МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Кафедра Телекоммуникационных сетей и систем

«Допущен к защите»
Зав.кафедрой Темырканова Э.К., доктор PhD, доц.
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Моделирование и анализ защищенности локальной сети с использованием программы Skybox

Специальность 5В071900 – Радиотехника, электроника и телекоммуникации

Выполнила Низамов Б. К. **Группа** РЭТз-16-1

Научный руководитель Чайко Е.В.PhD, профессор
(Ф.И.О., ученая степень, звание)

Консультанты
по технической части:
Ползик Е.В., доцент
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

по экономической части:
Ибришев Н.Н., д.э.н., профессор
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

по безопасности жизнедеятельности:
Бекбасаров Ш.Ш., д.т.н
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

по применению вычислительной техники:
Ползик Е.В., доцент
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

Нормоконтролер: Гармашова Ю.М., доц.
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

Рецензент: _____
(Ф.И.О., ученая степень, звание)
_____«____» _____2020 г.
(подпись)

Алматы 2020 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Космической инженерии и телекоммуникаций (ИКИТК)
Кафедра Телекоммуникационных сетей и систем
Специальность 5В071900 – Радиотехника, электроника и телекоммуникаций

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Низамов Бахтишату Канжахуновичу
Тема проекта «Моделирование и анализ защищенности локальной сети с использованием программы SkyBox»

Утверждена приказом ректора № 06 от «16» __января___ 2020 г.

Срок сдачи законченного проекта «25» _____мая____ 2020 г.

Исходные данные к проекту требуемые параметры результатов проектирования (исследования) и исходные данные объекта: Необходимо изучить и проанализировать сеть на основе выданных конфигурационных файлов сетевых устройств в банке 2 уровня. В главном офисе работают 618 человек 15 из которых являются сотрудниками ИТ и ИБ отдела. Каждый сотрудник ИТ и ИБ отдела обеспечен настольным ПК Intel Core i7 6700T, NVIDIA GeForce GTX960M, 16Gb DDR4, 1 Tb HHD, 128 Gb SSD, Gigabit Ethernet. Так же глав. офис оснащен 13 коммутаторами CISCO модели SX350X-12-K9 и SRW2016, 2 маршрутизатора Cisco 2951-SEC VPN и Cisco 1921/K9, 4 межсетевых экрана Palo Alto 5260, Palo Alto 5250

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта:
Понятие локальной сети
Описание сети
О программе и моделирование
Методы защиты для конкретно выбранной сети
Расчет эффективности сетевой защиты
Безопасность жизнедеятельности
Анализ условий труда внутри предприятия.
Финансовый план
Расчет капитальных вложений

Перечень графического материала (с точным указанием обязательных чертежей): Стандартная проводная и беспроводная корпоративная сеть
Пример передвижения фрейма по каналам Ethernet разных типов
Схема начала атакующих действий ;
Вектор атак ;
Схема архитектуры решения;
Настройка времени анализа;
Информация Firewall Assurance;
Access Compliance (соответствие стандартам);
Rule Compliance (неправильно настроенные правила);
Карта сети банка

Основная рекомендуемая литература:

1 Бирюков А. Информационная безопасность: защита и нападение. 2-е издание, ДМК-Пресс, 2017, 434 с.

2 Орлов, Л. В. Как создать защиту в сети. / Л. В. Орлов – изд. Бук-Пресс: Москва, 2016, – 384 с.

3 Бондарев В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства, МГТУ им. Н. Э. Баумана, 2017, -228 с.

4 Информационная безопасность и защита информации. Учебное пособие – М.: 2004 – 82 с.

5 Инструкция по установке и настройки системы Skybox (Reference Guide).

6 Холмогоров, В. Уязвимости в сети / В. Холмогоров. – СПб.: Питер, 2012. – 272 с.

7 Орлов, Л. В. Как создать защиту в сети. / Л. В. Орлов – изд. Бук-Пресс: Москва, 2016, – 384 с.

8 www.cisco.com (дата посещения 20.04.2020г)

Консультанты по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Техническая часть	Ползик Е.В.	25.05.2020 г.	
Экономическая часть	Ибришев Н.Н	25.05.2020 г.	
Безопасность жизнедеятельности	Бекбасаров Ш. Ш	25.05.2020 г.	
Применение вычислительной техники	Ползик Е.В.	25.05.2020 г.	
Нормоконтроль	Гармашова Ю.М.	28-30.05.2020 г.	

График
подготовки дипломного проекта

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1	Понятие локальной сети	13.01.20-15.02.2020	
2	Стандартная корпоративная локальная сеть	25.01.20-30.01.20	
3	Описание сети	02.02.20-20.02.2020	
4	Активное оборудование	22.02.20-01.03.2020	
5	Необходимость защиты	02.03.20-01.04.20	
6	О программе и моделирование	02.04.20-20.04.20	
7	Расчеты	21.04.20-30.04.20	
8	Методы защиты для конкретно выбранной сети	30.04.20-10.05.20	
9	Оценка защищенности при помощи рисков	10.05.20-18.05.20	
10	Безопасность жизнедеятельности	19.05.20-22.05.20	
11	Разработка эвакуационных путей	22.05.20-23.05.20	
12	Финансовый план	24.05.20-25.05.20	

Дата выдачи задания «13» января 2020 г.

Заведующий кафедрой _____ (подпись) (Темырканова Э.К.) (Ф.И.О.)

Научный руководитель проекта _____ (подпись) (Чайко Е.В.PhD) (Ф.И.О.)

Задание принял к исполнению студент _____ (подпись) (Низамов Б.К.) (Ф.И.О.)

Аңдатпа

Бұл дипломдық жобада Skybox жүйесін қолдану арқылы желіні талдау және модельдеу жұмыстары сипатталған. Негізгі бөлімде барлық желілік және желілік құрылғылар техникалық сипаттамаларға сәйкес зерттелді. Желі дұрыс конфигурация мен осалдықты анықтау үшін талданды. Экономикалық бөлімде жалпы күрделі шығындар, пайдалану шығындары және жобаны жүзеге асыру мерзімі анықталады. Қауіпсіз өмір бөлімінде жұмысшыларды эвакуациялау жолдары және өрт қауіпсіздігі туралы ақпарат, сонымен қатар көмірқышқыл газы мен фреон құрамын тұтыну және оператордың жұмыс орнын ұтымды ұйымдастыру туралы мәліметтер келтірілген.

Аннотация

В данной дипломной работе описывается работа по анализу и моделированию сети с помощью системы Skybox. В основной части было исследована вся сеть и сетевые устройства вплоть до технических характеристик. Сеть была подвергнута анализу на правильное конфигурирование и обнаружение уязвимостей. В экономической части определены общие капитальные расходы, эксплуатационные расходы и сроки реализации проекта. В разделе безопасности жизнедеятельности рассчитаны пути для эвакуации работников и сведения о пожаробезопасности, а также расход углекислотно-хладонового состава и рациональная организация рабочего места оператора.

Annotation

In this graduation project describes the work on the analysis and modeling of the network using the Skybox system. In the main part, the entire network and network devices were investigated up to the technical characteristics. The network was analyzed for proper configuration and vulnerability detection. In the economic part, the total capital expenditures, operating expenses and the terms of the project implementation are determined. In the section of life safety, ways for the evacuation of workers and information about fire safety are calculated, as well as the consumption of carbon dioxide and freon composition and the rational organization of the operator’s workplace.

Содержание

Введение

Обеспечение безопасности в компьютерных сетях – это основное условие защиты конфиденциальных данных от разного рода угроз, таких как шпионаж, уничтожение файлов и прочие несанкционированные действия. Каждый из перечисленных факторов может негативно повлиять на корректное функционирование локальной и глобальной сети, что, в свою очередь, нередко приводит к разглашению или утрате конфиденциальной информации.

Одной из распространенных сетевых угроз является несанкционированный доступ извне, причем не только умышленный, но и случайный. Также в данном случае велик риск доступа к информации, составляющей врачебную, коммерческую, банковскую или государственную тайну.

Следующая неприятность, с которой нередко встречаются пользователи во всем мире – это различные сбои в работе программного обеспечения, в том числе и спровоцированные вирусами, заражающими систему в момент выхода в интернет.

Анализ угроз, оценка возможного ущерба от неправильной настройки и выбора системы защиты.

Выбор наилучшей системы защиты по результатам анализа работы сети и моделирования сети в программе Skybox основные вопросы данного дипломного проекта.

1 Понятие локальной сети

Почти каждая корпоративная сеть компьютерных устройств состоит из двух технологических частей:

- локальной, LAN (Local-Area Network);
- распределительной, WAN (Wide-Area Network).

К локальной сети подключаются соседние компьютеры, расположенные в одном помещении, строении, в пределах одного территориального участка. Устройства, находящиеся на дальнем расстоянии друг от друга, объединяет глобальная сеть. Совмещение локальной и глобальной сетей образовывает общую корпоративную систему, направленную на решение главной сетевой задачи – обмен информацией между компьютерными устройствами.

За годы всеобщей компьютеризации было создано много вариантов сетей локального типа. Однако сегодня принято использовать только 2 варианта из них – Ethernet и беспроводные линии. В первых для соединения узлов применяют кабели, состоящие из медных проводов. Отсюда возникло определение «проводная локальная сеть» – wired LAN. Вторые не применяют кабели с проводами, поскольку соединение между узлами обеспечивается радиоволнами.

1.1 Классификация локальных сетей

Понятие Ethernet принадлежит к стандартам, совокупно определяющим уровни (канальные, материальные) проводной связи LAN, пользующейся большой мировой популярностью. Данные стандарты, разработанные в Институте инженеров по электротехнике и электронике (lnstitute of Electrical and Electronics Engineers - IEEE), регулируют правила соединения кабелей и разъемов на их окончаниях, порядок написания протоколов и проч. – все, что необходимо для установки и функционирования LAN Ethernet.

1.1.1 Стандартная домашняя LAN. Наиболее простой вариант LAN-сети Ethernet-технологии применяется в малом либо домашнем офисе (Small Office Hoте Office – SOHO). Для работоспособности системы передачи данных необходим, в первую очередь, коммутатор локальных сетей (LAN-switch), который имеет некоторое количество портов для кабельного соединения. В указанной выше технологии применяются любые кабели (Ethernet cable), подходящие под любой Ethernet-стандарт. В локальных сетях с помощью стандартных кабелей происходит подключение всевозможных устройств и узлов к порту стандартизованного коммутатора.

На рисунке 1.1 приведена схема стандартной малой домашней сети Ethernet. Здесь имеется 1 коммутатор локальной сети, 5 кабелей, 5 узлов – 3 компьютера, 1 принтер, 1 маршрутизатор (сетевое устройство). Последний является соединительным устройством между локальной и глобальной сетями (в данном случае – с всемирной сетью интернет).

И хотя средства коммутации и маршрутизации на изображении выше представлены отдельными устройствами, в наши дни эти функции выполняет

Рисунок 1.1- Пример малой домашней сети только на стандартах Ethernet

один сетевой узел. Устройства, объединяющие функции маршрутизатора и коммутатора стандарта Ethemet, пользуются популярностью у широкого круга потребителей. Несмотря на то, что упаковка данного вида товара позиционирует его как средство маршрутизации, большая часть моделей оснащена коммутатором локальных сетей с 4-9-ю портами.

Технология Ethernet подразумевает в локальных сетях только проводное соединение, с помощью кабелей. Однако современная домашняя сеть способна поддерживать и беспроводную связь. Поэтому в настоящее время выстраивают локальные сети, в которых одновременно применяется и проводная (Ethernet), и беспроводная (IEEE) технология. Это стало возможным после выхода стандарта IEEE 802.11 для сетей Wi-Fi, использующего радиоволны для передачи данных между узлами.

В большинстве локальных сетей, передающих информацию через радиоволны, существует беспроводная точка доступа (Access Point – AP). Ее функции аналогичны функциям коммутатора, который предоставляет всем беспроводным устройствам локальной сети соединяться с Ethemet-коммутатором для получения и передачи информации. Разумеется, отсутствие проводов предполагает и отсутствие множества портов Ethemet, кроме единственного – для соединения точки доступа с локальной сетью (см. рисунок 1.2).

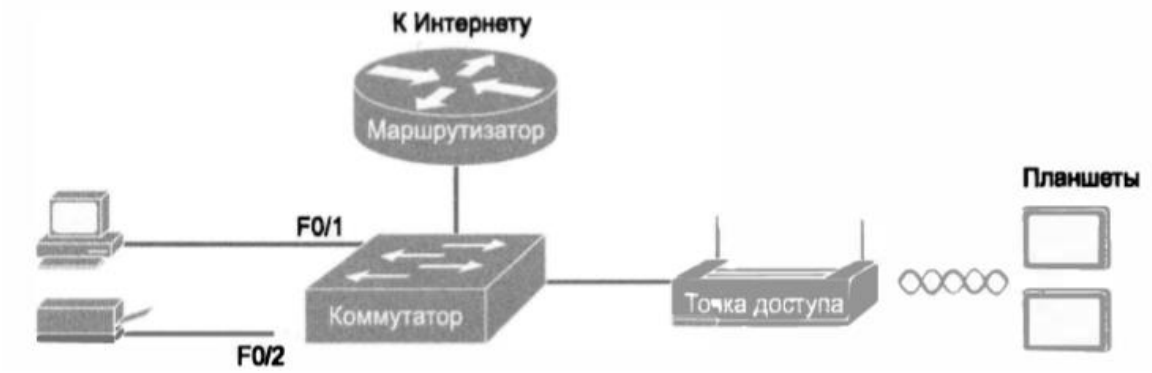


Рисунок 1.2 - Стандартная домашняя сеть, объединяющая проводное и беспроводное соединение

На рисунке 1.2 средства доступа, коммутации и маршрутизации представлены в виде отдельных устройств, для лучшего понимания их функционала. Однако большинство современных сетей малого или домашнего офиса используют единственное устройство, объединяющее данные функции – беспроводной маршрутизатор.

1.1.2 Стандартная корпоративная локальная сеть. Потребности корпоративной сети отличаются от потребностей малой или домашней лишь масштабами – у корпоративной они глобальнее. К примеру, отправной точкой типовой корпоративной LAN стандарта Ethernet являются коммутационные узлы. Они находятся на каждом этаже строения, в кабельных стволах, под замком. От данных узлов прокладываются Ethernet-кабели до комнат и помещений с устройствами, требующими подключения к локальной сети. В то же время современные учреждения и компании поддерживают беспроводное соединение, позволяющее сотрудникам не быть привязанным к рабочему месту, а свободно пользоваться сетью, перемещаясь в пределах доступа.

На рисунке 1.3 представлена концепция стандартной корпоративной локальной сети, установленной в строении из 3-х этажей. Каждый этаж здания оснащен Ethernet-коммутатором и беспроводной точкой доступа. Соединение между этажами обеспечивает подключение этажных коммутаторов к центральной коммутаторной станции. К примеру, устройство PC3 (3-й этаж) отправило данные устройству PC2 (2-й этаж). При этом отправленная информация прошла следующий путь: устройство PC3 (3-й эт.) – коммутатор SW3 (3-й эт.) – общий коммутатор SWD (1-й эт.) – коммутатор SW2 (2-й эт.) – устройство PC2 (2-й эт.)

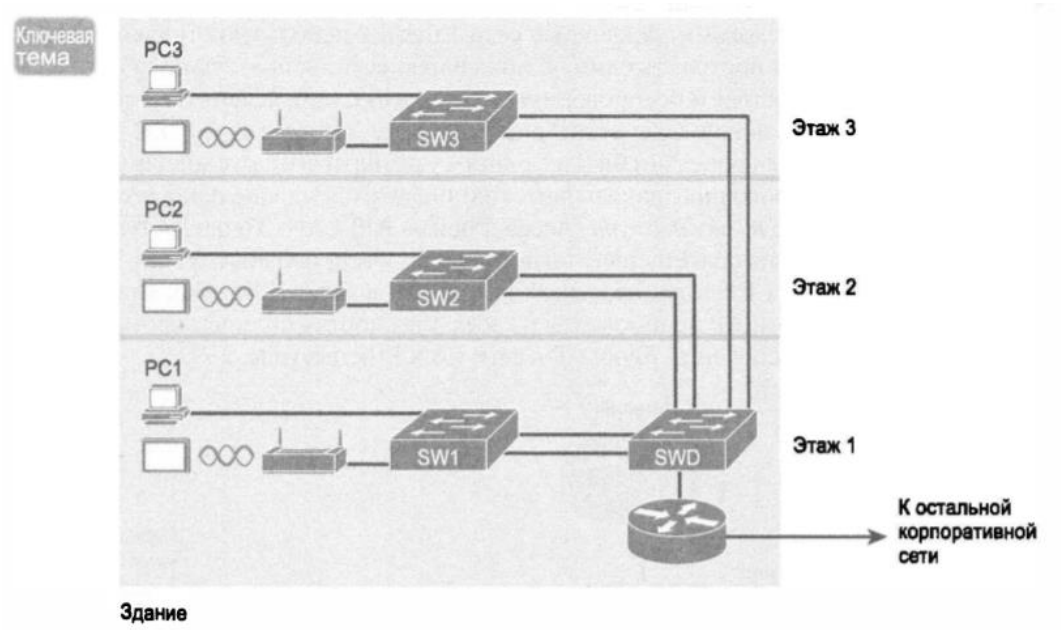


Рисунок 1.3 - Стандартная проводная и беспроводная корпоративная сеть

На рисунке 1.3 наглядно представлен стандартный метод

присоединения локальной сети LAN к глобальной сети WAN с помощью маршрутизатора, подключенного к обеим сетям. Локальную сеть создают устройства коммутации и беспроводных точек доступа. Маршрутизатор, при подсоединении к локальной сети, использует набор средств технологии Ethernet и соответствующий ей кабель. В дальнейшей части главы технология Ethernet будет рассмотрена более детально.

Многообразие физических стандартов технологии Ethernet.

Определение Ethernet применимо ко всем компонентам данного семейства. Одни из них задают специфику информационной передачи в соответствии с определенным типом физического соединения на определенной скорости. Другие задают правила (протоколы) для узлов, желающих стать частью локальной сети данной технологии. Все стандарты разработаны IEEE и имеют префикс 802.3 перед основным наименованием.

За более чем сорокалетнее существование технологии Ethernet освоила многообразные физические потоки передачи данных. На сегодняшний день существует множество стандартов, поддерживающих связь через разные типы кабелей (как медных, так и оптоволоконных) и скоростей в пределах от 10 Мегабит в секунду до 100 Гигабит/с.

Материал, из которого изготовлены провода кабеля для передачи данных, является основным показателем при его выборе. Это может быть либо медь, либо оптоволокно. И тот, и другой имеют определенные достоинства и недостатки:

- медный провод (витая, неэкранированная пара, Unshielded Twisted Pair – UTP) стоит меньше, чем оптическое волокно. Используя электричество для передачи данных, подобный кабель действенен на относительно небольших расстояниях;
- оптоволокно, физически представляющее собой стеклянную или пластиковую нитевидную структуру, передает данные в виде световых сигналов на более длинные дистанции, однако стоит дороже меди;
- поскольку скорость света выше скорости электронов, то и данные, передаваемые через оптоволоконный кабель, доставляются значительно быстрее, чем через медный.

Выбирая физические компоненты для организации локальной сети, специалист должен знать наименования стандартов и перечень средств технологии Ethemet, которые ими поддерживаются. При кабельной стандартизации Ethemet, институт IEEE разработал соглашения о наименовании. Все они начинаются с числового префикса 802.3, к которому добавляется буквенный суффикс. Также используются более понятные обозначения, включающие скорость передачи, материал изготовления проводов. Так, суффикс «Т» в наименовании кабеля означает медные провода, а «Х» - оптоволоконные.

На рисунке 1.4 представлена часть стандартов физических составляющих Ethernet. Разброс в наименованиях IEEE дает представление о формате их соглашений.

Скорость	Общеизвестное название	Неофициальное название стандарта IEEE	Официальное название стандарта IEEE	Тип кабеля, максимальная длина (м)
10 Мбит/с	Ethernet	10BASE-T	802.3	Медный, 100
100 Мбит/с	Fast Ethernet	100BASE-T	802.3u	Медный, 100
1000 Мбит/с	Gigabit Ethernet	1000BASE-LX	802.3z	Оптический, 5000
1000 Мбит/с	Gigabit Ethernet	1000BASE-T	802.3ab	Медный, 100
10 Гбит/с	10 Gig Ethernet	10GBASE-T	802.3an	Медный, 100

Рисунок 1.4 – Стандарты физических составляющих Ethernet

Несмотря на то, что в Ethernet прописано множество физических стандартов, она функционирует в рамках единой технологии локальных сетей, использующих общий канальный стандарт для всех физических подключений. Стандартом унифицирован дополнительный набор байтов «до» и «после» передаваемой информации – формат заголовка и концевика одинаков при всех средствах (UTP, оптоволокно) и скорости передачи.

Тогда как физические стандарты нацелены на битовой передаче сведений по проводам, протоколы Ethernet передают фреймы от отправляющего узла к получающему. Определение «Фрейм» (frame) применяется к протокольному заголовку и концевику, между которыми содержится передаваемая информация. Узлы, перенаправляя фрейм по обозначенным каналам, обеспечивают доставку сведений адресату.

Рисунок 1.5 отображает процесс. Цель: пересылка от компьютера PC1 фрейма к компьютеру PC3. Путь достижения: PC 1 – кабель UTP – коммутатор SW1 – оптоволоконный кабель – коммутатор SW2 – оптоволоконный кабель – коммутатор SW3 – кабель UTP – PC3.

Стоит обратить внимание также на скорость передачи битов между узлами (в мегабитах): 10–1.000–10.000–100 Мбит/с.

