Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

Модернизация защищенной локальной сети института безопасности СИБГУТИ

Выполнил студент гр. АБ-87
Медведев Н.В.
Руководитель: доц.каф БиУТ
Солонская О.И.

Новосибирск 2023

Актуальность темы

Институт хранит и использует персональные данные, коммерческую тайну и авторское право, которую необходимо защитить от несанкционированного доступа. Это, в свою очередь, требует внедрения новых программных и аппаратных средств защиты локальной сети, и необходимости обеспечить защитой сеть передачи данных между предприятием и его филиалами.

Объектом исследования дипломной работы – Институт безопасности (ИБ) входящая в одну структуру подразделений Федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» являющийся базовым образовательным комплексом Минцифры в регионе, крупным научным центром по изучению проблем связи и развитию телекоммуникационных технологий.

Цель

Модернизация защищенной локальной сети института безопасности СИБГУТИ

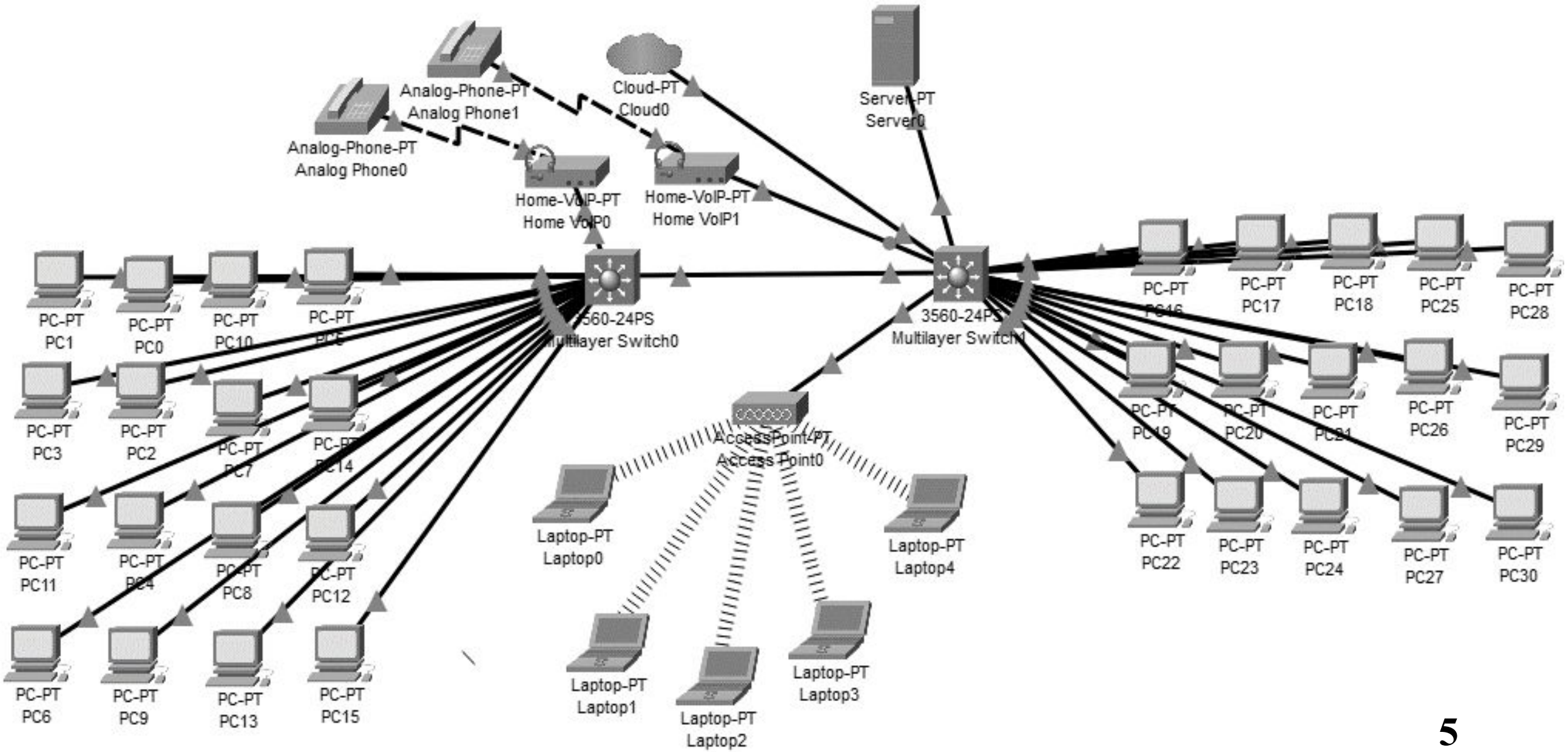
Решаемые задачи:

1) Анализ текущего состояния объекта модернизации;
2) Оценка угроз безопасности информации;
3) Модернизация системы защиты информации института безопасности;
4) Изучить безопасность жизнедеятельности.

Анализ текущего состояния объекта

Оборудование	ПК – 35 шт. Ноутбук – 5 шт. Коммутатор – 2 шт. Сервер – 1 шт. Беспроводная точка доступа – 1 шт.
Системное ПО	Windows 10 Windows Defender 1С Бухгалтерия
Информационные системы	ЭИОС ГосУслуги 1С
Вид информации	Персональные данные Коммерческая тайна Авторское право
Пользователи	Сотрудники Студенты
Выход в интернет	Есть
Количество субъектов ПДн, обрабатываемых в ИС	Менее 100 000
Объект КИИ	Нет

Схема локальной сети института безопасности



Виды обрабатываемой информации в системе и нормативная база

Вид информации	Персональные данные
Вид документа	
Федеральный закон	Федеральный закон "О персональных данных" № 152-ФЗ, Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ
Указ Президента	Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера" Указ Президента РФ от 01.05.2022 № 250 “О дополнительных мерах по обеспечению информационной безопасности Российской Федерации”
Постановление Правительства	Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 “ Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”
Приказ ФСБ	Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
Трудовой кодекс	Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 19.12.2022) (с изм. и доп., вступ. в силу с 11.01.2023) Глава 14. Защита персональных данных работника

Виды обрабатываемой информации в системе и нормативная база

Вид информации	Коммерческая тайна
Вид документа	
Федеральный закон	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ
Указ Президента	Указ Президента Российской Федерации от 06.03.1997 г. № 188 Об утверждении перечня сведений конфиденциального характера. Указ Президента РФ от 01.05.2022 № 250 “О дополнительных мерах по обеспечению информационной безопасности Российской Федерации”

Вид информации	Авторское право
Вид документа	
Закон Российской Федерации	Закон РФ № 5351-I "Об авторском праве и смежных правах".
Гражданский кодекс	"Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ (ред. от 05.12.2022) ГК РФ Глава 70. Авторское право. Статья 1250, 1251, 1252, 1266.

Вывод

В первой главе выполнен общий анализ Института безопасности. Рассмотрены виды деятельности, информационная, организационная и IT инфраструктура института безопасности и существующая компьютерная сеть.

В ходе анализа действующей сети предприятия, был сделан вывод о том, что система защиты имеет удовлетворительный вид из-за несоответствия требованиям по защите информации, существует необходимость в модернизации отдельных ее частей.

Необходимый вид защищаемой информации ограниченного доступа – персональные данные, коммерческая тайна и авторское право.

Также исходя из анализа объекта проектирования можно сказать, что институт безопасности не является объектом КИИ.

Разработка модели угроз

№	Виды риска (ущерба)	Возможные типовые негативные последствия
1	Ущерб физическому лицу	Нарушение конфиденциальности (утечка) персональных данных. Разглашение персональных данных граждан
2	Риски юридическому лицу	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Утечка конфиденциальной информации (коммерческой тайны, секретов производства и др.)
3	Ущерб государству	Нарушение законодательства Российской Федерации. Утечка информации ограниченного доступа.

Объекты воздействия:

а) информация в системах и сетях;
б) программно-аппаратные средства;
в) программные средства;
г) машинные носители информации;
д) телекоммуникационное оборудование;
е) средства защиты информации;
ж) автоматическое рабочие место пользователя;
з) информационные системы.

