах и завершит сеть с дублирующими

правилами на эшелонах. Если в эшелонированной сети правила были настроены близко к оптимальному, то она может быть лучше защиты с одним межсетевым экраном по скорости (в зависимости от нагрузки на сеть). С точки зрения надежности, лучшим вариантом из предложенных моделей будет эшелонированная защита с правильно настроенными эшелонами [9-10].

Таблица 1

Результаты скорости работы разных систем защиты

	5 эшелонов, правильная настройка	5 эшелонов, дублирующая настройка	1 эшелон	Без защиты
Минимум (мс)	0	0	0	0
Максимум (мс)	2	8	6	1
Среднее (мс)	0	1	0	0

Опыт продемонстрировал, что многократное использование одних и тех же правил негативно сказывается на скорости работы сети. Оптимально использовать только необходимые правила однократно и правильно их распределять.

Основная функция у эшелонированной защиты – безотказно и быстро работать, правильно фильтруя пакеты и обеспечивать защиту организации от угроз. Чтобы доказать работоспособность такой методики, был проведен опыт (рис. 4, 5). Для наглядности, вместо первого эшелона, правило с блокировкой ICMP было перенесено на четвертый эшелон. Из не доверительного компьютера, находящегося во внешней сети, был отправлен пакет ICMP во внутреннюю сеть. В результате чего четвертый эшелон, который отвечает за остановку вредоносного трафика ICMP, не пропустил дальше опасный пакет (рис. 5). При этом, все предыдущие эшелоны этот пакет пропустили, что говорит о правильной работе защиты и её способности бороться с вредоносным трафиком.