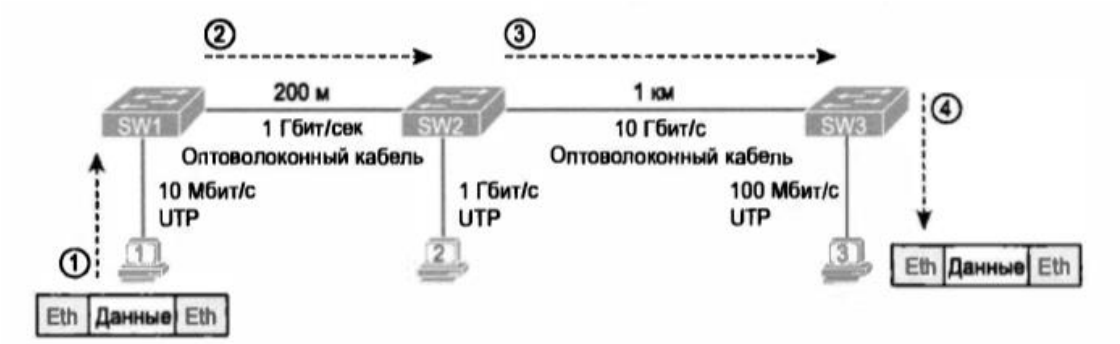


Рисунок 1.5- Пример передвижения фрейма по каналам Ethernet разных типов

Описывая технологию Ethernet, можно дать ей краткое определение. Это совокупность взаимодействующих компьютерных устройств, кабелей и

коммутаторов локальной связи. При этом в отдельном канале передачи могут использоваться различные кабели и скорости прохождения данных. Однако для доставки фреймов от одного сетевого устройства к другому необходимо взаимодействие каналов.

Локальная сеть объединяет «соседствующие» устройства, находящиеся на том же этаже, в том же строении, на той же территории.

Из множества предшествующих технологий локальных сетей, на данный момент наиболее востребованы лишь две – локальные Ethernet и беспроводные.

Сети Ethernet называют проводными, поскольку здесь каналами связи между узлами служат кабели, состоящие из медных проводов. В беспроводных оптоволоконных сетях узлы связи соединяют радиоволны.

Определение Ethernet охватывает большую группу стандартов локальных сетей, классифицирующих и структурирующих компоненты (физические, канальные) всемирной технологии LAN. Стандарты, разработанные IEEE, унифицируют провода в кабелях, разъемы на их концах, правила написания протоколов и прочее, необходимое для функционирования Ethernet.

В локальных сетях Ethernet для передачи данных используются только кабели.

Все стандарты разработаны Институтом IEEE и имеют префикс 802.3 перед основным наименованием.

Материал, из которого изготовлены кабельные провода для передачи данных, является основным показателем при его выборе – либо металл медь, либо оптоволокно.

UTP (витая неэкранированная пара) стоит меньше, чем оптическое волокно. Первая для передачи данных между узлами использует провода, по которым перемещаются электроны – электричество.

Данные через оптическое волокно передаются с помощью световых потоков.

Стоимость оптоволоконной передачи выше, чем электрической.

Принцип действия технологии Ethernet основан на адаптации всех физических устройств под разработанные стандарты.

Определение «Ethernet-канал» относится как к медному, так и к волоконному кабелю, соединяющему два узла передачи.

Фрейм Ethernet, в соответствии с протоколом, состоит из трех элементов: Заголовка, Данных, Концевика.

1.2 Защита информационных сведений

Определение «Защита сведений» объединяет термины безопасности информационных данных и охрану их инфраструктуры от преднамеренных или случайных поступков негативного характера, вызванных действиями различной природы (естественными или искусственными). Вследствие этого обладатели и пользователи данных, владельцы поддерживающей

инфраструктуры, могут понести непоправимые убытки. (Термин «поддерживающая инфраструктура» будет раскрыт ниже.)

Защита информационных сведений представляет собой совокупность процедур, обеспечивающих их закрытость от внешнего вмешательства. При этом грамотный выбор нужного решения в защите информационных данных предусматривает первоначальный анализ субъектов, хранящих непубличные данные, и их заинтересованность в скрытии таковых. Стоит отметить, что риск кражи или публикации хранящихся сведений является оборотной стороной медали использования информационных систем (ИС).

Отсюда следуют два умозаключения:

– значимость хранения важных сведений для каждого субъекта индивидуальна. К примеру, базы данных режимного государственного оборонного предприятия и образовательного учреждения высшего эшелона. Первые следуют девизу: «Пусть эти компьютеры сгорят раньше, чем выдадут наши разработки». Вторые: «Мы ничего не скрываем. Пожалуйста, не ломайте нам настроенную систему».

– сохранность данных – это не только защита от внешнего вмешательства. Моральный или материальный урон может быть нанесен вследствие технических неполадок в системе, вызвавших простой в деятельности предприятия.

Помимо этого, для некоторых компаний (к примеру, образовательных) безопасность хранения данных не является приоритетной темой. Поэтому проблема защиты сведений имеет много граней, и их успешное решение может прийти только с комплексным подходом.

Область защиты собственной информации отталкивается от следующих пунктов:

– предоставление доступности к данным;

– гарантия целостности информационных баз;

– конфиденциальность источника сведений и поддерживающей его инфраструктуры.

Порой к критериям информационной безопасности относят и несанкционированное копирование данных (интеллектуальных разработок, банковских сведений и т.п.). Однако подобные ситуации возникают в наше время все реже, поэтому не стоит заострять на них внимание.

Далее следует пояснить определения открытости, целостности и засекреченности сведений.

Доступность – получение в определенный временной промежуток необходимых информационных сведений.

Суть и цель создания информационных систем заключается в передаче необходимых сведений, доступности информационных услуг. Если по той или иной причине потребителю они недоступны, это является нанесением ущерба всем участникам информационных отношений – как отправителям, так и получателям. Отсюда проистекает вывод – вне зависимости от остальных

аспектов безопасности, доступность сведений, информации является важным компонентом ее безопасности.

Наиболее показательным примером важности фактора доступности являются системы управления различного рода – производства, транспорта и проч. Несмотря на внешнее спокойствие, продолжительная информационная недоступность для огромного количества потребителей внутренне имеет печальные последствия, как моральные, так и материальные. К примеру, сведения в банковской сфере или продажа билетов на железнодорожный, авиатранспорт.

Целостность предоставляемой информации – соответствие этих данных параметрам своевременности, правдивости и оригинальности, без внешнего вмешательства.

Данный параметр безопасности можно разделить на 2 части:

– статическая целостность, к которой относится неизменность, постоянство субъектов отправки/получения информационных сведений;

– динамическая целостность, подразумевающая корректное осуществление многоступенчатых действий, транзакций. Методы проверки этого фактора используются, к примеру, при анализе финансовой информации (при задаче выявления хищений и т.п.), для упорядочения или копирования некоторых сведений.

Полнота информационных данных является наиболее важной деталью их безопасности, если данные сведения являются указующим руководством. К примеру, лекарственная рецептура, назначенное медицинское лечение, пошаговое описание технологии создания чего-либо, состав и описание комплектующих элементов и т.п. – все это является образцом данных, повреждение целостности которых может привести к катастрофическим последствиям. К печальным итогам также может привести искаженность или недосказанность заявлений от официальных структур – ошибки в печати законодательных актов либо на сайте правительственных организаций.

Засекреченность – защита от неправомерного доступа к сведениям.

Засекреченность является в нашей стране наиболее проработанным элементом безопасности сведений. Однако, защита современных систем информации в настоящее время, на практике, испытывает определенные сложности:

– информация о физических способах утечки сведений является закрытой, поэтому большая часть потребителей услуг не может оценить масштаб потенциального риска от утечки данных;

– пользовательская криптография является значимым средством конфиденциальности, однако на ее пути возникает множество препятствий – как технического уровня, так и законодательного.

Основные понятия информационных угроз и их классификация.

Угрозой называется потенциальная вероятность действий конкретной направленности, нарушающих безопасность данных, сведений, информации.

Физические намерения, направленные на осуществление угроз, в мире современных технологий называют атакой. Человек, предпринявший попытку реализации злонамерений, называется злоумышленником. Потенциальный злоумышленник является отправной точкой угрозы, ее источником.

Как правило, наличие угрозы демонстрирует присутствие уязвимых компонентов защиты информационных сведений. К примеру, это оставшийся открытым доступ к программным файлам или, более простой вариант, – возможность постороннему лицу скачать стратегически важную информацию с доступного оборудования.

Временной промежуток, в течение которого имеется вероятность использования отсутствие информационной защиты до момента ее восстановления принято называть окном опасности, точкой уязвимости. Подобные окна предоставляют возможность злоумышленникам совершать атаки на информационные системы, и вполне успешно.

При обнаружении окна опасности в программном обеспечении риск информационной утечки существует с момента его «открытия», обнаружения, до момента наложения программных «заплаток», ликвидирующих ошибки программиста.

Однако данный процесс является длительным, занимающим период от нескольких дней до нескольких недель, в течение которого происходят события следующего характера:

- появление информации об атаке;
- разработка соответствующих мер защиты, доработка программного обеспечения;
- установка «заплаток», закрывающих окно опасности.

Стоит отметить стабильность возникновения очередных уязвимых точек и средств пользования ими. Поэтому окна опасности являются постоянной проблемой, которую нужно периодически отслеживать, а при обнаружении – оперативно выпускать и накладывать «заплатки».

Однако часть угроз не является следствием ошибочных действий группы ответственных за информацию индивидуумов – она может возникнуть под воздействием внешних факторов. Ярким примером тому являются скачки напряжения в электросети или ее резкое отключение, которые негативно влияют не только на корректность работы устройств доступа, но и в принципе могут ее прекратить.

Далее будут рассмотрены наиболее распространенные риски, которым подвергаются современные системы передачи данных.

Знать о предполагаемой опасности, о возможности появления точки внешнего доступа нужно для того, чтобы быть подготовленным, иметь запас средств безопасности.

Для начала сделаем акцент на программных оплошностях в сфере IT. Один из наиболее показательных примеров – глобальная ошибка программистов, «Y2K», внесшая путаницу в датировании событий по годам, «Ошибка-2000». Неправильно написанный код, скрипт, вверг в хаос не

только компании (банки, перевозчики и проч.), но и простых потребителей информационных услуг. (В цифровом обозначении года менялись только 2 последние цифры, две первые «19» оставались неизменными. Поэтому любой программный потребитель в 2000 году вернулся в 1900-й). Расходы на исправление данной проблемы привели к перерасходу и перенаправлению средств, необходимых для более уязвимых и важных окон опасности.

Стоит подчеркнуть, что понятие «угроза проникновения» в различных обстоятельствах понимается по-разному. К примеру, компания, демонстрирующая свою деятельность, не беспокоится о рисках внешнего вмешательства, поскольку сведения о ее работе доступны всем. Однако для большинства предприятий (как частных, так и государственных) стороннее внедрение во внутреннюю информацию является большой опасностью, влияющей не только на деятельность субъекта, но и на сам факт его существования.

Опасность информационной утечки классифицируется по следующим аспектам:

− информационная безопасность, являющаяся целью злоумышленников;

− компоненты систем передачи сведений – сама информация, ее программное обеспечение, устройства хранения и передачи, окружающая инфраструктура;

− способ осуществления умышленных действий, случайных или преднамеренных, естественной или техногенной природы;

− расположение источника опасности – внутреннее либо внешнее относительно данной информационной системы.

− Однако множество рисков имеют форс-мажорную подоплеку – наводнения, пожары, войны и т.п. одинаково опасны для всех систем информационного обеспечения.

Распространенные риски потери доступности

Наиболее часто встречаются (они же и являются наиболее опасными в плане масштаба нанесенного ущерба) непреднамеренные действия лиц, причастных к обслуживанию информационных систем. К ним относятся штатные сотрудники компании – операторы ввода сведений, системные администраторы и т.д. – лица, причастные к обслуживанию баз информационных данных. Порой подобные ошибки и представляют собой угрозу (некорректный ввод данных, лишний символ или отсутствие нужного в скрипте), создающую окна уязвимости для злоумышленников.

Согласно статистике, 65% из всех информационных потерь происходят вследствие непреднамеренных действий. И наличие форс-мажорных обстоятельств здесь стоит на последних пунктах перечня причин. Первые места отведены профессиональной безграмотности и беспечности. Поэтому оптимальным решением при возникновении подобных ошибок является минимизирование влияния человеческого фактора и внедрение строгого контроля.

Остальные виды опасностей можно классифицировать по составляющим информационных систем, являющимся объектами для угроз:

а) пользовательский отказ. Как правило, здесь опасностью для информации являются следующие факторы:

- отрицание компьютеризации информационных сведений. Как правило, это является следствием нежелания освоения IT-технологий;
- отсутствие соответствующей технической поддержки – некорректное руководство по пользованию ПО, пробелы в документации, ориентированной на пользователя;
- неспособность работать с базами данных, вызванная компьютерной неграмотностью, непониманием электронных мануалов и диагностических сообщений.

б) внутренняя неработоспособность ИС. Причинами возникновения данных рисков потери данных являются следующие:

- несоблюдение эксплуатационных правил пользования информационной системой, случайное либо умышленное. К нему относится превышение количества обращаемых запросов, объема обрабатываемых сведений и прочее;
- совершение ошибочных действий в ходе переконфигурирования системы;
- отказ в работе ПО или аппаратных устройств;
- удаление информации;
- уничтожение обеспечивающих связь устройств.

в) неработоспособность поддерживающей инфраструктуры. Этот пункт подразумевает следующие виды опасностей:

- подрыв работоспособности физических компонентов – отсутствие электричества, воды, тепла, кондиционирования;
- разрушение здания, помещения, в котором расположено аппаратное обеспечение;
- нежелание, отказ сотрудников либо потребителей исполнять свои обязательства (забастовка, общественные беспорядки, теракт либо угроза его возникновения и т.п.).

Не менее опасны и собственные сотрудники (как действующие, так и уволившиеся), наносящие вред в силу личных обид. Помимо порчи оборудования или удаления информационных сведений, они могут установить программу с таймером, которая в назначенную дату уничтожит данные либо ПО.

Они знают о правилах и порядках, существующих в компании, о существующей системе безопасности, ее элементах. Поэтому считается важным максимально ограничить доступ увольняющегося работника (как физический, так и логический) к базам хранящейся информации.

1.2.1 Примеры рисков отсутствия доступа. Опасность потери информации может быть вызвана природными явлениями, которые не только

частично повреждают, но и полностью выводят из строя устройства, обеспечивающие передачу данных. К примеру, удар молнии в источник бесперебойного питания может полностью лишить его работоспособности. Здесь окном опасности является отсутствие защиты оборудования от естественных непредумышленных атак.

Теоретически, подобную атаку можно вызвать и искусственно, генерацией мощного электрического импульса с использованием радиочастотных «пушек». Однако реалии нашего государства предоставляют более простые варианты нанесения ущерба информационной системе.

Так, неисправность отопительной или водопроводной системы в серверном помещении способна ослабить экономические позиции не только отдельного предприятия, но и всех взаимодействующих структур. Но эта проблема касается лишь предприятий малого бизнеса, не имеющих собственной территории или экономящих на аренде. Это трудно себе представить, но сетевой администратор одной столичной фирмы добровольно уволился по единственной причине – сетевой кабель перегрызла крыса. В тот момент финансовый урон был значителен и компания попыталась найти виновника бед, который бы компенсировал убытки.

Также поломка системы кондиционирования в наиболее жаркий период года является одной из причин отсутствия информационного доступа. Отказ кондиционеров в серверной комнате приводит к перегреву оборудования – срабатывает защитная функция выключения серверов. Рабочие компьютеры лишены сетевого доступа, деятельность компании приостанавливается – получение и передача данных невозможна.

Известно, что периодическое копирование сведений повышает вероятность их сохранности. Однако, даже при выполнении данного условия, резервные носители информации хранятся крайне небрежно, без учета защиты от вредоносного воздействия окружающей атмосферы. Поэтому, при восстановлении информационных данных, они зачастую являются недоступными для считывания.

Далее рассмотрим программные атаки, представляющие собой более серьезную угрозу информационной безопасности, чем тривиальные случаи протечки водопровода или отключения электричества.

Вывести систему из рабочего режима может агрессивное потребление ее данных. Как правило, это нагрузка на части пропускных сетевых полос, на память аппаратных устройств – как на оперативную, так и на внутреннюю.

Расположение источника опасности может быть локальным либо удаленным. Просчеты в конфигурировании информационной системы способны полностью захватить работу физической памяти и процессора, не дающие возможность оперативно действовать остальным программам, сводящим их работу «на нет».

Элементарный пример подобных сетевых атак – переполнение объема запросов с разных IP-адресов, с которым не справляется серверное оборудование, SYN-флуд (рисунок 1.6). В короткий временной период

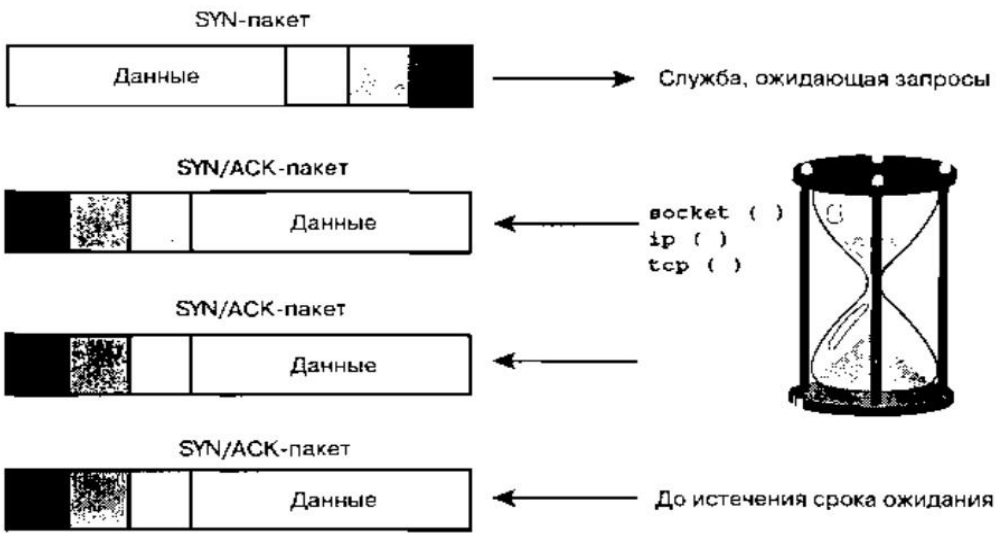


Рисунок 1.6 - Схема начала атакующих действий

соединения TCP начинаются, но не имеют возможности завершиться. Подобная атака злоумышленников не позволяет действительным пользователям воспользоваться информацией – сервер недоступен. Этот показатель сетевой атаки был выявлен в феврале 2000-го года, когда потерпевшими от них оказались владельцы и потребители известных торговых марок.

2 Описание сети

2.1 Компьютерная сеть фирмы

Компьютерная сеть фирмы – совокупность аппаратно-технических, программных средств, которая позволяет:

- организовать централизованное хранение информации;
- обеспечить стабильность документооборота;
- вести отчеты о текущих проектах, вести бухгалтерский учет;
- организовать сетевую печать.

Схематически сеть представлена в Приложении А.

Аппаратная часть компьютерной сети фирмы представлена в таблице 2.1.

Применяемое программное обеспечение - в таблице 2.2.

Активное оборудование рассмотрено в таблице 2.3.

Пассивное оборудование рассмотрено в таблице 2.4. Кабельная система устроена посредством «витой пары». Разъемы стандартные – RJ-45. Подключение к коммутатору, устройствам.

Серверы имеют некоторые специфичные функции, что определены предметной областью фирмы. Функции сервера представлены в таблице 2.5.

Аппаратное обеспечение сервера рассмотрено в таблице 2.6.

ПО сервера описано в таблице 2.7

Таблица 2.1 - Аппаратная часть

Позиция	Характеристики	Кол-во	Прим.
Рабочие станции универсальные	- 23,8”, 1920*1080; - Intel Core i3 6100U; - Intel HD Graphics 520; - 4Gb DDR4; - 1Tb HHD; - Gigabit Ethernet.	1,5 тыс. шт.	ASUS
Рабочие станции отдела ИБ и ИТ	- 23,8”, 3840*2160; - Intel Core i7 6700T; - NVIDIA GeForce GTX960M; - 16Gb DDR4; - 1Tb HHD, 128Gb SSD; - Gigabit Ethernet.	15 шт.	DELL
Серверный PC	- Intel Xenon E4-1200 v.3 LGA 1150; - 8Gb DDR3; - 128Gb SSD; - 2x Intel I210AT.	1 шт.	-
Коммутатор	- 16 портов; - 2 порта Ethernet.	18 шт.	CISCO
Принтер	- формат А4; - лазерное МФУ; - USB.	10 шт.	HP LaserJet Pro M125ra
Принтер	- формат А0; - печать: струйная, цветная, термическая.	1 шт.	HP, Canon

Таблица 2.2 - Программная часть

Позиция	Характеристики	Кол-во	Примечания
1	2	3	4
ОС сетевая	Windows Server 2016	1 шт.	ОС серверная
ОС на PC	Windows 10 Pro	300 шт.	Предустановка
ПО для бухгалтерского учета	1С: Предприятие	1 шт.	Автоматизация деловых процессов
ПО антивирусное	Kaspersky Endpoint Security 10	1 шт.	Защита сервера и станций Windows

Продолжение таблицы 2.2

1	2	3	4
Офисный пакет	MS Office 365 «Бизнес»	1 шт.	- эл. почта с ящиком до 500ГБ; - хранилище файлов до 1ТБ с общим доступом; - full-пакеты приложений MS для PC и MAC.
ПО для резервного копирования	Acronis Backup Advanced	1 шт.	Резервное копирование в локальных, удаленных средах

Таблица 2.3 - Активное оборудование

Позиция	Характеристики
Коммутатор CISCO	- управляемый, 2-ой ур.; - пропускная способность – 32Гбит/с; - 16 портов; - доп. порт Ethernet.