Актуальность и УБИ

УБИ	Угроза
011	Угроза деавторизации санкционированного клиента беспроводной сети
015	Угроза доступа к защищаемым файлам с использованием обходного пути
016	Угроза доступа к локальным файлам сервера при помощи URL
030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
063	Угроза некорректного использования функционала программного и аппаратного обеспечения
067	Угроза неправомерного ознакомления с защищаемой информацией
074	Угроза несанкционированного доступа к аутентификационной информации
086	Угроза несанкционированного изменения аутентификационной информации
088	Угроза несанкционированного копирования защищаемой информации
132	Угроза получения предварительной информации об объекте защиты
156	Угроза утраты носителей информации
157	Угроза физического выведения из строя средств хранения, обработки информации
158	Угроза форматирования носителей информации
160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации

Вывод

В данной главе была произведена актуализация модели угроз ИБ для Института безопасности.

В результате разработки актуальной модели нарушителя были определены потенциальные нарушители ИБ:

— отдельные физические лица (хакеры);
— разработчики программных, программно-аппаратных средств;
— лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
— поставщики услуг связи, вычислительных услуг;
— авторизованные пользователи систем и сетей;
— системные администраторы и администраторы безопасности;

бывшие (уволенные) работники (пользователи).

Основными актуальными угрозами Института безопасности были определены такие угрозы, как:

— угроза сканирования сети;
— угроза уничтожения, хищение аппаратных средств ИС и носителей информации;
— угроза использования уязвимостей;
— угроза внедрения вредоносного программного обеспечения;

Сравнение средств антивирусной защиты

Функциональная возможность	Windows Defender	Kaspersky Endpoint Security 11
Облачный режим функционирования	Отсутствует	Реализация KSN. Реализация режима легких баз для защиты угроз: легкие антивирусные базы при включенном KSN занимают меньше оперативной памяти и пространства на жестком диске
Защита HTTPS трафика	Отсутствует	Эксплуатация в роли дополнительного прокси с возможностью анализа зашифрованного трафика
Полноценная защита от майнинга	Отсутствует	Выявление и блокирование попыток запуска майнинг-программ. Пресечение попыток доступа к криптовалютным биржам
Анализ поведения	Получение данных о действиях программ и предоставление этой информации другим компонентам защиты с использованием шаблонов опасного поведения.	Получение данных о действиях программ и предоставление этой информации другим компонентам защиты с использованием шаблонов опасного поведения. Выбор действия при обнаружении вредоносной активности. Защита от внешнего шифрования сетевых ресурсов
Защита от сетевых атак	Отслеживание во входящем сетевом трафике активности, характерной для сетевых атак. Возможность изменения времени блокирования атакующего узла	Отслеживание во входящем сетевом трафике активности, характерной для сетевых атак. Возможность изменения времени блокирования атакующего узла. Защита от атак, использующих уязвимости в протоколе ARP для фальсификации MAC-адреса устройства.
Сертификаты ФСБ	Отсутствует	№ СФ/019-3468, № СФ/СЗИ-0431, № СФ/СЗИ-0524, № СФ/СЗИ-0599
Сертификаты ФСТЭК	Отсутствует	№ 3155

Сравнение коммутаторов

Функциональная возможность	Cisco Business 110 series	ELTEX MES2424P	QSW-3470-28TX-AC
Порты 10/100/1000BASE-T	16 порта	24 порта	20 порта
Порты 10GbE SFP+	0 портов	4 порта	2 порта
Порты консоли	5 портов RS-232 (RJ45)	1 порт RS-232 (RJ45)	1 порт RS-232 (RJ45)
Пропускная способность	32 Гбит/с	128 Гбит/с	128 Гбит/с
Таблица MAC-адресов	8К	16К	16К
Память	256 Мб RAM + 64 Мб	512 Мб RAM + 64 Мб	512 Мб RAM + 32 Мб
Страна	Америка	Россия	Россия
Сертификаты ФСБ	Отсутствует	Отсутствует	Отсутствует
Сертификаты ФСТЭК	Отсутствует	Отсутствует	Отсутствует