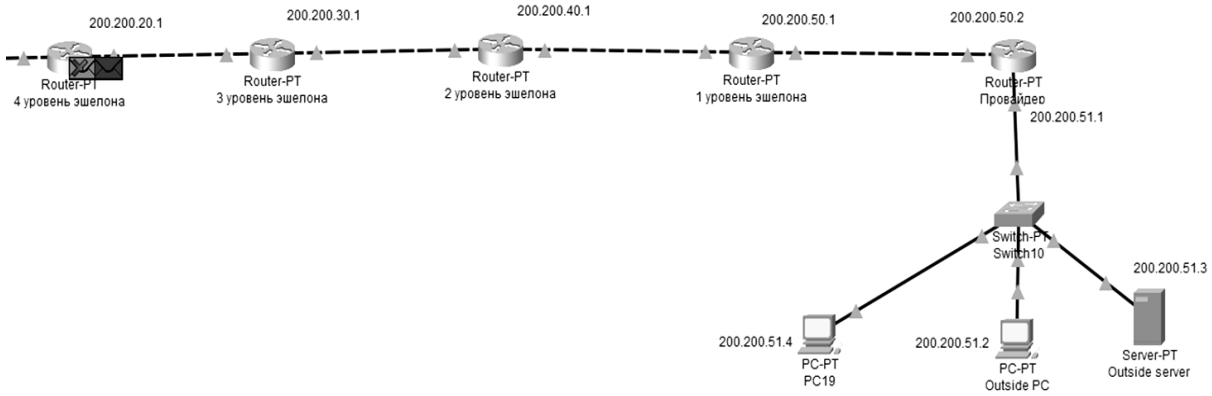

Рис. 4. Отработка эшелонированной системы защиты

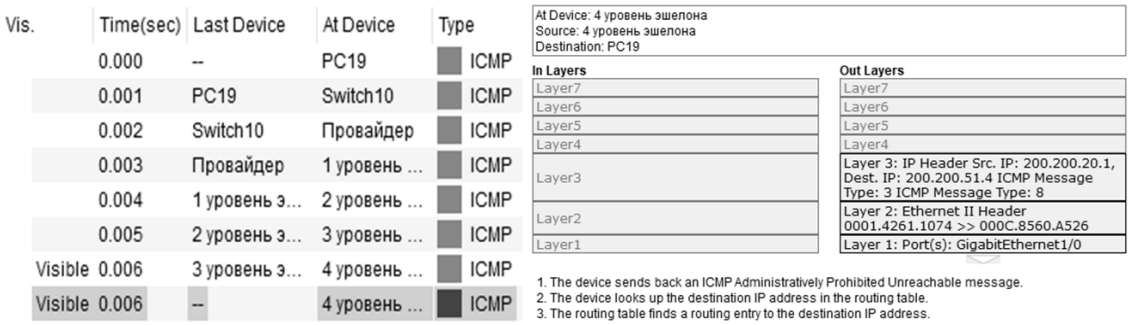

Рис. 5. Остановка вредоносного пакета

Заключение

Ежегодно количество информации, хранящееся и обрабатываемое организациями, увеличивается. Увеличивается и количество угроз, с которыми приходится бороться организациям. Для средних и больших существует вариант построения эшелонированной защиты для корпоративной сети. Эта защита имеет свои плюсы, связанные с надежностью и скоростью работы, а также свои минусы, связанные со стоимостью. Эшелонированная защита способна справляться с большим количеством разнообразных угроз, благодаря чему является хорошим вариантом для обеспечения защиты организации. В то же время нужно понимать, что хорошая защита достигается только с помощью комплекса мер, связанных с безопасностью. Если правильно настроить эшелонированную оборону на надежном оборудовании, предварительно проведя анализ угроз, докупить комплексы для мониторинга, анализа и защиты внутренней сети, ввести необходимый комплекс мер по безопасности и правильно обучить персонал работе с угрозами и атаками, то в итоге можно получить хорошо защищённую сеть. Информация, хранящаяся в такой сети, будет доступной, конфиденциальной, актуальной и целостной.

Список литературы

1. Баранова, Е.К. Информационная безопасность и защита информации / Е.К. Баранова. М.: РИОР, 2018. 165 с.

2. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.

3. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. М.: Инфра-М, 2018. 160 с.

4. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. М.: Форум, 2018. 256 с.

5. Яникеева И.О. — Перспективные направления развития и углубления международного взаимодействия по проблематике международной информационной безопасности // Мировая политика. 2022. № 1. С. 23 - 34.

6. Луков Д.К. Автоматизированные системы управления технологическим процессом (АСУ ТП) // European science. 2019. № 2(44). С. 19-21.

7. Королев, А.И. Выявление внутренних нарушителей информационной безопасности в организациях на основе методов машинного обучения / А.И. Королев, М.А. Поляничко // Региональная информатика и информационная безопасность : Сборник трудов, Санкт-Петербург, 23–25 октября 2019 года. СПб: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2019. С. 88-91.

8. Чернов, Д. В. Формализация модели нарушителя информационной безопасности АСУ ТП / Д. В. Чернов, А. А. Сычугов // Известия Тульского государственного университета. Технические науки. 2018. № 10. С. 22-27.

9. Сычев В.М. Формализация модели внутреннего нарушителя информационной безопасности // Вестник Московского государственного технического университета им. Н. Э. Баумана. Сер. Приборостроение. 2015. № 2. С. 92-106.

10. Zaytsev, A. S. Information security insider threat visualization: theft of intellectual property / A. S. Zaytsev, A. A. Malyuk // Scientific Visualization. 2015. Vol. 7. No 3. P. 53-68.

Тамбовский государственный технический университет
Tambov State Technical University

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 16.11.2022

Информация об авторах

Громов Юрий Юрьевич – д-р техн. наук, профессор, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru

Карасев Павел Игоревич – канд. техн. наук, МИРЭА – Российский технологический университет, e-mail: karasev@mirea.ru

Тихонов Александр Михайлович – студент, МИРЭА – Российский технологический университет, e-mail: silverkingi@mail.ru

DEPENDENT PROTECTION OF THE CORPORATE DISTRIBUTED NETWORK

Y.Y. Gromov, P.I. Karasev, A. M. Tichonov

The article discusses the method of protecting a corporate distributed network by creating a layered defense. The basic principle of separation is explained, a parallel is drawn between conventional and echeloned defense. The methodology of the correct construction of echeloned defense is given, and how redundancy affects it. The calculation of achieving efficiency when using the technology is carried out. In Cisco Packet Tracer, a model of a corporate distributed network was built, various protection options were worked out for this network, including properly configured layered defense. Experiments were conducted, the results of which are reflected in the article, proving the effectiveness of using properly configured layered protection. The cons and pros of the technology are given.

The methods of protection that allow to build a set of security measures together with the layered defense of the network are described.

Keywords: layered protection, information security, corporate distributed network, methods of information protection.

Submitted 16.11.2022

Information about the authors

Yurii Y. Gromov – Dr. Sc. (Technical), Professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru

Pavel I. Karasev – Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru

Alexander M. Tichonov – student, MIREA – Russian Technological University, e-mail: silverkingi@mail.ru