Таблица 2.4 - Пассивное оборудование

Позиция	Характеристики
Витая пара ATcom AT3802	- категория 5е; - 4 пары; - фольгированное экранирование, одна жила; - PoE; - l участка до 100 м; - пропускная способность – 1Гбит/с; - низкая стоимость; - устойчивость к помехам (дифференциальный сигнал).

Таблица 2.5 - Функции сервера

Тип	Специфичные функции
1	2
Главный сервер	1. Удаленное управление PC. 2. Управление группами пользователей, аудит. 3. Управление виртуальными сетями, копиями. 4. Управление доступом к интернету.
Файловый сервер	1. Хранение файлов. 2. Резервное копирование. 3. Обеспечение общего доступа.

Продолжение таблицы 2.5

1	2
Сервер БД	1. Хранение БД, поддержка целостности и полноты последних, актуальности. 2. Обработка запросов к БД, поддержка и обеспечение учета пользователей. 3. Разграничение доступа отдельных категорий пользователей. 4. Согласование изменений данных, инициаторами которых являются отдельные категории пользователей.

Таблица 2.6 - Аппаратное обеспечение сервера

Позиция	Подробнее	Прим.
Процессор	Intel Xenon E3-1200 v3 LGA1150	-
Чипсет	Intel C226	-
ОЗУ	UDIMM DDR3 8Gb 1600Mhz	-
Накопители	- 2.5” 128Gb SSD; - 3.5” 1Tb HDD.	-
Сеть	2x Intel I210AT	Передача данных на скорости до 1Гбит/с
Разъемы платы	- PS/2 KB/MS port (1 шт.); - S/PDIF Out (Optical) (1 шт.); - USB 3.0 ports (4 шт.); - USB 2.0 ports (9 шт.); - RJ-45 ports (2 шт.); - DVI-I (1 шт.); - 8-channel Audio I/O (1 шт.); - HDMI (1 шт.); - Display Port (1 шт.).	
Питание	600W 80PLUS Single Power Supply, Gold	- 100-240V; - 4-8A; - 50-60Hz (Class I).

Таблица 2.7 - ПО сервера

ПО	Характеристики
1	2
Netgear Network Management	Обеспечение и поддержка управления конфигурацией коммутатора
Western Digital My Cloud Access	Обеспечение управления сетевыми накопителями

Продолжение таблицы 2.7

1	2
Acronis BackUp for Windows Server	Задачи: - резервное копирование; - восстановление данных в локальной сети и удаленном хранилище.
MS Windows Server 2016	1. Полноценное развертывание и поддержка работоспособности IT. 2. Обеспечение возможности доступа и идентификации служб и приложений фирмы, обеспечение возможности контроля сред. 3. Поддержание безопасности посредством встроенных служб, разграничивающих права доступа при администрировании. 4. Шифрование. 5. Средства диагностики.
1С: Сервер	Ключевая задача – обеспечение работы бизнес-приложений. Посредством сервера можно: - создать запрос к БД; - записать информацию; - провести расчеты; - осуществить обработку; - сформировать отчетность; - создать резервную копию БД.
Kaspersky Endpoint Security 10	Задача – комплексная защита посредством многоуровневой системы: - контроль запуска и активности программных средств; - контроль внешних устройств; - контроль доступа к Интернету; - защита от вредоносного ПО; - защита от сетевых угроз.

2.2 Необходимость защиты

В общем случае, если дело касается безопасности фирмы, ее правление и руководители во многом недооценивают значимость информационного компонента. Ключевой считается задача обеспечения физической безопасности (пропускной режим, охрана, системы оповещения и т. п.).

Практика последних лет позволяет говорить о том, что учет только физической безопасности просто нецелесообразен. Для овладения тайнами фирмы вовсе не обязательно вторгаться в защищенные помещения или вскрывать сейфы. Проникновение в информационную среду, получение

доступа к конфиденциальным данным, нефизическая кража финансовых средств и другое – все это возможно даже без физического вмешательства.

Финансовый ущерб.

Такого рода ущерб может быть как прямым, так и косвенным. Примеров первого (прямого) слишком много. Особенно яркими стоит считать те, что характерны для финансовой сферы. Пример: совсем недавно Bank of America столкнулся с необходимостью взаимодействия с силовыми структурами, что было вызвано созданием злоумышленниками фальшивого интернет-ресурса, задачей которого было получение доступа к финансовым данным клиентов.

Еще один пример: подобным образом злоумышленники смогли обмануть множество клиентов eBay, заполучив доступ к данным об их платежных картах.

Важно понимать, что создание «левых» ресурсов – далеко не единственный способ получения конфиденциальной информации. К примеру, совершенно иным способом (посредством взлома) злоумышленники получили доступ к данным о более 3,5 тыс. кредитных карт клиентов Republic Bank (Флорида).

Любая фирма может столкнуться с ситуацией, когда потеря средств будет вызвана не просто мошенничеством или кражей. Так, целенаправленное выведение из строя определенных сетевых узлов – то, что приводит к необходимости восстановления их функционирования: требуется замена ПО, аппаратного обеспечения, оплата услуг специалистов и т. п. А нецелесообразное и неоправданное использование трафика сотрудниками (просмотр порнографических сайтов, общение в социальных сетях и т. п.) может обернуться для любой фирмы колоссальными расходами. Применение же средств контроля входящего интернет-содержимого (к примеру, MIMEsweeper) позволит исключить вероятность непродуктивного использования трафика.

Что касается способов борьбы с хакерскими атаками: решение проблемы возможно также посредством использования особых систем (к примеру, RealSecure). Расходы на подобные системы многократно ниже расходов, которые фирме придется понести в результате хакерской атаки.

Реальные цифры: одна хакерская атака может причинить фирме ущерб на 50 и более тыс. долларов США. Подтверждение тому – события февраля 2000 г., когда Amazon, eBay, Buy.com и сервера прочих всемирно известных компаний подверглись хакерской атаке, а в результате трехчасового простоя интернет-ресурсов названые компании потеряли несколько миллиардов долларов.

Ущерб репутации.

Важно понимать, что денежные средства – не единственное, чего может лишиться фирма из-за недооценки вопросов безопасности информации. Результатом этой недооценки может стать утрата репутации.

Яркий пример: в конце лета 2001 г. хакерами были выведена из строя система продаж акций Brass Eagle на известной бирже NASDAQ. Двухчасовое

отключение системы вместе с единовременным взломом сайта было спланировано, задачей его стала рассылка тысяч электронных писем клиентам фирмы с недостоверной финансовой информацией.

Это привело, что понятно, к утрате компанией Brass Eagle доверия клиентов, стоимость ее акций резко упала.

Еще один интересный случай – события августа 2000 г. Тогда служба пресс-релизов под названием Internet Wire получила fake-сообщение от Emulex Corp. о том, что директор последней ушел в отставку. Служба, что понятно, поверив сообщению, начала активно распространять информацию. Ее подхватили некоторые другие службы. Следствием этого злонамеренного действия недобросовестных лиц стало падение акций Emulex на 60%. Репутация последней и Internet Wire была практически «растоптана».

Банкротство.

Важно понимать и тот факт, что хакерские атаки могут довести любую фирму до банкротства. К примеру, некоторые западные специалисты в своих работах отмечают, что раскрытие порядка четверти объема конфиденциальной информации фирмы ставит ее на порог банкротства. И это реальность, а не вымысел,

Приведем пример: CloudNine Communications, будучи британским «ветераном-провайдером», столкнулся с атакой злоумышленников в начале года. Хакерами была реализована атака по принципу «отказ в обслуживании». Задача атаки – нарушение работоспособности сетевых узлов. Примечательно то, что злоумышленники использовали метод перегрузки узлов, при котором колоссальные объемы данных направлялись на отдельные узлы из множества точек одновременно.

Результатом действий злоумышленников стала ликвидация CloudNine и передача ее БД компании-конкуренту (Zetnet). Бывший совладелец CloudNine, Э. Мизги, позже рассказал СМИ о том, что атака против компании «была спланирована, она длилась несколько месяцев». При этом понятно, что хакеры в течение длительного периода времени анализировали информацию о серверах компании и их пропускной способности, а когда все было «готово», нанесли сокрушающий удар. Э. Мизги также отметил в своем интервью, что совершенно не понимает, почему CloudNine стала объектом интереса злоумышленников, подчеркивая, что инцидент привел к ущербу не только компании, но и ее клиентов.

Среди прочих примеров: атака на Tiscali (итал. провайдер), Donhost (британский). Стефан Хьют, представитель Tiscali, полагает подобного рода атаки серьезным ударом по любому бизнесу, предостерегая конкурентов и партнеров, отмечая, что «никто от них не застрахован».

Уголовный кодекс.

Если все приведенные только что примеры не кажутся убедительными, стоит обратиться к Казахстанскому Уголовному Кодексу. Нас интересует ст. 277. Неправомерный доступ к компьютерной информации, создание,

использование, распространение вредоносных программ для ЭВМ. Согласно положениям этой статьи:

а) Нарушение правил эксплуатации лицом, имеющим доступ, если это нарушение привело к блокированию, изменению или уничтожению данных, при этом причинило колоссальный ущерб, предполагает наступление ответственности (один из вариантов):

- лишение права занимать некоторые должности на срок до 5 лет;
- обязательные работы на срок от 180 до 240 часов;
- лишение свободы сроком до 2-х лет.

б) То же, но в случае, когда последствия носят тяжкий характер, может привести к лишению ответственного лица свободы на срок до 4-х лет.

Не стоит наивно полагать, что рассмотренные угрозы – какой-то миф или то, что не коснется Вас и Вашей фирмы. Даже если Вы не владеете фирмой, вероятность ответственности и определенные риски существуют. Почему? Все просто.

Любой из хакеров для совершения атаки может использовать как свой ПК, так и множество ПК и устройств других, ничего не подозревающих об этом пользователей. Вспоминаем ст. 277.

Да, в Казахстане пока не зафиксированы случаи подобного рода реализации хакерских атак, но в ряду западных стран такая практика довольно-таки распространена. Еще больше там распространена практика применения наказаний компаний и фирм по статьям, аналогичным ст. 277 УК РК.

Яркий пример: август 2001 г. Нашумевший червь Code Red. Тогда провайдер Qwest DSL был обязан судом выплатить клиентам компенсации за дестабилизацию доступа к интернету, что была вызвана выходом из строя оборудования компании.

3 Описание программы и моделирование

Skybox Security представляет собой программную аналитическую платформу, которая имеет модульную функциональную архитектуру. Каждый модуль отвечает за реализацию определенного функционала и может приобретаться и работать самостоятельно.

- Network Assurance – модуль контроля, анализа и визуализации состояния сетевой безопасности

- Firewall Assurance – модуль анализа и контроля настроек межсетевых экранов

- Change Manager – модуль контроля и автоматизации изменений настроек межсетевых экранов

- Vulnerability Control – модуль управления уязвимостями

Skybox Network Assurance

Модуль Network Assurance предназначен для работы с сетевыми устройствами (L3). Данный модуль может функционировать как самостоятельно, так и в комбинации с другими модулями. Модуль лицензируется по количеству сетевых устройств, включая межсетевые экраны.

Основными возможностями модуля Network Assurance (NA) являются:

- сбор конфигураций со всех поддерживаемых сетевых устройств (L3) и автоматические построение карты сети;
- контроль соответствия конфигураций сетевых устройств заданным стандартам конфигурирования и лучшим практикам, включая локальные принятые правила конфигурирования;
- вычисление и визуализация на карте сети возможных путей/маршрутов прохождения заданного типа трафика с демонстрацией разрешающих и запрещающих правил/настроек, которые задействованы для данного пути/маршрута;
- создание политики сетевого доступа (сетевого сегментирования) и автоматический контроль ее исполнения как в масштабах всей модели сети, так и на уровне настроек отдельных устройств.

Network Map представлен на рисунке 3.1.

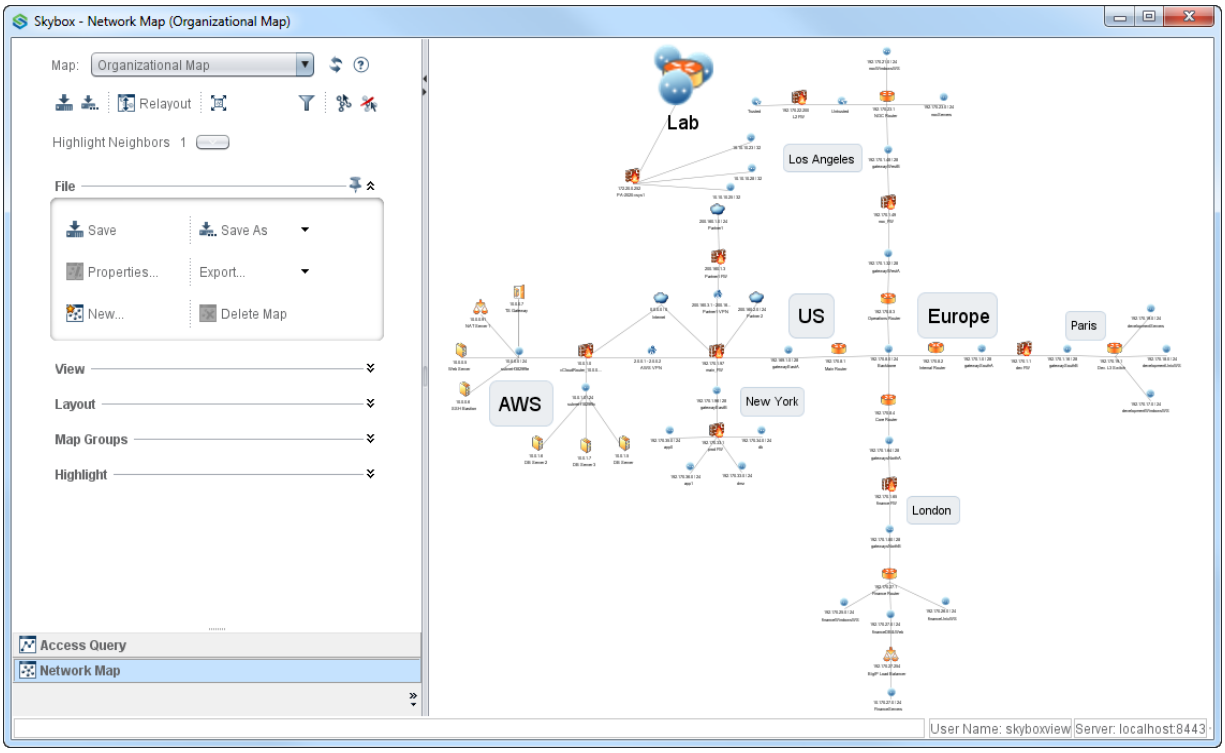


Рисунок 3.1- Network Map

Skybox Firewall Assurance.

Модуль Firewall Assurance (FA) предназначен для работы с межсетевыми экранами, и может функционировать как самостоятельно, так и в комбинации с другими модулями. Межсетевыми экранами для Firewall Assurance могут выступать как непосредственно межсетевые экраны, так и другие поддерживаемые сетевые устройства, использующие списки доступа (ACL). Skybox Security распознаёт наиболее полный список поставщиков межсетевых экранов и понимает сложные наборы правил даже для виртуальных и облачных межсетевых экранов, а также учитывает сигнатуры IPS. Модуль лицензируется по количеству межсетевых экранов.

Модуль отображает все межсетевые экраны в едином окне, осуществляет их постоянный мониторинг на соответствие политикам, оптимизирует правила межсетевых экранов, осуществляет непрерывный мониторинг настроек межсетевых экранов.

Основными возможностями модуля Firewall Assurance (FA) являются:

а) автоматический сбор конфигураций межсетевых экранов и непрерывный мониторинг настроек, включая отслеживание всех изменений;

б) оптимизация списков доступа межсетевых экранов:

- выявление затененных, избыточных и дублирующихся правил;
- выявление редко используемых правил и объектов;
- формирование рекомендаций по оптимизации конфигураций.

в) контроль соответствия конфигураций межсетевых экранов заданным стандартам конфигурирования и лучшим практикам, включая локальные правила конфигурирования, а также указание причины несоответствия вплоть до конкретных правил на конкретных устройствах:

- выявление правил, содержащих any в 2 или 3 полях, в поле сервис и т.д.
- выявление настроек, противоречащих рекомендациям производителей с точки зрения безопасности;
- выявление правил, разрешающих передачу паролей в открытом виде и т.д.

г) создание политики сетевого доступа (зон безопасности) и автоматический контроль ее исполнения (встроены стандарты PCI DSS, NIST) на уровне зон безопасности межсетевых экранов с указанием причины несоответствия вплоть до конкретных правил на конкретных устройствах.

Firewall Assurance изображен на рисунке 3.2.

Skybox Change Manager.

Change Manager (CM) является дополнением к модулю Firewall Assurance, при этом количество лицензий CM всегда соответствует FA.

CM позволяет контролировать и автоматизировать процесс изменения правил доступа от заведения заявки до ее выполнения, и гарантирует то, что все изменения произведены в полном соответствии с принятым регламентом предоставления сетевого доступа.

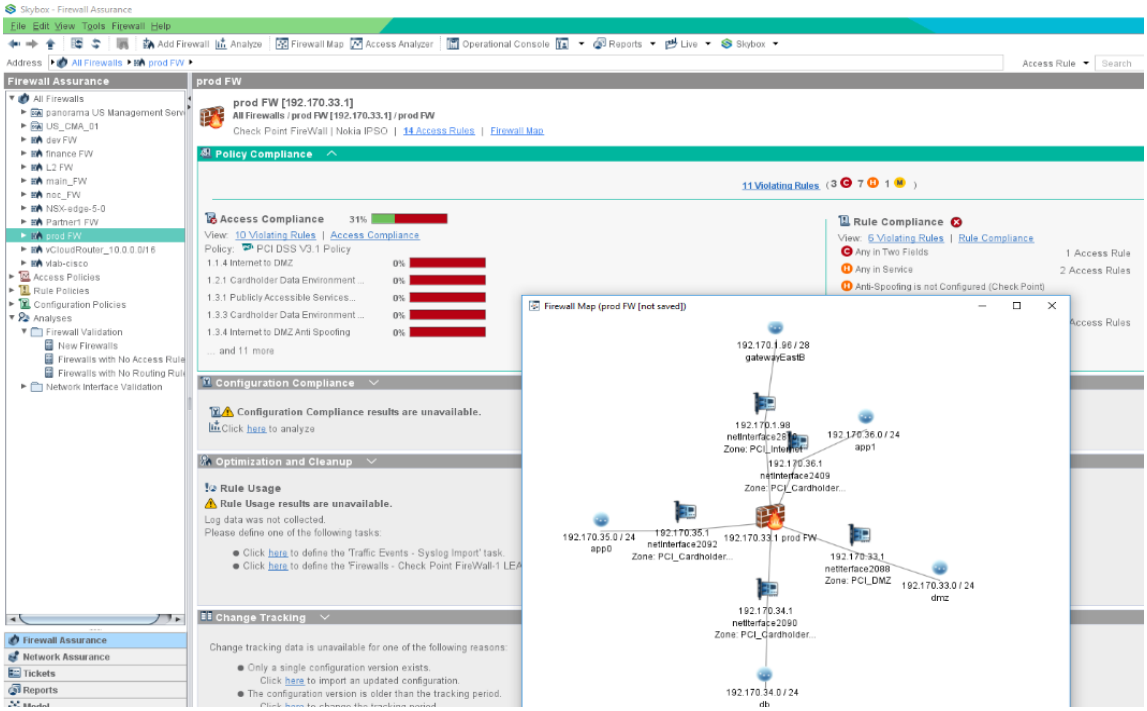


Рисунок 3.2- Firewall Assurance

Основными возможностями модуля Change Manager (CM) являются:

а) создание workflow на изменение сетевого доступа за счет встроенной системы заявок или интеграции с внешними системами:

- предоставление или изменение сетевого доступа;
- периодический пересмотр правил сетевого доступа;
- выявление изменений правил и настроек, выполненных без соответствующей заявки или согласования;

б) автоматическое выделение устройств, на которых необходимо произвести изменение;

в) формирование рекомендаций по вносимым изменениям конфигураций МЭ при изменении сетевых доступов;

г) автоматическое применение планируемых изменений правил МЭ (в частности, Check Point, Palo Alto, Fortinet, Cisco);

д) автоматическая оценка влияния планируемых изменений на политику сетевого доступа и безопасного конфигурирования, а также (в случае наличия модуля Vulnerability Control) на защищенность ИТ-активов с точки зрения появления дополнительных уязвимостей, связанных с изменением.

Skybox Vulnerability Control.

Модуль Vulnerability Control (VC) является модулем работы с уязвимостями и лицензируются по числу ИТ-активов (например, серверы или рабочие станции (по сути, сканируемые IP-адреса)), в отношении которых необходимо производить анализ и расчет векторов атак. Минимальная лицензия включает пакет до 100 активов.

Vulnerability Control объединяет данные со всех сканеров, систем патч-менеджемента и систем инвентаризации, информацию о потенциальных уязвимостях и источниках угроз, коррелирует данные об уязвимостях с картой сети и позволяет визуализировать вектора возможных атак.

Основными возможностями модуля Vulnerability Control являются:

а) автоматический сбор информации об ИТ-активах (имеющиеся уязвимости, актуальный состав и версии ПО) из сканеров, систем инвентаризации и патч-менеджмента;

б) автоматический сбор конфигураций сетевых устройств и построение карты сети (на сетевые устройства при этом должны быть приобретены лицензии VC);

в) расчет возможных векторов атак с учетом настроек сетевого оборудования, включая активированные сигнатуры IPS (см. рисунок 3.3);

Выявление вновь появляющихся уязвимостей в период до/между сканированиями (ежедневно обновляемая собственная база);

г) приоритезация найденных уязвимостей с учетом:

- возможности ее реальной эксплуатации в условиях конкретной сети и ее настроек;
- сведений о частоте эксплуатации данной уязвимости (на основе подписок Threat Intelligence Feeds);
- сведений о ценности актива, содержащего данную уязвимость и т.д.
- критичности уязвимости;
- наличие готовых инструментов атак (exploits), направленных на эксплуатацию конкретной уязвимости;
- факты атак, в ходе которых зафиксирована эксплуатация конкретной уязвимости.