Сравнение серверов

Функциональная возможность	Cisco ucs c220	QSRV-260422GPU	KARMA DATA
Процессор	Intel Xeon 1-2	Intel Xeon Scalable Gen2	Intel Xeon 1–2
Память	16 DIMM	12 DDR4 RDIMM	DIMM,DDR4/DDR-T
PCIe слоты	2x PCIe x8 / x16	4x PCIe x16 (Gen3 x16 bus) для GPU; Слот_2: 1 x PCIe x8 (Gen3 x8 bus)	3x PCIe x8; 3x PCIe x16;
RAID	LSI MegaRAID SAS9266-8i	Intel RSTe RAID 0, 1, 10	Intel RSTe RAID 0, 1
Жесткие диски	8x 2.5' SAS, SATA или SSD с поддержкой горячей замены	4 x SAS/SATA 12 x SAS/SATA 16 x SAS/SATA 8 x SAS/SATA 24 x SAS/SATA	4 x SAS/SATA 12 x SAS/SATA 16 x SAS/SATA 8 x SAS/SATA 24 x SAS/SATA
Страна	Америка	Россия	Россия
Сертификат ФСБ	Отсутствует	Отсутствует	Отсутствует
Сертификат ФСТЭК	Отсутствует	Отсутствует	Отсутствует

Сравнение серверов

Функциональная возможность	Cisco SB WAP150-R-K9	ELTEX WEP-200L	TP-Link CPE210
Стандарты беспроводной связи	IEEE 802.11a, IEEE 802.11ac, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n	IEEE 802.11a, IEEE 802.11ac, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Частота работы передатчика	2.4 ГГц / 5 ГГц	2.4 ГГц / 5 ГГц	2.4 ГГц
Максимальная скорость беспроводного соединения	До 1000 Мбит/с	До 1733 Мбит/с	300 Мбит/с
Защита сети	WEP, WPA-PSK, WPA2-PSK	WPA/WPA2, Поддержка Captive Portal	WEP, WPA, WPA2, WPA-PSK, WPA2-PSK
Страна	Америка	Россия	Китай
Сертификат ФСБ	Отсутствует	Отсутствует	Отсутствует
Сертификат ФСТЭК	Отсутствует	Отсутствует	Отсутствует

Сравнение сканеров уязвимости

Функциональная возможность	Xspider	«Ревизор Сети»	RedCheck
Обнаружение уязвимостей в сервисах	SMB, RDP, HTTP, SNMP, FTP, SSH	FTP, RPC, SMB, SNMP, RDP	HTTP, FTP
Параллельное многопоточное тестирование	Одновременное сканирование большого числа компьютеров	Позволяет осуществлять параллельное многопоточное сканирование узлов сети.	Поддерживает многопоточное сканирование.
Сканер портов	Сканирует порты TCP/UDP. Для быстрой проверки можно вручную настроить сканирование часто используемых портов	Сканирование TCP и UDP портов на узлах проверяемой сети;	Присутствует
Логирование составления отчетов	Выдает в структурированном виде данные о результатах сканирования для детального анализа текущей ситуации в системе	Все результаты выполненных проверок для каждого из сеансов работы могут быть сохранены в базе данных	Результаты сканирования сохраняются и могут быть экспортированы в форматы PDF и CSV.
Страна	Россия	Россия	Россия
Сертификат ФСБ	Отсутствует	Отсутствует	Отсутствует
Сертификат ФСТЭК	3247	3413	3172

Вывод

В данном разделе были разработаны модели угроз и нарушителя Института безопасности по документам ФСТЭК, также было проанализировано оборудование для модернизации защищенной локальной сети Института безопасности.