д) формирование рекомендаций по устранению уязвимостей с возможностью реализации workflow на базе встроенной системы заявок.

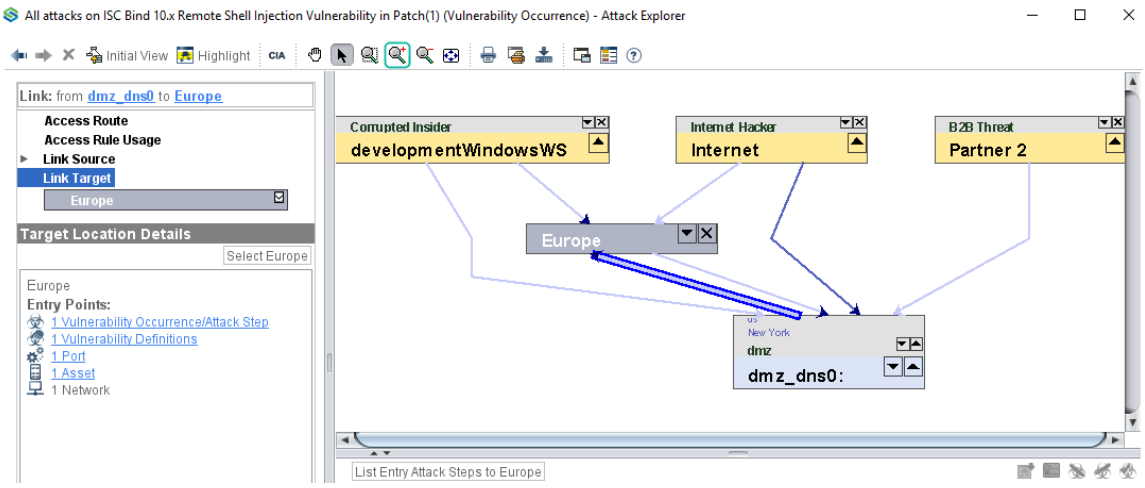


Рисунок 3.3 - Вектор атак

Важно отметить, что модуль VC также дает возможность построить карту сети по аналогии с Network Assurance и выполнять анализ доступа, но без расчетов Policy Compliance, так как для вычисления векторов атак требуется полное моделирование сетевой инфраструктуры. Визуализация приведена на рисунке 3.4.

Рисунок 3.4- Визуализация

Архитектура решения.

В общем виде архитектура решения представлена на рисунке 3.5.

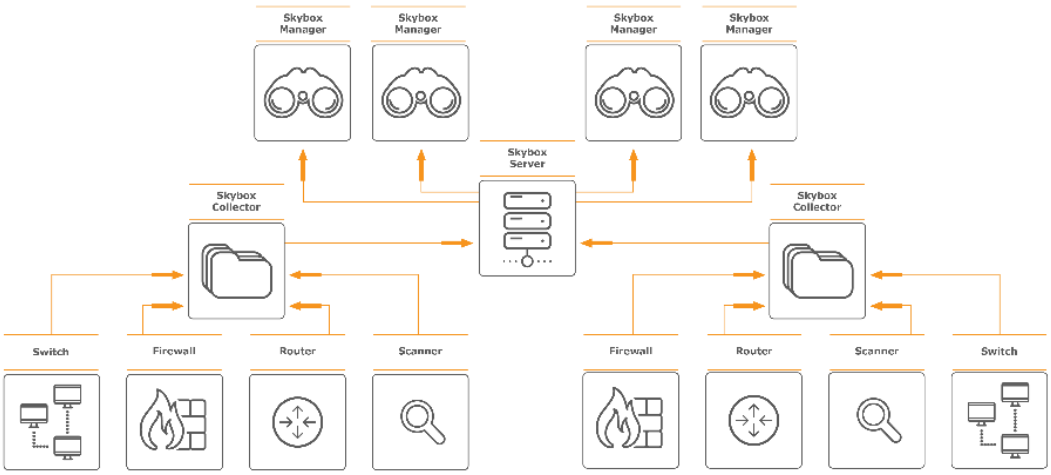


Рисунок 3.5 - Схема архитектуры решения

3.1 Расчеты

При интеграции решения были заполнены опросные листы и собраны конфигурационные файлы сетевого оборудования.

Первоначальной задачей является загрузка конфигурационных файлов и добавление сетевого оборудования посредством функции Operational Console.

Добавление сетевого оборудования представлено на рисунке 3.6.

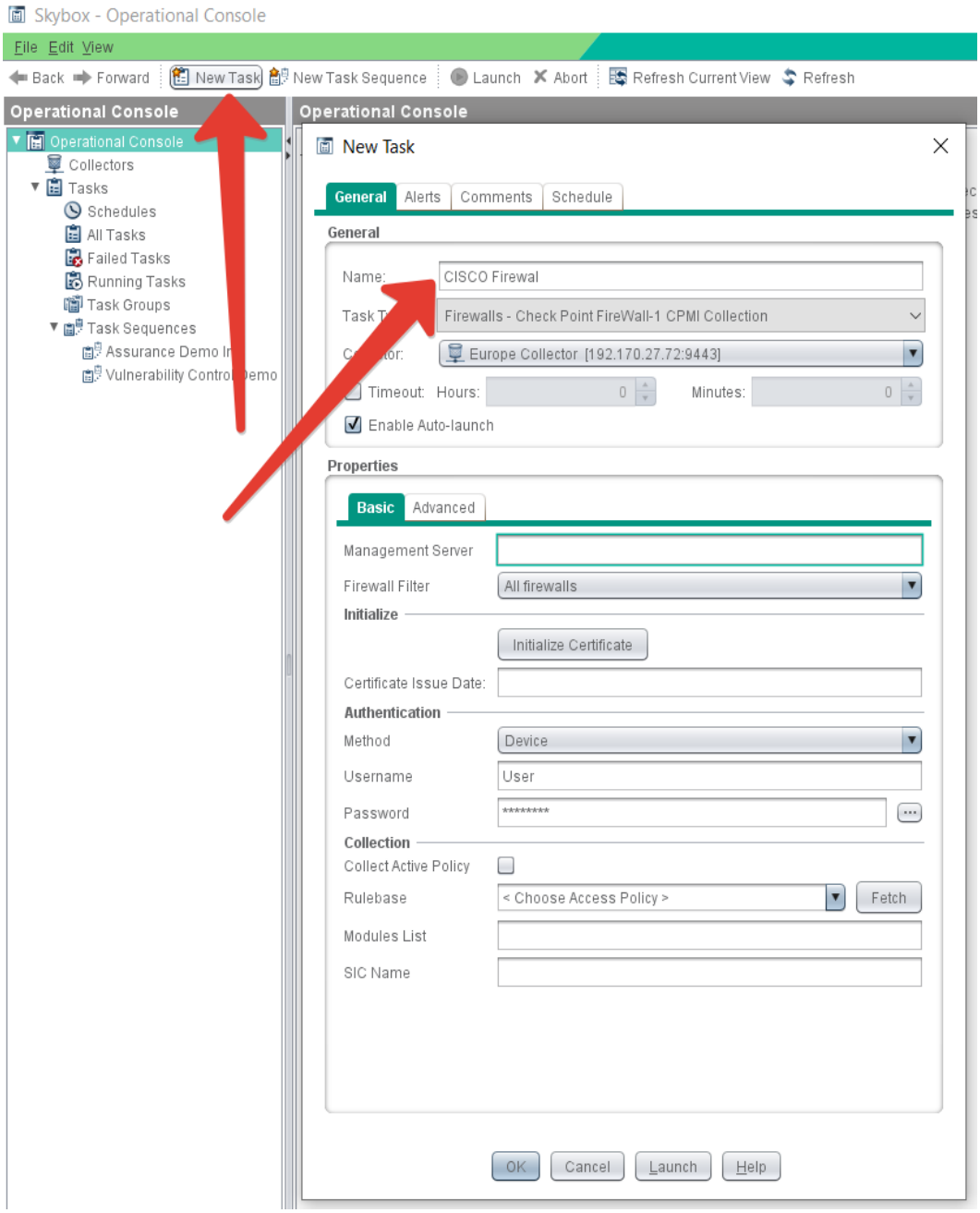


Рисунок 3.6 - Добавление сетевого оборудования

Аналогичном образом добавлялось все сетевое оборудование. В данном случае потребовался логин и пароль для подключения, а так же конфигурационный файл.

Было настроено так же время проведения анализа всего сетевого оборудования (см. рисунок 3.7).

Анализ будет проводиться один раз в неделю в не рабочее время в субботу в 00.00.

После добавления и настройки всего сетевого оборудования были проведены работы по созданию задач которые выполняют следующий функционал:

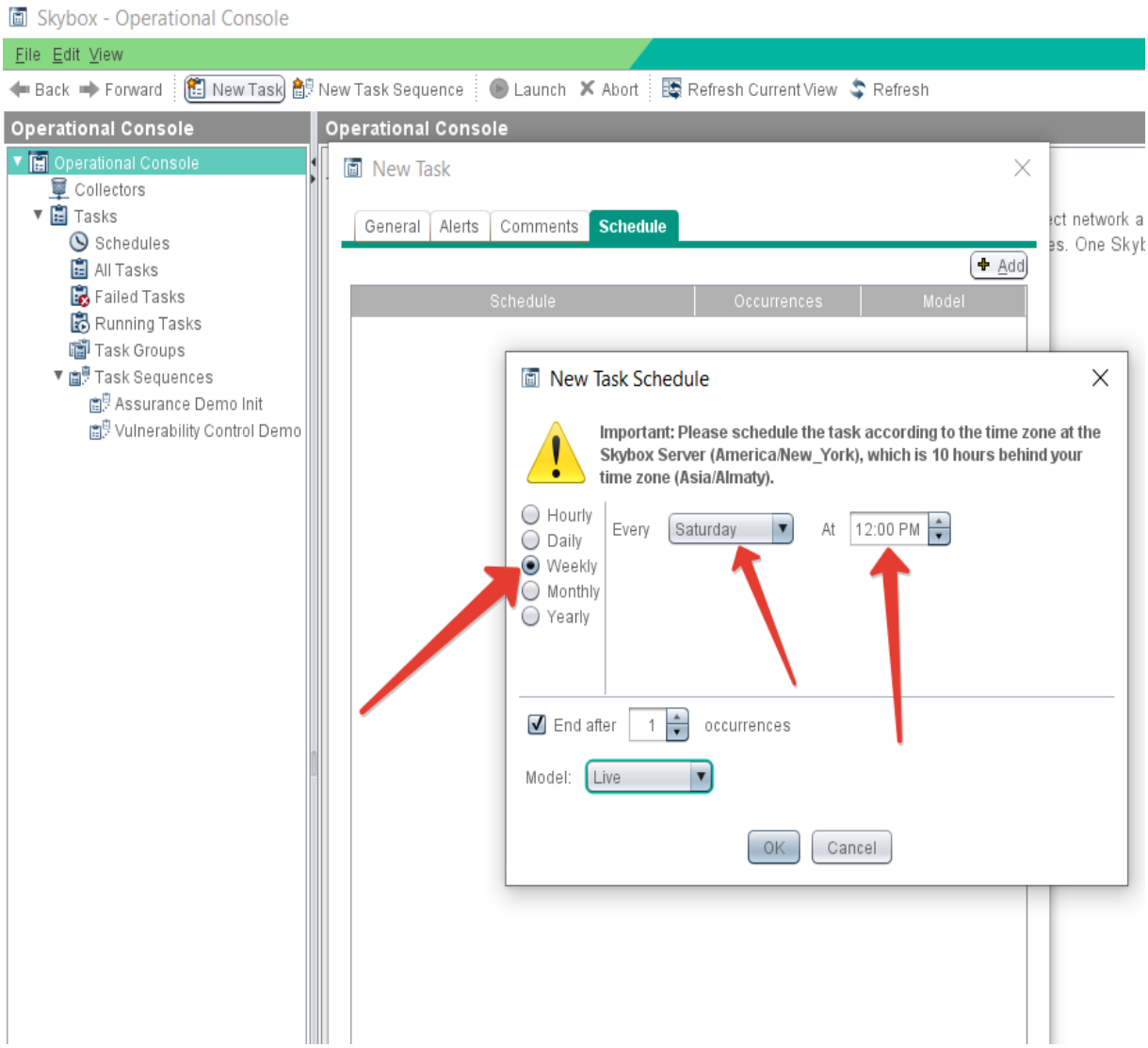


Рисунок 3.7 - Настройка времени анализа

– Analyze Firewall Changes – анализ межсетевых экранов на наличие изменений

– Analyze Firewall Policy Compliance – анализ правил безопасности сети

– Analyze Network Policy Compliance – анализ маршрутизаторов, коммутаторов и балансировщиков нагрузок и т.д.

– Analyze Rule Optimization Status – анализ оптимизации правил межсетевых экранов

– Backup Data – сохранение модели сети и настроек

– Generate Firewall/Network/Risks/ Security Report – автоматическая генерация отчета всего сетевого оборудования, рисков и безопасности.

Диспетчер задач рассмотрен на рисунке 3.8. Информация Firewall Assurance представлена на рисунке 3.9.

После проведения анализа сети можно увидеть все уязвимости и плохо сконфигурированное сетевое оборудование. В данном случае в качестве примера рассмотрим межсетевой экран Cisco.

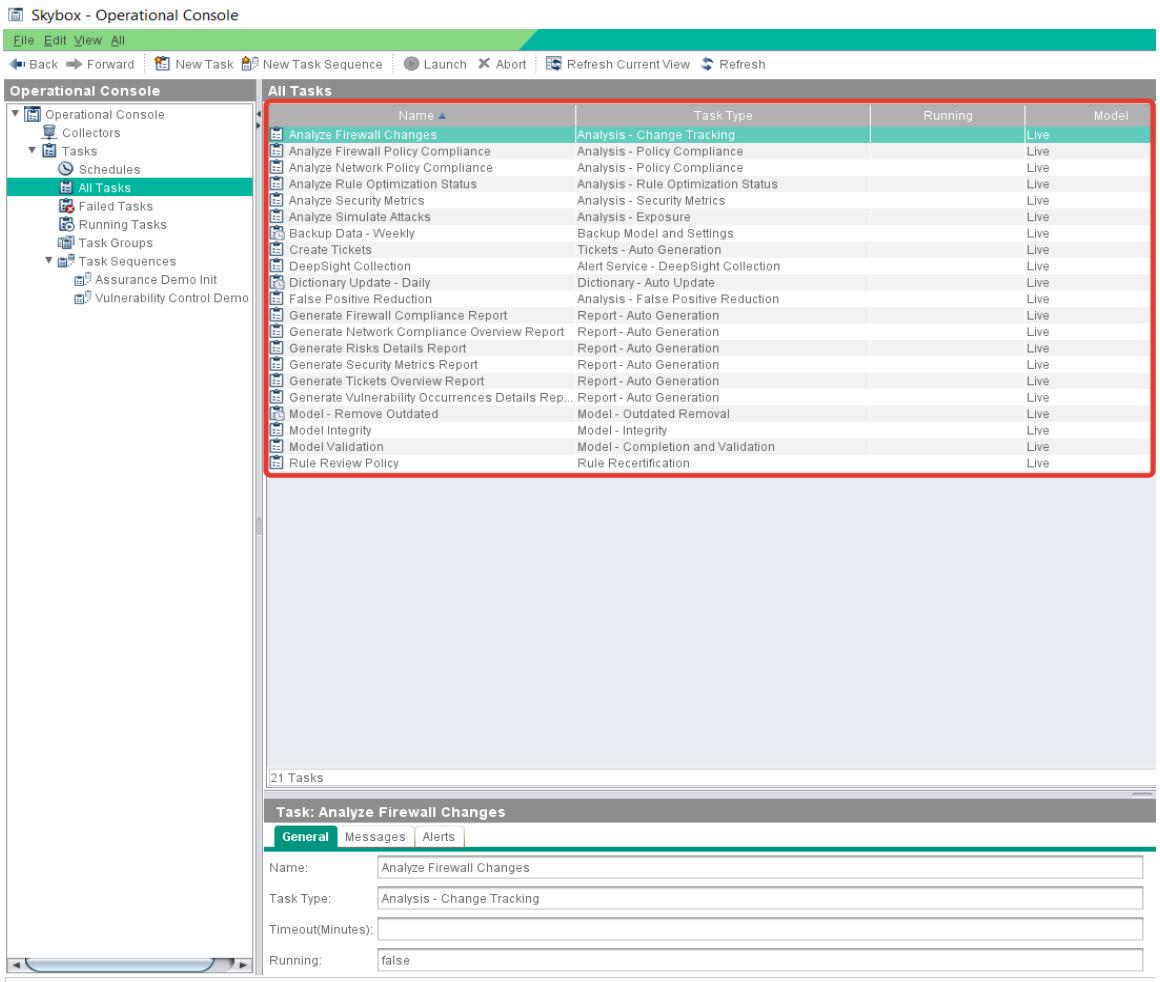


Рисунок 3.8 - Диспетчер задач

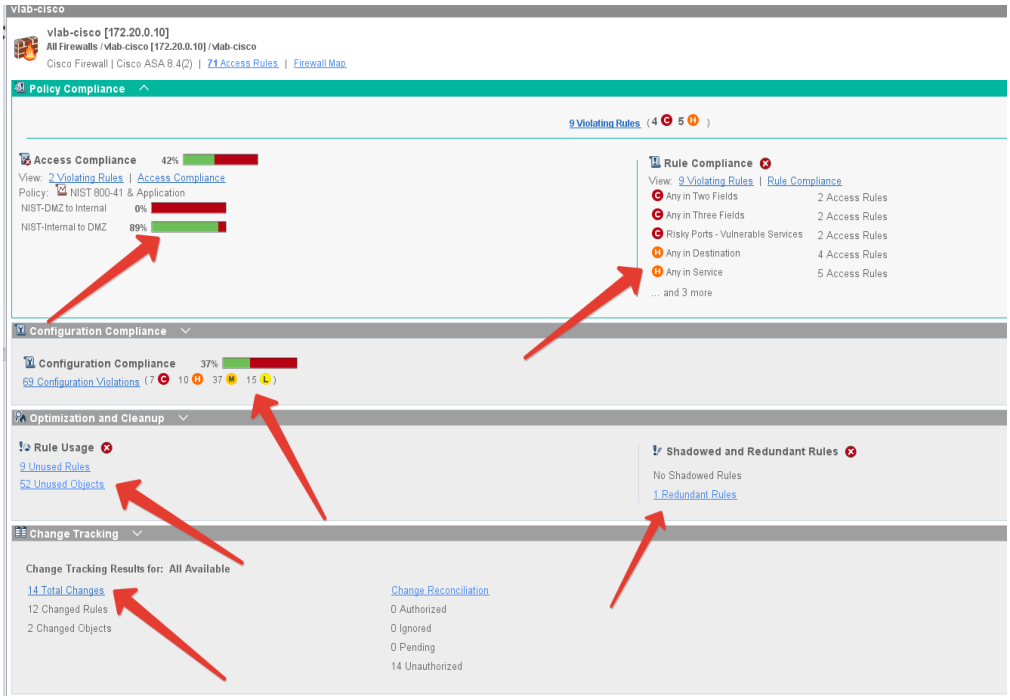


Рисунок 3.9 - Информация Firewall Assurance

В данном межсетевом экране было выявлено следующее:

а) не соответствие международному стандарту NIST 800-41 (см. рисунок 3.10);

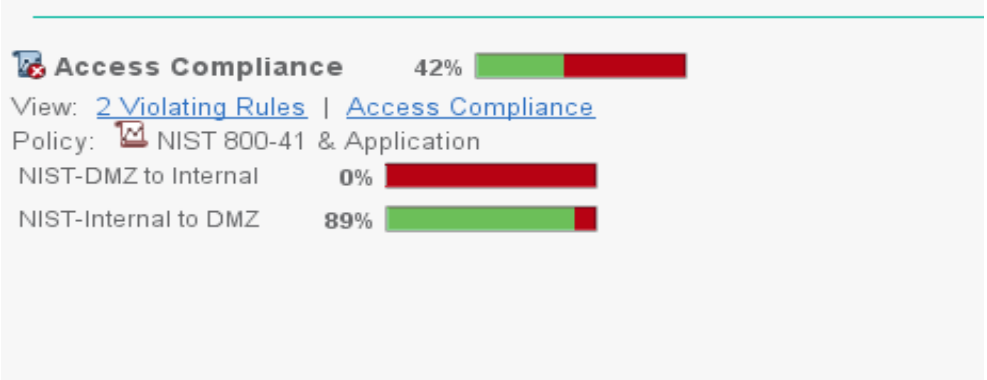


Рисунок 3.10 – Access Compliance (соответствие стандартам)

б) правила в межсетевом экране с широким доступом, а именно “Any” в двух полях и “Any“ в трех полях, порт повышенного риска с уязвимыми сервисами, Any in Destination и т.д. (см. рисунок 3.11);

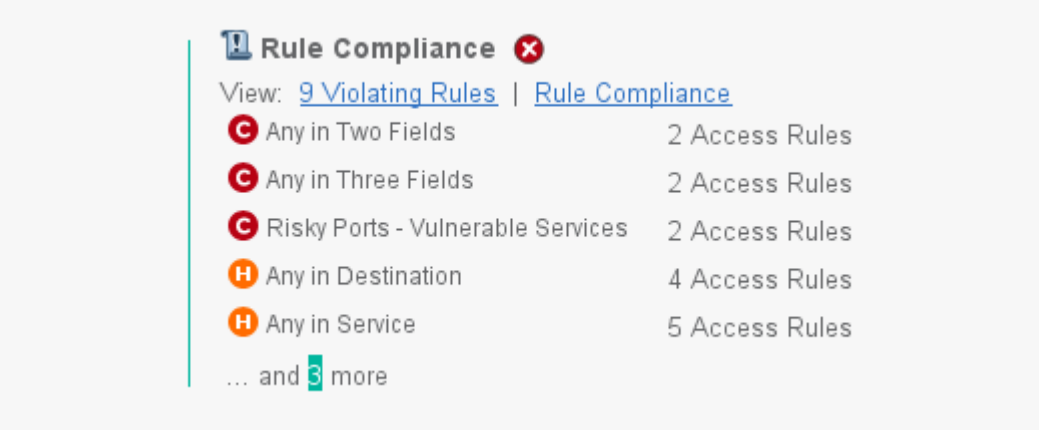


Рисунок 3.11 – Rule Compliance (неправильно настроенные правила)

в) выявлено несоответствие настроек межсетевого экрана согласно рекомендациям производителя сетевого оборудования (см. рисунок 3.12);

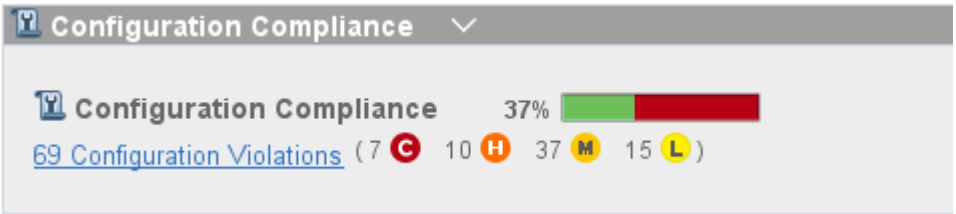


Рисунок 3.12 – Configuration Compliance (статистика правильно настроенной конфигурации МЭ)

г) были выявлены неиспользуемые правила, неиспользуемые объекты, замененные правила и избыточные правила (см. рисунок 3.13);

Рисунок 3.13 – Optimization and Cleanup (статистика правил МЭ)

д) изменения в межсетевых экранах (см. рисунок 3.14);

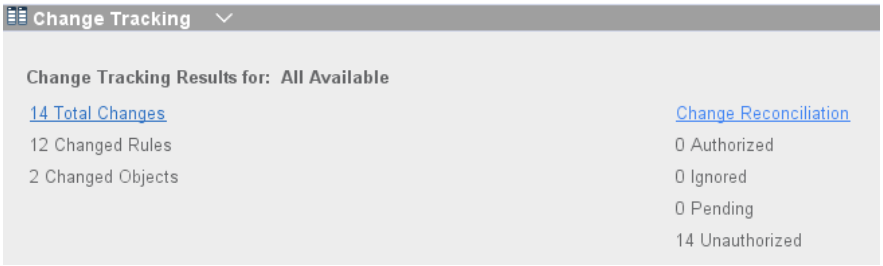
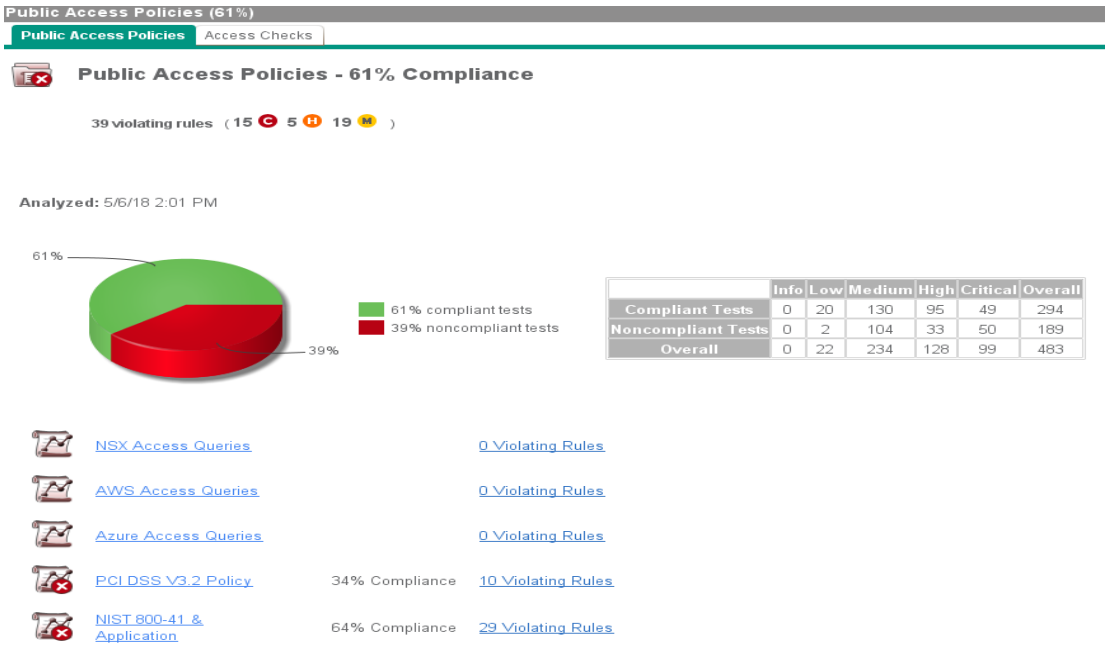


Рисунок 3.14 – Change Tracking (статистика изменения в МЭ)

Далее рассмотрим в деталях весь функционал и особенности

С помощью Access Policies было выявлено множество правил не соответствующих международным стандартам (PCI DSS, NIST, AWS, Azure, NSX) (см. рисунок 3.15).



	Info	Low	Medium	High	Critical	Overall
Compliant Tests	0	20	130	95	49	294
Noncompliant Tests	0	2	104	33	50	189
Overall	0	22	234	128	99	483

Рисунок 3.15 - Access Policies

Политика правил.

Были обнаружены правила не соответствующие рекомендациям международных практик (см. рисунок 3.16).

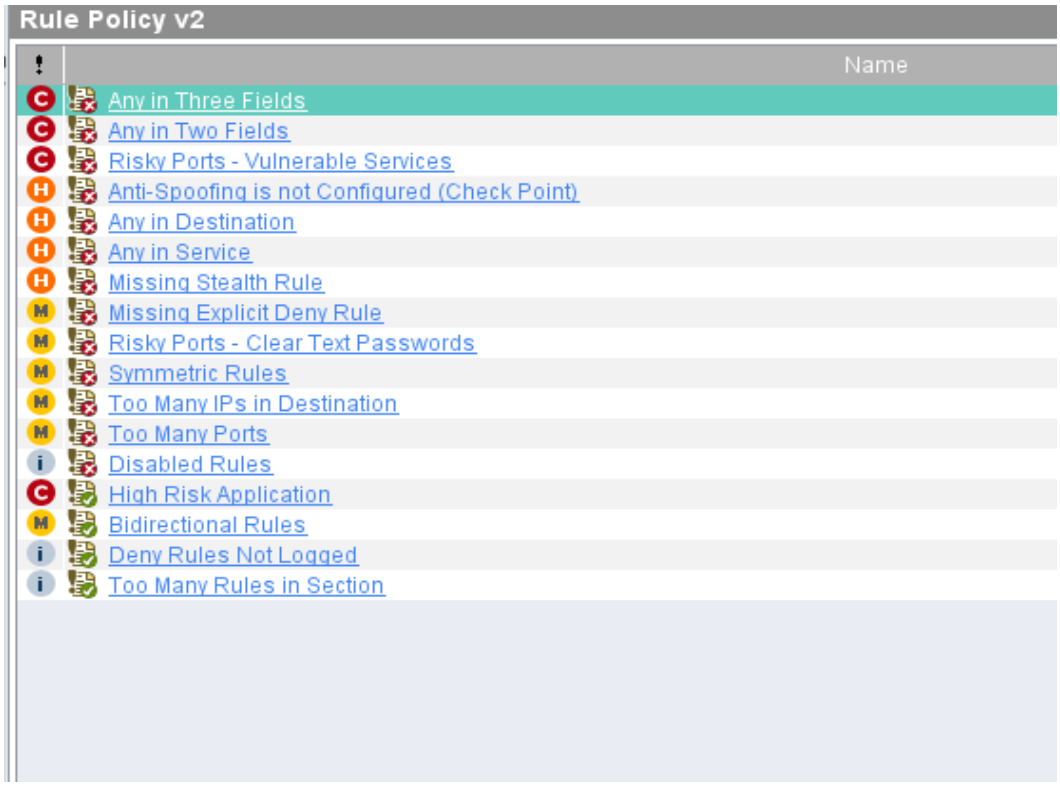


Рисунок 3.16 - Rule Policy

Следующим этапом проверили список плохо сконфигурированных правил межсетевого экрана, что влечет за собой уязвимости в сети. Все пункты обозначены уровнем риска (см. рисунок 3.17).

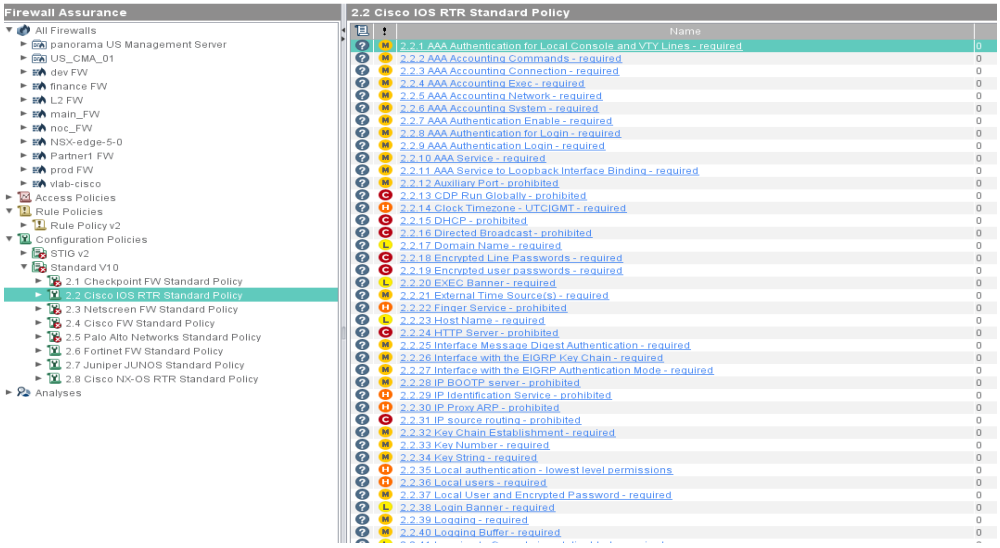


Рисунок 3.17 - Configuration Policies

На основе все информации полученной с сетевого оборудования с системе автоматически моделируется сеть предприятия (см. рисунок 3.18).

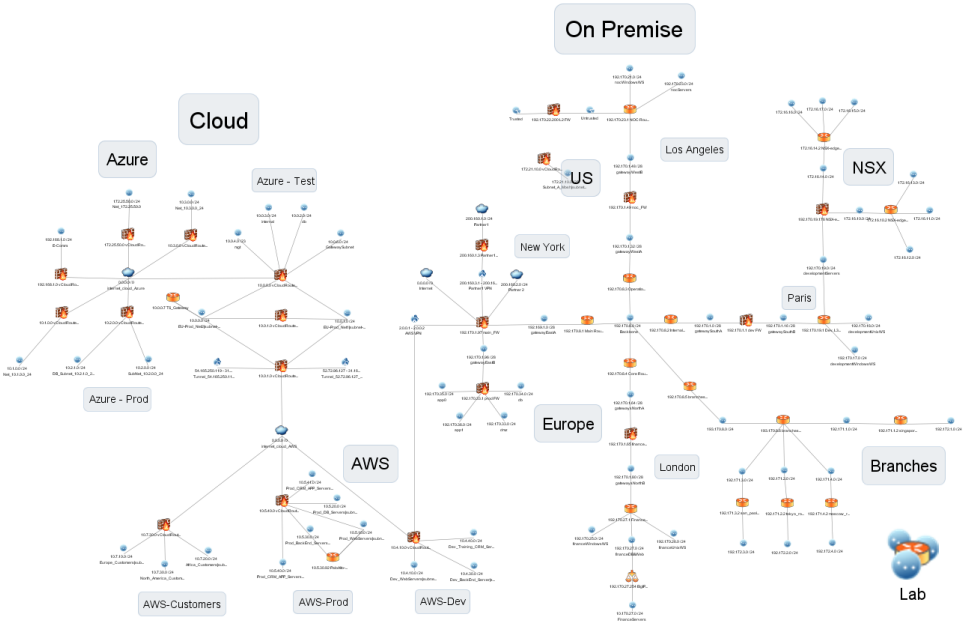


Рисунок 3.18 - Карта сети банка

Смоделированная сеть вручную с помощью сетевого администратора была поделена на сегменты, межсетевые экраны и другое сетевое оборудование.

Была проведена работа по туннелированию сети, которая позволила выявить часть сети недоступной из точки А до точки Б (см. рисунок 3.19).

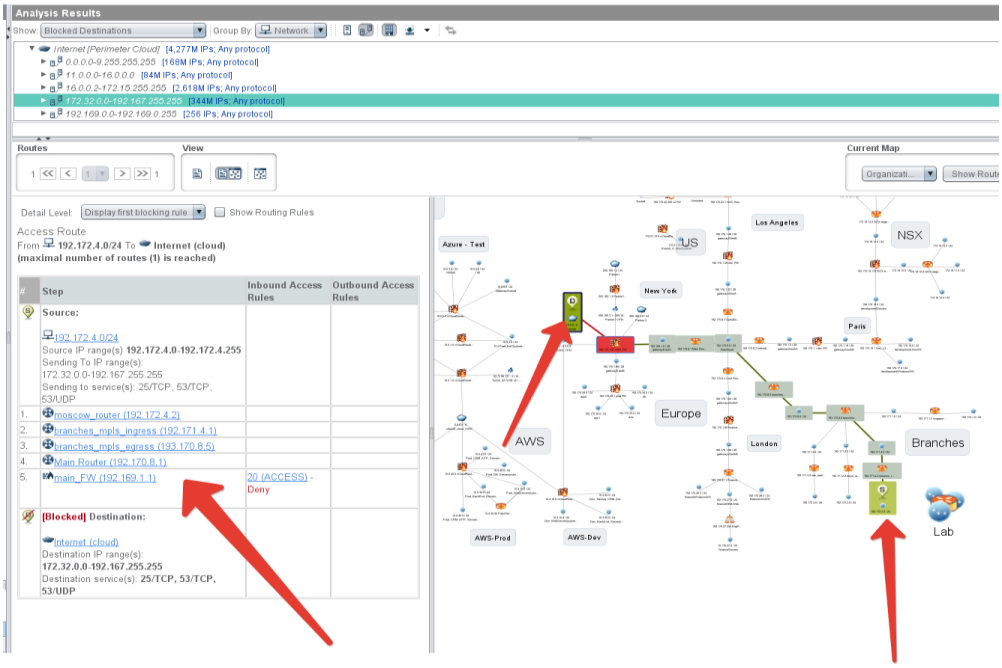


Рисунок 3.19 - Туннелирование

На данном скриншоте видно какие маршрутизаторы участвуют при туннелировании сети и почему нас нет доступа, так как правило 20 (deny_implicit_outbound) в межсетевом экране прописано таким образом что блокирует доступ из точки А до точки Б.

Углубившись в правила есть возможность увидеть какие правила блокируют доступ (см. рисунок 3.20).

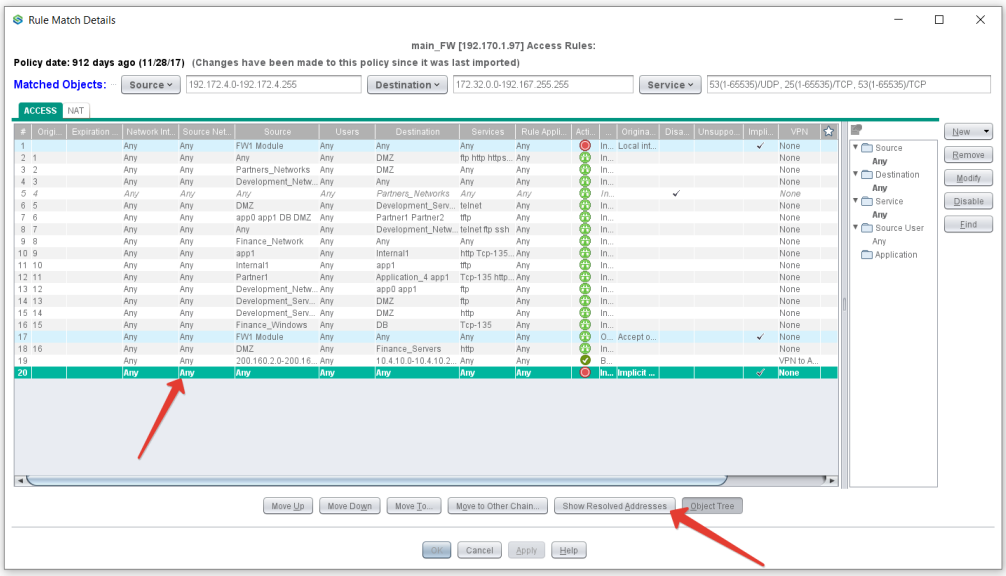


Рисунок 3.20 – Обнаружение блокирующего правила

Следующим этапом мы провели анализ сети на доступ к информационным система, где наглядно виден весь спектр атак. Используя внутренние утилиты атаки “Интернет хакера” на примере определенного актива банка были выявлены вектора атак где визуализировано как и почему злоумышленник получил доступ к активу.

Запустив задачу Analyze Exposure мы получили следующие показания(см. рисунок 3.21).

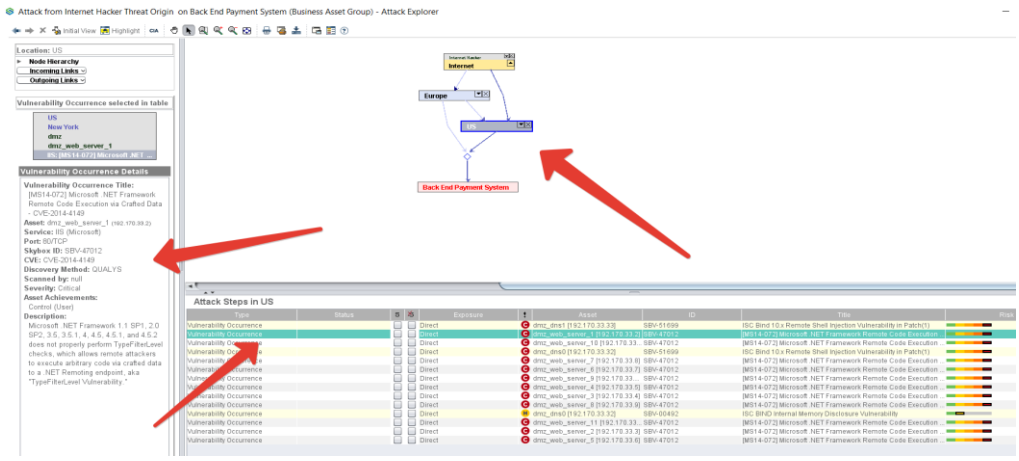


Рисунок 3.21 – Вектор атак злоумышленник

Был выявлен весь спектр атак и то как злоумышленик получил доступ к активу (см. рисунок 3.22).

Vulnerability Occurrence Title:
[MS14-072] Microsoft .NET Framework Remote Code Execution via Crafted Data - CVE-2014-4149
Asset: dmz_web_server_1 (192.170.33.2)
Service: IIS (Microsoft)
Port: 80/TCP
Skybox ID: SBV-47012
CVE: CVE-2014-4149
Discovery Method: QUALYS
Scanned by: null
Severity: Critical
Asset Achievements:
Control (Root)
Description:
Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, and 4.5.2 does not properly perform TypeFilterLevel checks, which allows remote attackers to execute arbitrary code via crafted data to a .NET Remoting endpoint, aka "TypeFilterLevel Vulnerability."

Рисунок 3.22 – Анализ атаки

То есть использовав уязвимости в Framework – сервис IIS Microsoft – Порт 80/TCP злоумышленник получает доступ к учетной записи с правами локального администратора.

Углубившись мы получаем способ решения данной уязвимости в сети (см. рисунок 3.23).