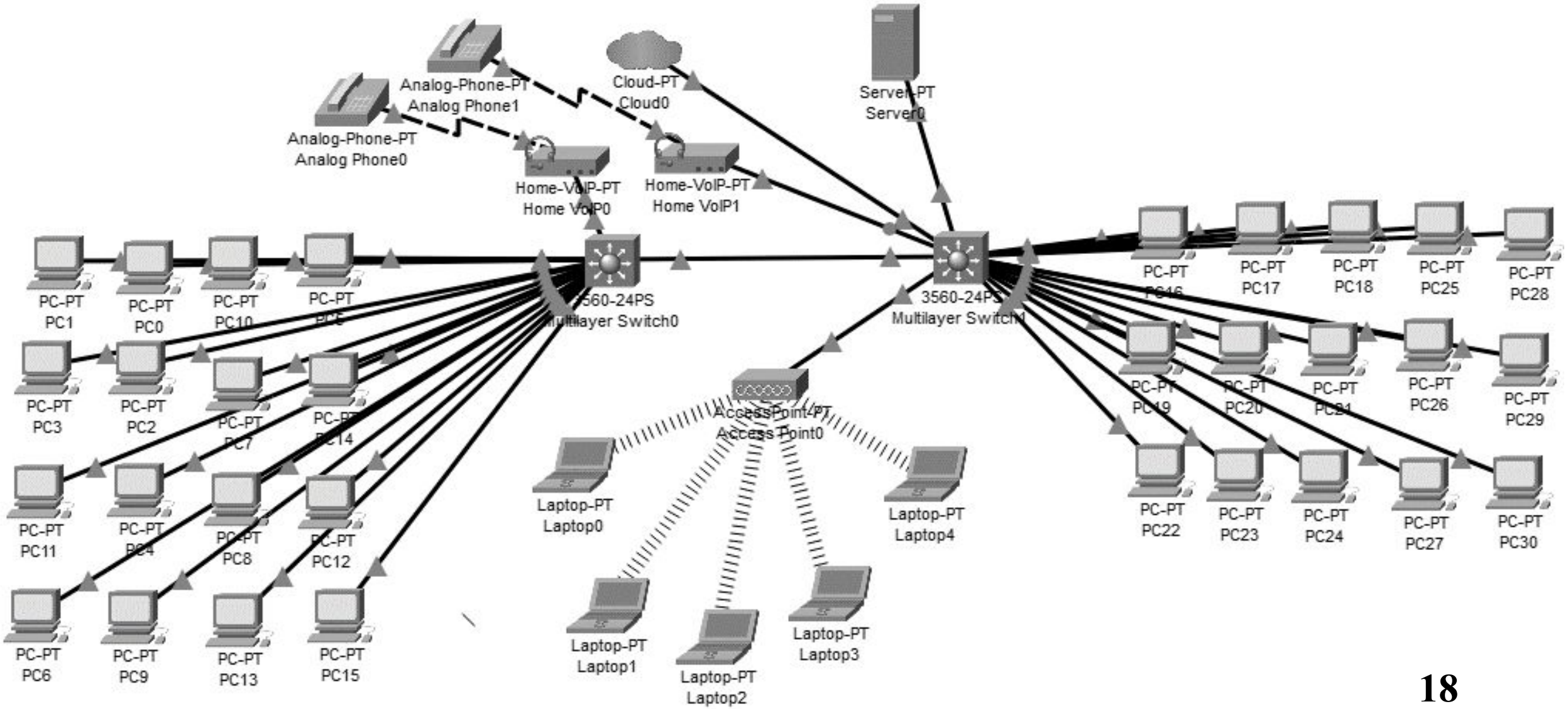
Данные меры по модернизации, включают в себя основную цель – повышение зашиты обрабатываемой и хранимой информации в Институте безопасности.

На основе выбранных оборудования и программных обеспечений были приняты меры по повышению безопасности защиты информационной системы предприятия, а также выбраны технологические и организационные мероприятия.

Результаты модернизации:

- повышение защиты локальной сети;
- актуализация антивирусного ПО;
- актуализация коммутирующего оборудования;
- актуализация серверного оборудования;
- актуализация беспроводной точки доступа;
- защита от НСД;
- защита при пользовании сетью Интернет;
- курсы на повышение квалификации.

Модернизированная схема локальной сети института безопасности



Заключение:

Целью данного дипломного проекта являлось модернизация защищённой локальной сети Института безопасности высшего учебного заведения СибГУТИ. Для достижения поставленной цели решили следующие задачи:

- провели анализ текущего состояния объекта модернизации;
- разработали модель угроз Института безопасности учебного заведения;
- модернизировали системы защиты информации Института безопасности.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

Спасибо за внимание!

Выполнил студент гр. АБ-87
Медведев Н.В.
Руководитель: доц.каф БиУТ
Солонская О.И.

Новосибирск 2023