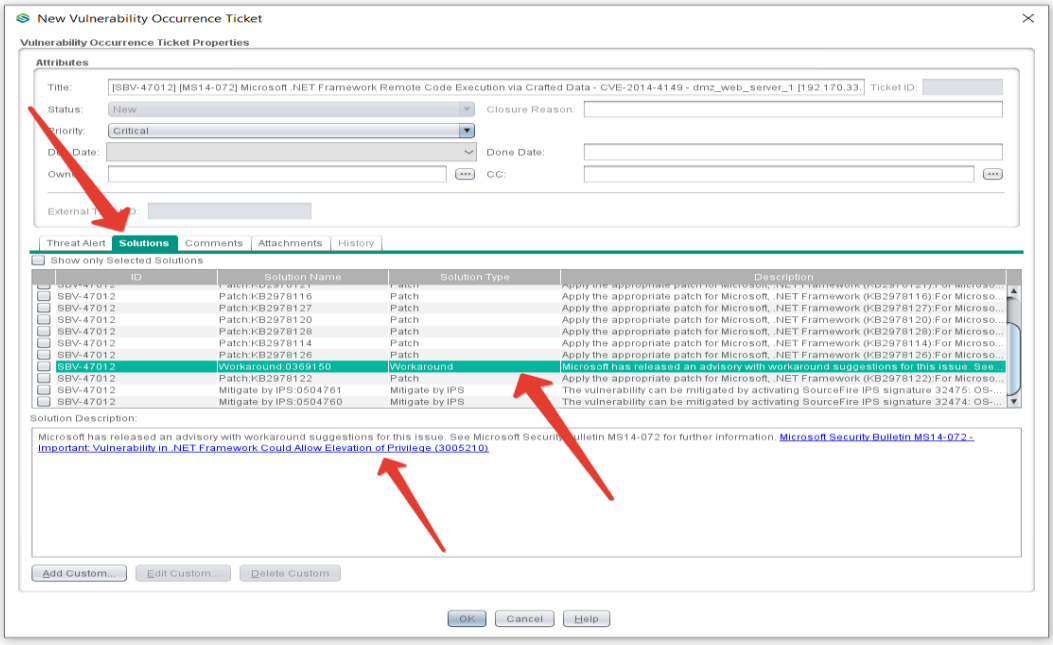


Рисунок 3.23 - Рекомендации решения уязвимостей

Уязвимость SBV-47012 связана с тем, что данный система не получила обновления (патчи) Microsoft в связи с чем появилась возможность атаки “Интернет хакера”.

4. Методы защиты для конкретно выбранной сети

4.1 Пассивный анализ:

- возможности ее реальной эксплуатации в условиях конкретной сети и ее настроек;
- сведений о частоте эксплуатации данной уязвимости;
- сведении о ценности актива, содержащего данную уязвимость и т.д.
- критичности уязвимости;
- наличие готовых инструментов атак (exploits), направленных на эксплуатацию конкретной уязвимости;
- факты атак, в ходе которых зафиксирована эксплуатация конкретной уязвимости.

Контроль соответствия конфигураций межсетевых экранов заданным стандартам конфигурирования и лучшим практикам, включая локальные правила конфигурирования, а также указание причины несоответствия вплоть до конкретных правил на конкретных устройствах:

- выявление правил, содержащих any в 2 или 3 полях, в поле сервис и т.д.;
- выявление настроек, противоречащих рекомендациям производителей с точки зрения безопасности;
- выявление правил, разрешающих передачу паролей в открытом виде и т.д.

Патч-менеджмент:

а) обновление ПО (в которые входит обновление безопасности) во всех устройствах имеющих IP-адрес;

б) анализ на соответствие конфигураций МЭ рекомендациям от вендора. Контроль соответствия конфигураций межсетевых экранов заданным стандартам конфигурирования и лучшим практикам, включая локальные правила конфигурирования, а также указание причины несоответствия вплоть до конкретных правил на конкретных устройствах;

в) анализ на соответствиям международным политикам безопасности. Создание политики сетевого доступа (зон безопасности) и автоматический контроль ее исполнения (встроены стандарты PCI DSS, NIST) на уровне зон безопасности межсетевых экранов с указанием причины несоответствия вплоть до конкретных правил на конкретных устройствах.

Псевдо-атака злоумышленника:

а) эмуляция атаки злоумышленника на ценные активы и выявления векторов атак и способов захвата контроля учетной записи администратора;

б) расчет возможных векторов атак с учетом настроек сетевого оборудования, включая активированные сигнатуры IPS;

в) контроль и автоматизация процесса изменения правил доступа от заведения заявки до ее выполнения, и гарантирует то, что все изменения произведены в полном соответствии с принятым регламентом предоставления сетевого доступа.

- периодический пересмотр правил сетевого доступа;
- выявление изменений правил и настроек, выполненных без соответствующей заявки или согласования;
- формирование рекомендаций по вносимым изменениям конфигураций МЭ при изменении сетевых доступов.

4.2 Технические характеристики оборудования

Межсетевые экраны:

а) Palo Alto 5260:

- пропускная способность брандмауэра — 72,3 Гбит/с (с включенным App-ID1);
- пропускная способность при предотвращении угроз — 30,2 Гбит/с;
- пропускная способность IPSec VPN — 21 Гбит/с;
- максимальное количество сеансов — 32 000 000;
- количество новых сеансов в секунду — 458 000;
- 225 виртуальных маршрутизаторов;
- 25/225 виртуальных систем (базовый вариант/максимум2).

б) Palo Alto 5250 (см. таблицу 4.1):

- пропускная способность брандмауэра — 35,9 Гбит/с (с включенным App-ID1);
- пропускная способность при предотвращении угроз — 20,4 Гбит/с;
- пропускная способность IPSec VPN — 14 Гбит/с;
- максимальное количество сеансов — 8 000 000;
- количество новых сеансов в секунду — 348 000;
- 125 виртуальных маршрутизаторов;
- 25/125 виртуальных систем (базовый вариант/максимум).

CISCO FPR4140-ASA-K9.

Основные характеристики Cisco FPR4140-ASA-K9:

- 25 000 000 одновременных сессий;
- два протокола SSL VPN, осуществляющие симметричное шифрование и ассиметричную криптографию для аутентификации ключей обмена;
- оснащен 8 встроенными GE-портами, 4 портами SFP+, а также 4 портами QSFP;
- виртуальные интерфейсы (VLANs) – 1024;

Таблица 4.1 - Palo Alto 5250

Характеристики	Значения
AC Input Voltage (input Hz)	100-240VAC (50-60Hz)
AC Power Supply Output	1200 Watt/power supply
Max Current	AC power supplies — 6.5A@100-240VAC DC power supplies — 19A@-40 to -60VDC
Max Inrush Current	AC power supplies — 50A@230VAC, 50A@120VAC DC power supplies — 200A@72VDC
Mean Time Between Failure (MTBF)	9.23 Years
Rack Mount (Dimensions)	3U, 19” Standard Rack 5.25”H X 20.5”D X 17.25”W (13.33cm X 52.07cm X 43.81cm)
Weight	46lbs (20.87Kg) System only, 62lbs (28.13Kg) as shipped
Safety	cCSAus, CB IEC60950-1
I/O	PA-5260 | PA-5250 - (4) 100/1000/10G Cu, (16) Gig/10Gig SFP/SFP+, (4) 40G/100G QSFP28 PA-5220 – (4)100/1000/10G Cu, (16) Gig/10Gig SFP/SFP+, (4) 40G QSFP+
Management I/O	PA-5260 | PA-5250 - (2) 10/100/1000, (1) 40G/100G QSFP28 HA, (1) 10/100/1000 out-of-band management, (1) RJ45 console port PA-5220 - (2) 10/100/1000, (1) 40G QSFP+ HA, (1) 10/100/1000 out-of-band management, (1) RJ45 console port
Storage Capacity	240GB SSD, RAID1, System Storage 2TB HDD, RAID1, Log Storage
Power (Max Power Consumption)	870 Watts
Rack Mount (Dimensions)	3U, 19” Standard Rack 5.25”H X 20.5”D X 17.25”W (13.33cm X 52.07cm X 43.81cm)
Weight	46lbs (20.87Kg) System only, 62lbs (28.13Kg) as shipped
Safety	cCSAus, CB IEC60950-1
EMI	FCC Class A, CE Class A, VCCI Class A
Environment	Operating Temperature: 32°F to 122°F (0° to 50°C) Non-Operating Temperature: -20° to 70°C (-4°F to 158°F)

- SSD на 400 GB.

Особенности FPR4140-ASA-K.

FPR4140-ASA-K9 имеет пропускную способность в 25 Гбит/с, один источник питания переменного тока, набор 20 000 IPSec VPN туннелей, с

помощью которых осуществляется аутентификация, проверка целостности и шифрование IP-пакетов, а также снабжен двумя протоколами SSL VPN, осуществляющими симметричное шифрование и ассиметричную криптографию для аутентификации ключей обмена, 8 встроенными Gigabit Ethernet-интерфейсами, 4 SFP+ портами, 4 QSFP-портами, и 1 GE-портом для управления. Кроме того, FPR4140-ASA-K9 обеспечивает 25 000000 соединений в секунду и 350 000 одновременных соединений брандмауэра

Технологии, применяемые в FPR4140-ASA-K9.

Усиленная защита сети с синхронным сканированием местного трафика и усиленным контролем глобальной сети осуществляются при помощи следующих технологий:

− Cisco Firepower Management Center (formerly FireSIGHT) обеспечивает централизованное управление NGFW Firewall NGFW, Cisco Firepower NGIPS и Cisco AMP для сетей. Он также обеспечивает корреляцию угроз для сетевых датчиков и Advanced Malware Protection (AMP) для конечных точек;

− Cisco Firepower Device Manager доступен для локального управления 4100 Series, работающих под управлением программного обеспечения защиты от угроз Cisco Firepower;

− Cisco Adaptive Security Device Manager обеспечивает локальное управление устройствами Cisco Firepower 4100 Series, работающими с программным изображением ASA;

− Cisco Defense Orchestrator обеспечивает последовательное управление политиками безопасности в устройствах Cisco, на которых работает программное обеспечение ASA, что позволяет повысить эффективность управления распределенным предприятием.

CISCO FPR4120-ASA-K9.

Основные характеристики Cisco FPR4110-ASA-K9:

- 15 000 000 одновременных сессий;
- два протокола SSL VPN, осуществляющие симметричное шифрование и ассиметричную криптографию для аутентификации ключей обмена;
- оснащен 8 встроенными GE-портами, 4 портами SFP+, а также 4 портами QSFP;
- виртуальные интерфейсы (VLANs) – 1024;
- SSD на 200 GB.

Особенности FPR4120-ASA-K9.

FPR4120-ASA-K9 имеет пропускную способность в 20 Гбит/с, один источник питания переменного тока, набор 15000 IPSec VPN туннелей, с помощью которых осуществляется аутентификация, проверка целостности и шифрование IP-пакетов, а также снабжен двумя протоколами SSL VPN, осуществляющими симметричное шифрование и ассиметричную криптографию для аутентификации ключей обмена, 8 встроенными Gigabit Ethernet-интерфейсами, 4 SFP+ портами, 4 QSFP-портами, и 1 GE-портом для

управления. Кроме того, FPR4120-ASA-K9 обеспечивает 15 000000 соединений в секунду и 250 000 одновременных соединений брандмауэра.

Технологии, применяемые в FPR4120-ASA-K9.

Усиленная защита сети с синхронным сканированием местного трафика и усиленным контролем глобальной сети осуществляются при помощи следующих технологий:

− Cisco Firepower Management Center (formerly FireSIGHT) обеспечивает централизованное управление NGFW Firewall NGFW, Cisco Firepower NGIPS и Cisco AMP для сетей. Он также обеспечивает корреляцию угроз для сетевых датчиков и Advanced Malware Protection (AMP) для конечных точек;

− Cisco Firepower Device Manager доступен для локального управления 4100 Series, работающих под управлением программного обеспечения защиты от угроз Cisco Firepower;

− Cisco Adaptive Security Device Manager обеспечивает локальное управление устройствами Cisco Firepower 4100 Series, работающими с программным изображением ASA;

− Cisco Defense Orchestrator обеспечивает последовательное управление политиками безопасности в устройствах Cisco, на которых работает программное обеспечение ASA, что позволяет повысить эффективность управления распределенным предприятием.

Маршрутизаторы.

Характеристики CISCO 2951-SEC VPN приведены в таблице 4.2. CISCO 2951-V - в таблице 4.3.

Таблица 4.2 - CISCO 2951-SEC VPN

Характеристики	Значения
1	2
Серия	Cisco 2900 Series ISR
Рекомендуемая замена	ISR4351/K9 Cisco LAN маршрутизатор модульный 3 x GE, 3 x NIM, 1 x ISC, 2 x SM, 3 x SFP, IP Base
Универсальные порты Ethernet	1 x SFP
WAN порты Ethernet	3 x GE
LAN порты Ethernet	Совмещаются с WAN
Слоты интерфейсных карт	4 слота
Память FLASH	256 Мб
Память FLASH максимум	4 Гб
Объем ОЗУ	512 Мб
Память ОЗУ максимум	2 Гб
Гарантия	90 дней Cisco Limited Warranty
Потребляемая мощность номинальная/максимальная	70/340 Ватт
Тип питания	AC 220В/DC 24-60В

Продолжение таблицы 4.2

1	2
Типы поддерживаемых карт	4 слота EHWIC
Слоты DSP ресурсов	3 слота PVDM
Высота RM UNIT	2U
Внутренний сервисный слот	1 слот ISM
Тип установки	Стоечное/настольное
Порты консольные	RJ-45 (RS232), AUX RJ-45(RS232), USB, mini-USB
Сетевой слот NM/SM	2 слота SM
Порты USB	2 x USB 2.0

Таблица 4.3 - CISCO 2951-V

Характеристики	Значения
Серия	Cisco 1900 Series
Рекомендуемая замена	ISR4321 Cisco LAN маршрутизатор модульный 2 x GE, 2 x NIM, 1 x ISC, 1 x SFP, IP Base
WAN порты Ethernet	2 x GE
LAN порты Ethernet	Совмещаются с WAN
Слоты интерфейсных карт	2 слота
Память FLASH	Память FLASH
Объем ОЗУ	512 Мб
Гарантия	1 год Cisco Limited Warranty
Потребляемая мощность номинальная/максимальная	25/80 Ватт
Тип питания	AC 100-240В
Типы поддерживаемых карт	2 слота EHWIC (1 Doublewide)
Высота RM UNIT	1U
Тип установки	Стоечное/настольное
Порты консольные	RJ-45 (RS232)/mini-USB
Порты USB	1 x USB 2.0

Коммутаторы.

Характеристики коммутатора SX350X-12-K9 представлены в таблице 4.4. SRW2016 (SG300-20) в таблице 4.5.

Таблица 4.4 - SX350X-12-K9

Характеристики	Значения
1	2
Производитель	Cisco
Серия	Cisco 350X Series Stackable Managed Switches

Продолжение таблицы 4.4

1	2
Тип коммутатора	Стекируемый
Уровень коммутатора	3 уровень
Матрица коммутации	240 Гбит/с
Универсальные порты Ethernet	2 x comboSFP+
Таблица MAC адресов	32000 MAC адресов
Стекирование	Stack/4
Протоколы VLAN	802.1Q
Максимальный VLAN ID	4094
Коммутация Мпакетов/с (MPPS)	178,56 MPPS
Порты консольные	RJ-45
Память FLASH	256 Мб
Объем ОЗУ	512 Мб
Гарантия	Cisco Limited Lifetime Hardware Warranty
Тип питания	AC 100-240В
Тип установки	Стоечное
Высота RM UNIT	1U

Таблица 4.5 - SRW2016 (SG300-20)

Характеристики	Значения
Производитель	Cisco
Серия	Cisco 350X Series Stackable Managed Switches
Тип коммутатора	Стекируемый
Уровень коммутатора	3 уровень
Матрица коммутации	240 Гбит/с
Универсальные порты Ethernet	2 x comboSFP+
Таблица MAC адресов	32000 MAC адресов
Стекирование	Stack/4
Протоколы VLAN	802.1Q
Максимальный VLAN ID	4094
Коммутация Мпакетов/с (MPPS)	178,56 MPPS
Порты консольные	RJ-45
Память FLASH	256 Мб
Объем ОЗУ	512 Мб
Гарантия	Cisco Limited Lifetime Hardware Warranty
Тип питания	AC 100-240В
Тип установки	Стоечное
Высота RM UNIT	1U

4.3 Оценка защищенности при помощи рисков

Рассмотрим защищенность системы с точки зрения риска. Заметим, что использование теории рисков для оценки уровня защищенности на сегодняшний день является наиболее часто используемым на практике подходом. Риск (R) — это потенциальные потери от угроз защищенности:

$$R(p) = C_{инф} \cdot \lambda_{взл.}.$$

По существу, параметр риска здесь вводится как мультипликативная свертка двух основных параметров защищенности.

С другой стороны, можно рассматривать риск как потери в единицу времени

$$R(l)=C_{инф} \cdot l_{взл} ,$$

где lвзл — интенсивность потока взломов (под взломом будем понимать удачную попытку реализации угрозы информации).

В качестве основного критерия защищенности будем использовать коэффициент защищенности (D), показывающий относительное уменьшение риска в защищенной системе по сравнению с незащищенной системой.

$$D\% = \left(1 - \frac{R_{зац}}{R_{нез}}\right) \cdot 100\%, \qquad (4.1)$$

где Rзащ – риск в защищенной системе;

Rнез – риск в незащищенной системе.

Таким образом, в данном случае задача оптимизации будет сводится к выбору параметров сети, снижение цены применяемых средств защиты (Цзад) при наибольшем коэффициенте защиты.

Для решения задачи введем некоторые ограничения на цену средств защиты и производительность системы.

Целевая функция выбрана исходя из того, что именно она отражает основное функциональное назначение системы защиты — обеспечение безопасности информации.

Производительность системы Псзи рассчитывается с применением моделей и методов теории массового обслуживания и теории расписаний (в зависимости от того, защищается ли система оперативной обработки, либо реального времени) [32]. На практике возможно задание ограничения по производительности (влияние на загрузку вычислительного ресурса защищаемой системы) не непосредственно в виде требуемой производительности системы, а как снижение производительности (dПсзи) информационной системы от установки системы защиты.

Такой принцип сведения задачи к однокритериальной целесообразен, т.к. в любом техническом задании на разработку системы защиты указывается, в какой мере система защиты должна оказывать влияние на производительность системы. Как правило, внедрение системы защиты не должно снижать производительность системы более чем на 10%. Кроме того, обычно вводится ограничение на стоимость системы защиты.

Если рассчитанное значение коэффициента защищенности (D) не удовлетворяет требованиям к системе защиты, то в допустимых пределах можно изменять заданные ограничения и решить задачу методом последовательного выбора уступок. При этом задается приращение стоимости и снижение производительности:

$$Ц_{зад} = Ц_{зад} + DЦ,$$

$$П_{зад} = П_{зад} - DП \text{ или } dПзад = dП_{зад} + DdП.$$

В таком виде задача решается в результате реализации итерационной процедуры путем отсеивания вариантов, не удовлетворяющих ограничительным условиям, и последующего выбора из оставшихся варианта с максимальным коэффициентом защищенности.

Теперь выразим коэффициент защищенности через параметры угроз. В общем случае в системе присутствует множество видов угроз. В этих условиях зададим следующие величины:

- W – количество видов угроз, воздействующих на систему;
- $C_i(i=\overline{1,w})$ – стоимость (потери) от взлома i-того вида;
- $\lambda_i(i=\overline{1,w})$ – вероятность возникновения взломов i-того вида, соответственно;
- $p_i(i=\overline{1,w})$ – вероятность отражения угроз i-того вида системой защиты.

Соответственно, для коэффициента потерь от взломов системы защиты имеем:

$$R(p) = \sum_{i}^{N} R_i(p) = \sum_{i}^{N} C_i \cdot p_{\text{взл } i},$$

где R_i (p) – коэффициент потерь от взлома i-того типа; показывает, какие в среднем потери приходятся на один взлом i-того типа.

Соответственно, для коэффициента потерь от взломов системы защиты в единицу времени имеем:

$$R(\lambda) = \sum_{i}^{W} R_i(\lambda) = \sum_{i}^{W} C_i \cdot \lambda_{\text{ВЗЛ } i},$$

где $R_i(\lambda)$ – коэффициент потерь от взломов i-того типа в единицу времени.

Для незащищенной системы $\lambda_{взлi}=\lambda_i$, для защищенной системы $\lambda_{защi}=\lambda_i\cdot(1-p_i)$. Соответственно, из (4.2) имеем:

$$D = 1 - \frac{\sum_i^w C_i \cdot Q_i \cdot (1 - p_i)}{\sum_i^w C_i \cdot Q_i} = 1 - \frac{\sum_i^w C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_i^w C_i \cdot \lambda_i} \quad . \qquad (4.2)$$

Если в качестве исходных параметров заданы вероятности появления угроз, то коэффициент защищенности удобно считать через вероятности появления угроз. Если же в качестве исходных параметров заданы интенсивности потоков угроз li , то, естественно, коэффициент защищенности считается через интенсивность.

Очевидно, что при использовании любого математического метода проектирования системы защиты необходимо задавать определенные исходные параметры для оценки ее защищенности. Однако именно с этим связаны основные проблемы формализации задачи синтеза системы защиты. Поэтому мы отдельно рассмотрим основные пути решения данной задачи, рассмотрим возможные способы задания вероятностей и интенсивностей угроз.

Основной проблемой проведения количественной оценки уровня защищенности является задание входных параметров для системы защиты — вероятностей и интенсивностей угроз. Рассмотрим возможные способы задания вероятностей и интенсивностей угроз.

Метод статистической оценки λ i и pi .

Основным способом задания вероятностей угроз и вероятностей предотвращения взломов pi является получение этих значений на основе имеющейся статистики угроз безопасности информационных систем, в которых реализуется система защиты. Если существует статистика для аналогичной информационной системы, то задавать исходные параметры для оценки защищенности можно на ее основе. При этом желательно, чтобы сходные информационные системы эксплуатировалась на предприятиях со сходной спецификой деятельности.

Однако при практической реализации такого подхода возникают следующие сложности. Во-первых должен быть собран весьма обширный материал о происшествиях в данной области. Во-вторых данный подход оправдан далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если же система сравнительно невелика и эксплуатирует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз могут оказаться недостоверными

Заметим, что статистика угроз периодически публикуется достаточно авторитетными изданиями, т.е. всегда существуют исходные данные для использования данного подхода для большинства приложений средств защиты информации. Обычно эта статистика доступна в Интернете на сайтах специализированных организаций.

Если же необходимая статистика по угрозам безопасности отсутствует, то можно воспользоваться одним из других подходов, описанных далее.

Подход первый. В рамках данного подхода предусмотрено два разных способа.

Первый способ — это способ равных интенсивностей "li = a , a = const. При этом способе для расчета защищенности константа a может быть выбрана любой. В формуле (3.4) она будет вынесена за скобки и в конечном итоге сократится, так что защищенность в данном случае будет зависеть только от потерь:

$$D = 1 - \frac{\sum_i^w C_i \cdot \lambda_i \cdot (1-p_i)}{\sum_i^w C_i \cdot \lambda_i} = 1 - \frac{\sum_i^w C_i \cdot \alpha \cdot (1-p_i)}{\sum_i^w C_i \cdot \alpha} = \tag{4.3}$$

$$1 - \frac{\alpha \sum_i^w C_i \cdot (1-p_i)}{\alpha \sum_i^w C_i} = 1 - \frac{\sum_i^w C_i \cdot (1-p_i)}{\sum_i^w C_i \cdot}$$

Второй способ — это способ пропорциональности потерям

li = a·Ci , a = const.

При этом способе предполагается, что чем больше потери от взлома, тем чаще осуществляются попытки несанкционированного доступа к этой информации. То есть интенсивности потоков угроз прямо пропорциональны потерям. В этом случае защищенность будет зависеть от квадрата потерь:

$$D = 1 - \frac{\sum_i^w C_i \cdot \lambda_i \cdot (1-p_i)}{\sum_i^w C_i \cdot \lambda_i} = 1 - \frac{\sum_i^w C_i \cdot \alpha \cdot C_i \cdot (1-p_i)}{\sum_i^w C_i \cdot \alpha \cdot C_i} = \tag{4.4}$$

$$1 - \frac{\alpha \sum_i^w {C_i}^2 \cdot (1-p_i)}{\alpha \sum_i^w {C_i}^2} = 1 - \frac{\sum_i^w {C_i}^2 \cdot (1-p_i)}{\sum_i^w {C_i}^2 \cdot}$$

Исходные данные расчета приведены в таблице 4.6.

Для оценки защищенности воспользуемся уравнением (4.3). Рассчитаем (Rзащ) риск в защищенной системе и (Rнез) риск в незащищенной системе.

Таблица 4.6 - Исходные данные

Виды атак	Вероятность атаки λi	Цена взлома, C_i	Средства защиты, вероятность отражения угрозы, p_i			
			Межсетевой экран	Сервер антивирусной защиты	VPN шлюз	Сервер обновлений
DOS	0,03		0,8	0,95	0,99	0,95
Вирусы	0,1		0,9	0,9	0,9	0,9
IP Spoofing	0,02		0,7	0,9	0,9	0,95
DNS Spoofing	0,05		0,9	0,8	0,9	0,9
Потеря данных	0,1		0,8	0,8	0,8	0,9
Нарушение конфиденциальности данных	0,08		0,9	0,8	0,3	0,9

Затем определим коэффициент защищенности для разных средств защиты.

$$R_{\text{НЕЗ}} = \sum_i^N C_i \cdot \lambda_i,$$

$$R_{\text{ЗАЩ}} = \sum_i^N C_i \cdot \lambda_i \cdot (1 - p_i).$$

Выполним расчет для всех видов угроз при одинаковой цене потерь C i =const=100

$$R_{\text{НЕЗ}}=100\cdot(0{,}03+0{,}1+0{,}02+0{,}05+0{,}1+0{,}08)=38.$$

Риск потерь рассчитаем для случаев с различными средствами защиты.

При применении межсетевого экрана:

$$R_{\text{ЗАЩ1}}=100\cdot(0{,}03\cdot(1-0{,}8)+0{,}1\cdot(1-0{,}9)+0{,}02\cdot(1-0{,}7)+0{,}05\cdot(1-0{,}9)+ 0{,}1\cdot(1-0{,}8)+ +0{,}08\cdot(1-0{,}9))=100\cdot(0{,}006+0{,}01+0{,}006+0{,}005+0{,}02+0{,}008)=5{,}5.$$

$$D = \left(1 - \frac{R_{\text{ЗАЩ}}}{R_{\text{НЕЗ}}}\right) \cdot 100\% = \left(1 - \frac{5{,}5}{38}\right) \cdot 100\% = 85{,}6(\%).$$

При применении Антивирусного сервера

$$R_{\text{ЗАЩ1}}=100\cdot(0{,}03\cdot(1-0{,}95)+0{,}1\cdot(1-0{,}9)+0{,}02\cdot(1-0{,}9)+0{,}05\cdot(1-0{,}9)+ 0{,}1\cdot(1-0{,}8)+ 0{,}08\cdot(1-0{,}8))=100\cdot(0{,}0015+0{,}01+0{,}002+0{,}005+0{,}02+0{,}016)=6{,}8.$$

$$D = \left(1 - \frac{R_{\text{ЗАЩ}}}{R_{\text{НЕЗ}}}\right) \cdot 100\% = \left(1 - \frac{6{,}8}{38}\right) \cdot 100\% = 82{,}1(\%).$$

При применении VPN шлюза

$$R_{\text{ЗАЩ1}}=100\cdot(0{,}03\cdot(1-0{,}99)+0{,}1\cdot(1-0{,}9)+0{,}02\cdot(1-0{,}9)+0{,}05\cdot(1-0{,}9)+ 0{,}1\cdot(1-0{,}8)+ +0{,}08\cdot(1-0{,}3))=100\cdot(0{,}0003+0{,}01+0{,}002+0{,}005+0{,}02+0{,}056)=9{,}3.$$

$$D = \left(1 - \frac{R_{\text{ЗАЩ}}}{R_{\text{НЕЗ}}}\right) \cdot 100\% = \left(1 - \frac{9{,}3}{38}\right) \cdot 100\% = 75{,}5(\%).$$

При применении сервера обновлений

$$R_{\text{ЗАЩ1}}=100\cdot(0{,}03\cdot(1-0{,}95)+0{,}1\cdot(1-0{,}9)+0{,}02\cdot(1-0{,}95)+0{,}05\cdot(1-0{,}9)+ 0{,}1\cdot(1-0{,}9)+ +0{,}08\cdot(1-0{,}9))=100\cdot(0{,}0015+0{,}01+0{,}001+0{,}005+0{,}01+0{,}008)=3{,}5$$

$$D = \left(1 - \frac{R_{\text{ЗАЩ}}}{R_{\text{НЕЗ}}}\right) \cdot 100\% = \left(1 - \frac{3{,}5}{38}\right) \cdot 100\% = 90{,}7\%$$

Результаты сведены в таблицу 4.7.

Таблица 4.7

Средства защиты	Межсетевой экран	Сервер антивирусной защиты	VPN шлюз	Сервер обновлений
$R_{\text{НЕЗ}}$	38	38	38	38
$R_{\text{ЗАЩ1}}$	5,5	6,8	9,3	3,5
D	85,6%	82,1%	75,5%	90,7%

Согласно моим расчетам наибольшую вероятность отражения угроз обеспечивает своевременное серверное обновление, а именно патч информационной безопасности от того или иного производителя.

5 Безопасность жизнедеятельности

5.1 Анализ условий труда

Тема данной дипломной работы Моделирование и анализ защищенности локальной сети банка с использованием программы SkyBox. ТОО «Акнур Секъюрити» в городе Алматы».

Целью данного проекта является разработать план проекта, создать условия для сетевых администраторов и офицеров безопасности по своевременному обнаружению уязвимостей и плохой конфигурации сетевого оборудования. Весь комплекс мероприятий, это интеллектуальный труд,

который подразумевает разработку проекта не для продажи, а значит не ставит целью получение материального дохода от работы. Проект разрабатывается для того чтобы инфраструктура банка была защищена от вторжения из вне хакерами, вредоносными системами и инсайдерами.

5.2 Рациональная организация рабочего места оператора

В помещении установлено 9 ЭВМ, подключенных к локальной сети. Поскольку диспетчер весь рабочий день взаимодействует непосредственно с ЭВМ, то очень важно правильно организовать его рабочее место. С точки зрения учета человеческого фактора рабочее место диспетчера обладает рядом эргономических свойств и показателей. Эргономичность связана с показателями производительности, надежности и экономичности эксплуатации. Поэтому при конструировании и размещении рабочих мест предусмотрены меры, предупреждающие или снижающие преждевременное утомление работающего человека, предотвращающие возникновение у него психофизиологического стресса, а также появление ошибочных действий. Такая конструкция рабочего места обеспечивает быстроту, безопасность, простоту и экономичность технического обслуживания, полностью отвечать функциональным требованиям и предполагаемым условиям эксплуатации.

Согласно нормативам конструкция рабочего места и взаимное расположение всех его элементов соответствуют антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. Данные помещения обладают достаточной, для функционирования трудовой деятельности, площадью. Данное размещение оборудования, рабочих столов диспетчеров является удобным и оптимальным для выполнения рабочих обязанностей сотрудников.

При проектировании письменного стола учитываестся следующее: высота стола выбрана с учетом возможности сидеть свободно, в удобной позе, при необходимости опираясь на подлокотники;
нижняя часть стола сконструирована так, чтобы инженер удобно сидел, не был вынужден поджимать ноги; поверхность стола обладает свойствами, исключающими появление бликов в поле зрения инженера; конструкция стола предусматривает наличие выдвижных ящиков (не менее 3 для хранения документации, листингов, канцелярских принадлежностей, личных вещей).

Параметры рабочего места были выбраны в соответствии с антропометрическими характеристиками. При использовании этих данных в расчетах исходим из максимальных антропометрических характеристик.

Система навигации эксплуатируется 24 часа в сутки, и для технического обслуживания задействовано 2 человек. Инженеры по эксплуатации работают в одну дневную смену по 8 часов в сутки, 5 дней в неделю с перерывом на обед.

При конструировании рабочего места диспетчера создадим следующие условия: достаточное рабочее пространство для работающего человека, позволяющее осуществлять все необходимые движения и перемещения при

эксплуатации и обслуживании оборудования; достаточные физические, зрительные и слуховые связи между работающим человеком и оборудованием, а также между людьми в процессе выполнения общей трудовой задачи; оптимальное размещение рабочих мест в производственных помещениях, а также безопасные и достаточные проходы для работающих людей; необходимое естественное и искусственное освещение для выполнения трудовых задач технического обслуживания; допустимый уровень акустического шума и вибрации, создаваемых оборудованием рабочего места или другими источниками шума и вибрации.

На рабочем месте оператора используем:

-средства отображения информации (дисплей);

-средства связи и передачи информации (телефонный аппарат, модем);

-средства документирования и хранения информации (принтеры, дисковые накопители);

-вспомогательное оборудование.

Рабочее место оператора организуем следующим образом. Дисплей оборудован поворотной площадкой, позволяющей перемещать его в горизонтальной и вертикальной плоскостях. Дисплей разместим на столе так, чтобы расстояние наблюдения информации на экране было в пределах 450-500 мм. Экран дисплея расположим так, чтобы угол между нормалью к центру экрана и горизонтальной линией взгляда составлял 20 градусов. Клавиатуру расположим на столе или на подставке так, чтобы высота клавиатуры по отношению к полу составляла 650-800 мм, наклон клавиатуры сделаем в пределах 5-10 градусов.

Рациональная организация рабочего места оператора изображена на рисунке 5.1.

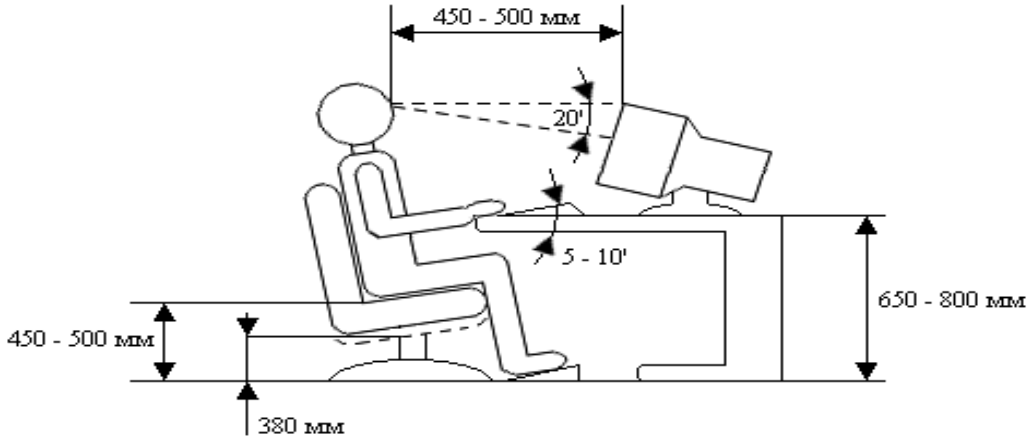


Рисунок 5.1 – Рациональная организация рабочего места оператора

5.3 Анализ искусственного освещения

Правильно спроектированное и выполненное производственное освещение улучшает условия зрительной работы, снижает утомляемость,

способствует повышению производительности труда, благотворно влияет на производственную среду, оказывая положительное психологическое воздействие на работающего, повышает безопасность труда и снижает травматизм.

Недостаточность освещения приводит к напряжению зрения, ослабляет внимание, приводит к наступлению преждевременной утомленности. Чрезмерно яркое освещение вызывает ослепление, раздражение и резь в глазах. Неправильное направление света на рабочем месте может создавать резкие тени, блики, дезориентировать работающего. Все эти причины могут привести к несчастному случаю или профзаболеваниям, поэтому столь важен правильный расчет освещенности.

Естественное и искусственное освещение нормируется в зависимости от характеристики зрительной работы, наименьшего размера объекта различения, фона контраста объекта с фоном. Для естественного освещения нормируется коэффициент естественного освещения, причём для бокового освещения нормируется минимальное значение КЕО, а для верхнего и комбинированного - среднее значение.

Для каждого помещения строится кривая распределения КЕО и освещенности в характерном разрезе помещения - фронтальная плоскость, проходящая по середине помещения перпендикулярно плоскости остекления. Измерение Евнутреннего осуществляется на уровне 0. 8 м от уровня пола. Нормированной характеристикой для искусственного освещения является минимальная освещённость на рабочем месте Emin (люкс).

Освещённость на рабочем месте соответствует характеру зрительной работы; равномерное распределение яркости на рабочей поверхности и отсутствие резких теней; величина освещения постоянна во времени (отсутствие пульсации светового потока); оптимальная направленность светового потока и оптимальный спектральный состав; все элементы осветительных установок долговечны, взрыво-, пожаро-, элекгробезопасны.

Кроме того, все поле зрения освещено достаточно равномерно – это основное гигиеническое требование. Иными словами, степень освещения помещения и яркость экрана компьютера одинаковы, т.к. яркий свет в районе периферийного зрения значительно увеличивает напряженность глаз и, как следствие, приводит к их быстрой утомляемости.

5.4 Разработка эвакуационных путей

Для обеспечения безопасности эвакуации в проекте рассчитано время эвакуации людей из рабочих помещений. В главном офисе банка работают – 618 человек.

Здание 4 этажное, с размерами в коридорах шириной 2 м, в которых есть схема эвакуации людей при пожаре на каждом этаже, как показано на рисунке 5.2. Кабинет объемом 36м3 расположен на четвертом этаже в прямой близости от лестницы, которая ведет до первого этажа. В кабинете работают 9 человек.

Таблица 5.1 – Информация по количеству людей и этажей

Количество людей находящихся в здании Этаж	Количество человек
4	185
3	207
2	150
1	76

Рисунок 5.2 – План эвакуации

По разряду рабочее помещение относится с малой пожароопасностью и II степени огнестойкости. В зданиях II степени огнестойкости приемлемая длительность эвакуации tдоп ≤ 3мин[7].

Период замедления начала эвакуации примем как 1,1 мин с учетом этого, то что сооружение обладает механическую систему сигнализации и уведомления о ЧС.

$$t_p = t_{н.э} + t_1 + t_d + t_2 + t_3 \ldots t_i; \quad (5.1)$$

где tp – время замедления начала эвакуации;

t1 – время перемещения потока на начальном участке, мин;

t2, t3,... ti – период перемещения потока в любом из последующих после 1-ого участка пути, мин.

С целью расчета времени перемещения людей по начальному участку, учитывая габаритные размеры кабинета 6х6 м, обуславливается плотность перемещения людского потока на начальном участке по формуле (5.2)

$$D=N1\cdot fL/1\cdot b1=9\cdot 0/16\cdot 6=0{,}03 \text{ (м2/м2)} \qquad (5.2)$$

где N1 – кол-во человек на начальном участке, чел.;

f – средний участок горизонтального отображения человека, 0.1 м2/чел.;

L1 и b1 – длина и ширина начального участка пути, м.

Скорость перемещения при плотности 0,03 м2/м2 составляет 100 м/мин, с интенсивностью перемещения 1 м/мин, отсюда время перемещения по начальному участку

$$t1=L1/V1=6/100=0{,}06 \text{ (мин).} \qquad (5.3)$$

Длина проема в двери примем как ноль. Самая осуществимая интенсивность перемещения через проем в стандартных обстоятельствах gmax=19,6 м/мин, интенсивность перемещения через проем шириной 1,2 м рассчитывается

$$q_d=2{,}5+3{,}25\cdot b=2{,}5+3{,}25\cdot 1{,}2=7 \text{ (м/мин).}$$

где qd ≤ qmax , соответственно перемещение в проеме беспрепятственное.

Период перемещения через проем рассчитывается по формуле

$$tdl=N\cdot f/q\cdot b=9\cdot 0\cdot 1/7\cdot 1{,}2=0{,}11 \text{ (мин).} \qquad (5.4)$$

В связи с тем, что на четвертом этаже работают 185 человек, плотность потока работающих четвертого этажа будет

$$D=N1\cdot f/L1\cdot b1=185\cdot 0\cdot 1/40\cdot 2=0{,}23 \text{ (м2/м2).}$$

Скорость перемещения равняется 60 м/мин, насыщенность перемещения 12 м/мин, отсюда период перемещения по 2-му участку (из коридора на лестницу) будет равна:

$$t2=L1/V1=40/60=0{,}7 \text{ (мин).}$$

Чтобы определить скорости перемещения по лестнице определяется интенсивность перемещения на третьем участке по формуле

$$qi=qi-1\cdot bi-1/bi=5\cdot 2/1{,}5=8{,}3 \text{ (м/мин).}$$

Следует, что на лестничной клетке скорость потока уменьшается до 90 м/мин. Период перемещения по лестнице

$$t3=L3/V3=6/90=0{,}06 \text{ (мин).} \qquad (5.5)$$

В проходе на третий этаж осуществляется объединение с потоком, которая движется по третьему этажу. Насыщенность человеческого потока для третьего этажа

$$D=N4\cdot f/L4\cdot b4=207\cdot 0\cdot 1/40\cdot 2=0{,}25 \text{ (м2/м2),}$$

$$qi=qi-1\cdot bi-1/bi=5\cdot 2/1\cdot 5=8{,}3 \text{ (м/мин),.}$$

$$t4=L4/V4=6/18=0{,}3 \text{ (мин).}$$

При переходе на второй этаж следует объединение с потоком, движущихся по второму этажу. Насыщенность человеческого потока для второго этажа

$$D=N5\cdot f/L5\cdot b5=150\cdot 0{,}1/40\cdot 2=0{,}18 \text{ (м2/м2),}$$

$$t5=L5/V5=6/18=0{,}3 \text{ (мин).} \qquad (5.6)$$

На первом этаже образуется смешивание с людским потоком, движущихся по первому этажу. Насыщенность потока для первого этажа

$$D=N6\cdot f/L6\cdot b6=76\cdot 0{,}1/40\cdot 2=0{,}1 \text{ (м2/м2).}$$

При этом напряженность перемещения будет около 8 м/мин.

Во время перехода на 6-й участок произойдет слияние людей, отсюда насыщенность перемещения рассчитаем по формуле :

$$qi\Sigma q \quad -1\cdot bi-1/bi= (8{,}3\cdot 1{,}5)+(8\cdot 2)/2=11{,}2 \text{ (мин).}$$

Скорость перемещения равняется 18 м/мин, исходя из этого скорость перемещения по коридору 1-ого этажа:

$$t6=L6/V6=40/18=2{,}2 \text{ (мин).}$$

Тамбур с выходом на улицу обладает ширину 1,2 метров, а время перемещения по тамбуру составит:

$$tdl = N \cdot f / q \cdot b = 618 \cdot 0{,}1 / 7 \cdot 1{,}2 = 7{,}3 \text{ (мин)}.$$

Расчетный период эвакуации определяется по формуле

$$tp = 1{,}1 + 0{,}06 + 0{,}11 + 0{,}7 + 0{,}6 + 0{,}3 + 0{,}3 + 2{,}2 + 7{,}3 = 12{,}5 \text{ (мин)}. \quad (5.7)$$

5.5 Обеспечение средствами пожаротушения

Согласно СНиП 2.04.09-84 здание по степени опасности развития пожара от функционального назначения и пожарной нагрузки горючих материалов, относится к 1-ой группе категории D. В соответствии с требованиями правил пожарной безопасности помещение оборудованы углекислотными огнетушителями ОУ-5 с учетом того, что один огнетушитель на 100 м2 . Общая площадь помещения управления составляет 35 м2 таким образом устанавливаются 1 огнетушитель. В качестве огнетушащего вещества применяется комбинированный углекислотно- хладоновый состав. Размещение огнетушителей изображено на рисунке 5.3.

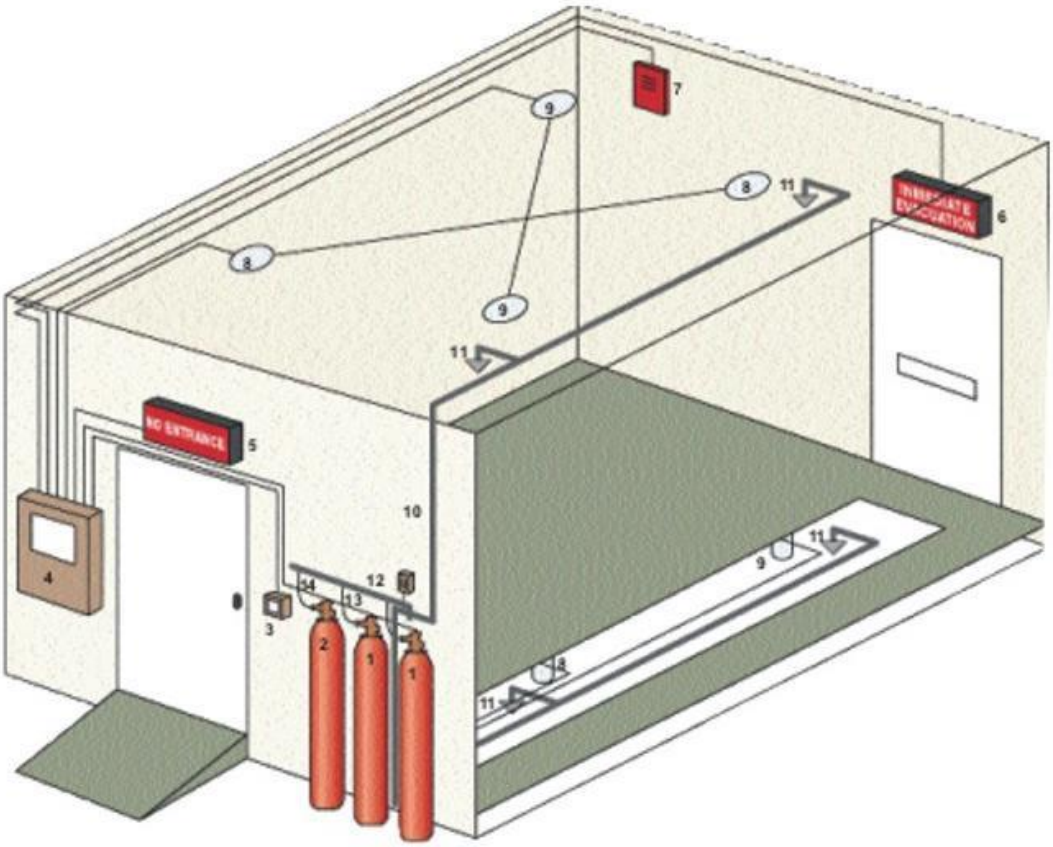


Рисунок 5.3 – Размещение огнетушителей

Расчетная масса комбинированного углекислотно-хладонового состава md, кг, для объемного пожаротушения определяется по формуле

$$m_d = k \cdot g_n \cdot V, \quad (5.8)$$

где k = 1,2 – коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава;

gN = 0,04 – нормативная массовая концентрация углекислотно-хладонового состава;

V - объем помещения, м3.

$$V = A \cdot B \cdot H, \quad (5.9)$$

где A = 7 м – длина помещения;

B = 5 м – ширина помещения;

H = 3 м – высота помещения.

Тогда:

$$V = 7 \cdot 5 \cdot 3 = 105 \text{ (м3)}. \quad (5.10)$$

Следовательно

$$md = 1{,}2 \cdot 0{,}04 \cdot 105 = 5 \text{ (кг)}.$$

Расчетное число баллонов ξ определяется из расчета вместимости в 20-литровый баллон 12 кг углекислотно-хладонового состава. Внутренний диаметр магистрального трубопровода di, мм, определяется по формуле

$$di = 12 \cdot \sqrt{2} = 17 \text{ (мм)}.$$

Эквивалентная длинна магистрального трубопровода 12,м, определяется по формуле

$$l2 = k1 \cdot l2, \quad (5.11)$$

где k1=1,2 - коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь;

l=3м - длина трубопровода по проекту тогда,

$$l2 = 1{,}2 \cdot 3 = 3{,}6 \text{ (м)}.$$

Расход углекислотно-хладонового состава Q, кг/с, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,4 кг/с. Расчетное время подачи углекислотно-хладонового состава t. мин, определяется по формуле

$$t = md/60 \cdot Q \quad t = 5/60 \cdot 1{,}4 = 0{,}06 \text{ (мин)}.$$

Масса основного запаса углекислотно-хладонового состава m, кг, определяется по формуле:

$$m=1,1\cdot md\cdot (1+k2/k), \quad (5.12)$$

где k2 = 0,2 - коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах.

$$m=1,1\cdot 5\cdot (1+0,2/1,2)=6 \text{ (кг)}.$$

Углекислотный огнетушитель – это закачной огнетушитель высокого давления с зарядом жидкой двуокиси углерода, находящийся под давлением ее насыщенных паров. Углекислотный огнетушитель — один из видов первичных средств пожаротушения. Его баллон заполнен составом двуокиси углерода, находящегося под высоким давлением закаченного внутрь газа. Применение углекислотных огнетушителей широко распространено в промышленности и быту.

Огнетушители как первичные средства пожаротушения, заполненные углекислотой, незаменимы как средство тушить пожары там, где с другим видом огнетушащего вещества это сделать невозможно, смертельно опасно для жизни…..или нецелесообразно использовать из-за попадания на дорогостоящее и ценное производственное оборудование, электрическую аппаратуру, приборы, бытовую технику воды, химической пены, порошка, что приводило еще к большему материальному ущербу. Напротив, CO2 в ходе тушения просто быстро испаряется, не оставляя абсолютно никаких следов – загрязнений и повреждений.

Таким образом, из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно- хладонового состава вместимостью 20 литров, с массой смеси 6 кг для одного рабочего помещения. Автоматические установки газового пожаротушения имеют устройства для автоматического пуска в соответствии с ГОСТ 12,4.009-83. Также произведен расчет и план эвакуационных путей.

6 Финансовый план

Тема данной дипломной работы Моделирование и анализ защищенности локальной сети банка с использованием программы SkyBox. ТОО «Акнур Секъюрити» в городе Алматы».

Целью данного проекта является разработать план проекта, создать условия для сетевых администраторов и офицеров безопасности по своевременному обнаружению уязвимостей и плохой конфигурации сетевого оборудования. Весь комплекс мероприятий, это интеллектуальный труд, который подразумевает разработку проекта не для продажи, а значит не

ставит целью получение материального дохода от работы. Проект разрабатывается для того чтобы инфраструктура банка была защищена от вторжения из вне хакерами, вредоносными системами и инсайдерами. В последние годы процент киберпреступлений становится лишь больше согласно статистки ЦАРКА, где особенно подвержены атакам банки 2 и 3 уровня.

В данном разделе приводится рассмотрение экономической составляющей реализации данной работы, отражающей временные, трудовые и финансовые затраты на проект.

6.1 Убытки, ущерб банков и информационная безопасность

Согласно результатам исследования «Лаборатории Касперского» («Финансовые киберугрозы в 2019 году», проведено среди 800 представителей финансовых организаций из 15 стран мира), потери финансовых организаций от кибератак становятся все более ощутимыми: средний совокупный ущерб от одного инцидента достиг $926 тыс. Помимо прямого ущерба эта цифра включает дополнительную расходы на заработную плату персонала, привлечение внешних специалистов, репутационные издержки, упущенную выгоду, а также страховые выплаты и компенсации клиентам.

Самыми разорительными стали атаки на POS-терминалы: средний урон от них составил $2,1 млн. Следом идут угрозы, связанные со взломом мобильных устройств ($1,6 млн ущерба), и целевые атаки ($1,3 млн).

Рост потерь вынуждает финансовые организации увеличивать расходы на кибербезопасность. Хотя основной причиной остается необходимость соблюдать требования регуляторов, 63% респондентов считают такое соответствие лишь отправной точкой в построении системы защиты. Другой фактор, который вынуждает компании увеличивать расходы в этой области, — усложнение инфраструктуры. Наконец, расходы на безопасность могут увеличиваться, когда компания осознает недостаточность собственных знаний в этой области, а также по указанию руководства или из-за расширения бизнеса. Резюмируя, можно сказать, что объем средств, выделяемых на информационную безопасность, будет расти и в дальнейшем: в этом уверены 83% опрошенных.

Результаты исследования показали, что финансовые организации концентрируются на изучении киберугроз и проведении аудитов системы безопасности: 73% респондентов считают такие меры эффективными.

Эксперты «Лаборатории Касперского» при разработке стратегии кибербезопасности советуют принимать во внимание также следующие рекомендации:

- остерегайтесь целевых атак. Они могут проводиться через третьих лиц или ваших подрядчиков. Такие компании часто слабо защищены, что может стать вашей проблемой;

– учитывайте человеческий фактор: злоумышленники очень часто и изобретательно применяют методы социальной инженерии для проникновения в инфраструктуру компании;

– помните, что одно лишь соответствие требованиям безопасности не дает гарантированной защиты. Не менее важно применять комплексный подход к безопасности;

– проводите регулярные тесты на проникновение. Уязвимости инфраструктуры должны быть известны вам раньше, чем до них доберутся злоумышленники;

– принимайте во внимание угрозу инсайдеров. Злоумышленники могут подкупить сотрудников компании, чтобы обойти систему защиты. Противостоять этому можно применением политик ИБ, грамотным разграничением доступа и вспомогательными методами для обнаружения аномальных активностей внутри организации.

Согласно результатам исследования «Лаборатории Касперского», средний годовой бюджет банков на кибербезопасность достигает $58 млн: это в три раза больше, чем у нефинансовых организаций. В большинстве случаев подобные траты оправдываются: представители банков сообщают о значительно меньшем количестве компьютерных преступлений, чем компании такого же размера в других отраслях. Более того, 64% опрошенных заявили, что будут вкладывать в улучшение защиты независимо от окупаемости этих инвестиций.

Рост вложений в киберзащиту имеет веские основания: в последние несколько лет количество угроз для финансовой индустрии неуклонно растет, они становятся все более сложными и чреваты серьезными последствиями, указали в компании. Так, 70% банков сообщили о том, что за последний год они понесли денежные потери в результате кибермошенничества. Больше всего опасений вызывают риски, связанные с мобильным банкингом: 42% респондентов считают, что в ближайшие три года им будет пользоваться подавляющее число клиентов, в то время как уровень киберграмотности пользователей останется низким. Это грозит увеличением количества инцидентов, связанных с кражей денег через мобильные устройства.

Среди других актуальных угроз для пользователей банки выделили фишинг: с ним в 2019 г. сталкивались клиенты 46% компаний. Еще одна сфера повышенного риска — банкоматы. Причем всего 19% банков обеспокоены угрозой атак на них, в то время как в 2016 г. объем вредоносного ПО для банкоматов вырос на 20% по сравнению с 2015 г.

По информации «Лаборатории Касперского», неосторожность пользователей и возрастающее количество атак заставляют банки пересмотреть приоритеты по обеспечению безопасности: 61% участников исследования назвали улучшение защиты приложений и сайтов одним из главных приоритетов. На втором месте (52%) оказалось внедрение более надежных систем авторизации.

6.2 Расчет капитальных вложений

Затраты по капитальным вложениям на реализацию проекта включают в себя затраты на приобретение основного оборудования, монтаж оборудования, транспортные расходы и проектирование, и рассчитывается по формуле

$$K_{\Sigma} = K_0 + K_M + K_{\text{тр}} + K_{\text{пр}}\ , \qquad (6.1)$$

где КО – капитальные вложения на приобретение основного оборудования;

КМ. – расходы по монтажу оборудования;

КТР – транспортные расходы;

КПР – затраты на проектирование.

Общий перечень необходимого основного оборудования и его стоимость приведены в таблице 6.1

Таблица 6.1 - Основное оборудование и общая стоимость

Наименование	Количество, шт	Цена за ед, тг	Сумма, тг (без НДС)
Аналитическая система по выявлению уязвимости и моделирования сети Skybox	1	21 000 000	23 520 000
Опора под оборудование	1	400 000	400 000
Кабель питания	1	18 000	18 000
Сетевой кабель Ethernet RJ-45	1.5 метра	7 000	10 500
Итого:			23 948 500

Транспортные расходы, составляют 3% от стоимости всего программного комплекса и рассчитываются по формуле

$$K_{mp} = 0{,}03 \cdot K_0 = 0{,}03 \cdot 23\ 948\ 500 = 718\ 455 \text{ (тенге).}$$

Интеграция оборудования, пуско-наладка производится инженерами-интеграторами, расходы составляют 1% от стоимости всего оборудования и рассчитываются по формуле

$$K_m = 0{,}01 \cdot K_0 = 0{,}01 \cdot 23\ 948\ 500 = 239\ 485 \text{ (тенге).}$$

Расходы по проектированию и разработке проекта составляют 0,5% от стоимости всего оборудования и рассчитываются по формуле

$$K_{\text{п}p} = 0{,}005 \cdot K_0 = 0{,}005 \cdot \ = 119\ 742 \text{ (тенге).}$$

Общая сумма капитальных вложений по реализации проекта составляет

$K_{\Sigma=}$23 948 500 + 718 455 + 239 485+119 742=25 026 182 (тенге).

6.3 Сроки реализации проекта

Проектирование системы видеонаблюдения *(СВ)* включает в себя следующие этапы (таблица 6.2):

- 1 этап: Постановка задачи;
- 2 этап: Разработка задания;
- 3 этап: проектирование системы видеонаблюдения на программе AutoCAD;
- 4 этап: создание прототипа и проверка работоспособности с использованием тестирующих программ;
- 5 этап: Оформление отчетов.

Таблица 6.2 – Этапы и сроки реализации проекта

Перечень работ		Недели от начала работ							
		1	2	3	4	5	6	7	8
1 этап	Постановка задачи								
	Обзор и анализ технологий, применяемых в проекте								
	Подбор и изучение литературы по теме проекта								
2 этап	Разработка задания								
	Выбор оборудования, изучение его функциональных возможностей								
3 этап	Проектирование системы								
4 этап	Создание прототипа и проверка работоспособности с использованием тестирующих программ								
	Тестирование настроек								
	Отладка недочетов								
5 этап	Оформление отчетов								

6.4 Эксплуатационные расходы

Текущие затраты на эксплуатацию данной системы связи определяются по формуле

$$\text{Э}_\text{р} = \text{ФОТ} + \text{О}_\text{с} + A_0 + \text{Э} + \text{Н}\ , \qquad (6.2)$$

где ФОТ – фонд оплаты труда;

ОС – отчисления на соц. нужды;

$А_о$ – амортизационные отчисления;

Э – электроэнергия для производственных нужд;

Н – накладные затраты;

Фонд оплаты труда.

В штате данного проекта состоят 4 инженера-техника. Месячная зарплата у инженера-техника составляет 150 000 тенге. Заработная плата сотрудников приведена в таблице 6.3.

Таблица 6.3 – Заработная плата сотрудников

Должность	Количество	Месячная заработная плата, тенге	Годовая заработная плата, тенге
Сетевой администратор	1	350 000	4 200 000
Офицер безопасности	1	400 000	4 800 000
Итого			9 000 000

Затраты по оплате труда состоят из основной и дополнительной заработных плат и рассчитываются по формуле:

$$ФОТ = З_{осн} + З_{доп}\ , \qquad (6.3)$$

где Зосн - основная заработная плата,

Здоп - дополнительная заработная плата.

Основная заработная плата в год составляет:

Зосн = 9 000 000 (тенге).

Дополнительная заработная плата составляет 10% от основной заработной платы и рассчитывается по формуле

$$З_{доп} = 0{,}1 \cdot З_{осн}\ , \qquad (6.4)$$

$$З_{доп} = 0{,}1 \cdot 9\,000\,000 = 900\,000 \text{ (тенге).}$$

Общий фонд оплаты труда за год составит

ФОТ=9 000 000 + 900 000 = 9 900 000 (тенге).

Расчет затрат по социальному налогу.

В соответствии со статьей 385 Налогового кодекса РК социальный налог составляет 11% от начисленных доходов и рассчитывается по формуле

$$O_c = 0{,}11 \cdot (\text{ФОТ} - \text{ПО}) \ , \qquad (6.5)$$

где ПО – отчисления в пенсионный фонд.

ФОТ – фонд оплаты труда

0,11 – ставка на социальные нужды

Отчисления в пенсионный фонд составляют 10% от ФОТ, социальным налогом не облагаются и рассчитываются по формуле

$$\text{ПО} = 0{,}1 \cdot \text{ФОТ} \ , \qquad (6.6)$$

$$\text{ПО} = 0{,}1 \cdot 9\,900\,000 = 990\,000 \ \text{(тенге).}$$

Тогда социальный налог будет равен

$$\text{О}_\text{с} = 0{,}11 \cdot (9\,900\,000 - 990\,000) = 980\,100 \ \text{(тенге).}$$

Расчет затрат на амортизацию:

Амортизационные отчисления берутся исходя из того, что норма амортизации на оборудование по анализу и защите составляет 25% и вычисляются по следующей формуле

$$\text{А}_0 = \text{Н}_\text{А} \cdot \Sigma\,\text{К} \ , \qquad (6.7)$$

где НА- норма амортизации;

∑К – стоимость оборудования;

Тогда амортизационные отчисления составляют

$$\text{А}_0 = \text{Н}_\text{А} \cdot \Sigma\,\text{К} = 0{,}25 \cdot 25\,026\,182 = 6\,256\,545.5 \ \text{тенге}$$

Расчет затрат на электроэнергию

Затраты на электроэнергию рассчитываем по формуле

$$\text{С}_\text{ЭЛ}. = \text{W} \cdot \text{T} \cdot \text{S} \ , \qquad (6.8)$$

где СЭЛ - стоимость электроэнергии;

W - потребляемая мощность, W=300Вт;

T - время работы T=4 380 ч/год;

S - стоимость киловатт-часа электроэнергии S = 14,02 тенге / квт-час

$$\text{С}_\text{ЭЛ} = 0{,}5 \cdot 8760 \cdot 14{,}02 = 30\,703 \ \text{(тенге).}$$

Затраты на дополнительные нужды составляют 5% от затрат на электроэнергию оборудования и рассчитываются по формуле:

$$З_{доп.нуж.} = 0{,}05 \cdot З_{эл.обор.}\ , \qquad (6.9)$$

где $З_{ЭЛ.ОБОР}$ - затраты на электроэнергию для оборудования;

Затраты на электроэнергию для дополнительных нужд

$$З_{доп.нуж.} = 0{,}05 \cdot 30\ 703 = 1535{,}15 \text{ (тенге).}$$

Тогда суммарные затраты на электроэнергию будут равны

$$Э = 30703 + 1535{,}15 = 32\ 238 \text{ (тенге).}$$

Расчет накладных затрат.

Накладные расходы составляют 45 % от всех затрат и рассчитываются по формуле

$$Н = 0{,}45 \cdot (ФОТ + О_с + А_0 + З_{эл.обор})\ , \qquad (6.10)$$

где ФОТ - фонд оплаты труда;

Тогда накладные затраты составят

$$Н = 0{,}45 \cdot (9\ 900\ 000 + 990\ 000 + 6\ 256\ 545.5 + 32\ 238) =$$
$$= 7\ 730\ 452{,}57 \text{ (тенге).}$$

Результаты расчета годовых эксплуатационных расходов проекта по организации систем видеонаблюдения представлены в таблице 6.4.

Таблица 6.4 - Годовые эксплуатационные расходы

Наименование показателей	Сумма, тенге
ФОТ	9 990 000
Отчисления на социальные нужды (Ос)	980 100
Амортизационные отчисления ($А_0$)	6 256 545,5
Затраты на электроэнергию (Э)	32 238
Накладные расходы (Н)	7 730 452.57
Итого:	24 989 336

Таким образом доля фонда оплаты труда составляет 23,5%, социальный налог 2,3%, амортизационные отчисления 43%, затраты на электроэнергию 0,2%, накладные расходы 31% от общей суммы эксплуатационных затрат.

6.5 Вывод по разделу экономика

Анализ полученных результатов показывает, что капитальные затраты составляют – 25 026 182 тенге, эксплуатационные расходы – 24 989 336 тенге.

Затраты для обслуживания системы Skybox и ее компонентов относительно небольшие. Вместе с тем положительный эффект от поддержания вычислительной системы в состоянии готовности предотвратить попытки хищения, модификации, либо подмены информации, значительный.

Заключение

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

Исходя из проделанной мной работы могу сказать с уверенностью, что сети могу быть защищены, но в наше время технологии развиваются с огромной скоростью, что не позволяет защитить сеть на 100%. Так как с технологиями приходят и уязвимости, а так же злоумышленники.

Список литературы

1 Бирюков А. Информационная безопасность: защита и нападение. 2-е издание, ДМК-Пресс, 2017, 434 с.

2 Орлов, Л. В. Как создать защиту в сети. / Л. В. Орлов – изд. Бук-Пресс: Москва, 2016, – 384 с.

3 Бондарев В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства, МГТУ им. Н. Э. Баумана, 2017, 228 с.

4 Информационная безопасность и защита информации. Учебное пособие – М.: 2004 – 82 с.

5 Инструкция по установке и настройки системы Skybox (Reference Guide).

6 Холмогоров, В. Уязвимости в сети / В. Холмогоров. – СПб.: Питер, 2012. – 272 с.

7 Орлов, Л. В. Как создать защиту в сети. / Л. В. Орлов – изд. Бук-Пресс: Москва, 2016, – 384 с.

8 www.cisco.com (дата посещения 20.04.2020г)

9 www.habr.com/информационная_безопасность_в_локальной_сети (дата посещения 23.04.2020г)

10 Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT-CCNA ICND1 100-101

11 https://fireman.club/statyi-polzovateley/uglekislotnyiy-ognetushitel-kakie-byivayut-naznachenie-i-primenenie (дата посещения 25.04.2020г)

12 http://gidro.tech-group.pro/ognetushiteli_uglekislotnye(дата посещения 29.04.2020г)

13 Н.Г. Приходько, Ф.Р. Жандаулетова. Основы пожарной безопасности. Методические указания к выполнению курсовой работы для студентов специальности 5В073100 – Безопасность жизнедеятельности и защита окружающей среды. - Алматы: АУЭС, 2013

14 Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009.