

Слайд 1

Уважаемый председатель, уважаемые члены государственной аттестационной комиссии!

Тема моей выпускной квалификационной работы – **«Защита локальной сети»**.

Слайд 2

Итак, **целью** работы является разработка и реализация политики безопасности в локальной сети на примере предприятия.

Задачи исследования представлены на слайде.

Слайд 3

Итак, при выполнении работ можно использовать следующую модель построения корпоративной системы защиты информации, основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 “Информационная технология – методы защиты – критерии оценки информационной безопасности”, стандарту ISO/IEC 17799 “Управление информационной безопасностью” и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам защиты информации. Представленная модель защиты информации – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Слайд 4

Итак, ООО «АйТиЭл» было создано в апреле 2018 года. Компания занимается ремонтом, обслуживанием и продажей компьютерной техники. Главный бухгалтер несет ответственность за формирование Учетной политики, ведение бухгалтерского учета, своевременное представление полной и достоверной бухгалтерской отчетности, обеспечивает соответствие хозяйственных операций законодательству Российской Федерации, контроль за движением имущества и выполнением обязательств.

Слайд 5

Итак, для построения информационной модели системы управления необходимо четко представлять структуру информационных потоков

организации. Составим схематически существующую структуру информационной модели предприятия, основываясь на организационно-штатной структуре.

Слайд 6

Далее составим универсальную структуру информационной модели предприятия. Полученная совокупность информационных потоков послужит основой для разработки локальной информационной сети подразделения, с целью повышения эффективности управленческого процесса.

Слайд 7

Итак, использование локальной компьютерной сети на предприятии позволяет сократить бумажный документооборот, имеющийся на предприятии, повысить производительность труда, сократить время на обработку информации, что существенно влияет на качество выполнения управленческих задач. На выбранном предприятии, работы по созданию и внедрению информационной системы выполняются в условиях наличия разрозненной компьютерной техники, используемой каждым отделом самостоятельно. На предприятии принято решение о создании единой информационной системы с целью организации оперативного и эффективного учета товарно-материальных ценностей, проведения оперативного бухгалтерского учета, маркетингового анализа и интеграции бухгалтерской отчетности подразделения в бухгалтерский учет головного предприятия.

Слайд 8

Итак, в штатной структуре предприятия имеется четыре отдела, самостоятельно выполняющие функции учета и оперативного управления. Они и послужат основой структуры будущей локальной информационной системы подразделения. Каждая структурная единица имеет минимальное необходимое оборудование, т.е. процесс внедрения сети будет заключаться в объединении имеющейся оргтехники на основе выбранной оптимальной типологий сети. В таблице приведен состав имеющейся оргтехники по каждой структурной единице.

Слайд 9

Далее сопоставляя имеющуюся оргтехнику с разработанной информационной моделью и выбранного типа сети, определим недостающие оборудование для построения законченной структуры локальной информационной системы.

Слайд 10

Итак, фирма понесет затраты на приобретение недостающего для организации локальной информационной сети оборудования и программного обеспечения, в таблицах приведен расчет необходимых денежных средств. Общая стоимость внедрения сети составит 105843 рубля. Срок окупаемости составит 1 год.

Слайд 11

Далее для организации подсистемы защиты выбраны следующие основные средства:

- 1) Средства разграничения доступа. Будут организованы виртуальные локальные сети (VLAN). Кроме того, будут настроены права доступа индивидуально каждому работнику.
- 2) Установка межсетевых экранов. Firewall (брандмауэр) будет установлен на границе между внутренней сетью и Интернет для противодействия несанкционированному межсетевому доступу.
- 3) Система обнаружения вторжений Intrusion Detection System, IDS - служит для обнаружения попыток несанкционированного доступа путем фоновое сканирование трафика.
- 4) Защита информации при передаче по каналам связи, которые не контролируются или контролируются лишь частично (например - Интернет). Распространенные способы защиты - криптография, физические средства защиты.
- 5) Системы идентификации, аутентификации и авторизации.
- 6) Антивирусная защита.

Слайд 12

Итак, при создании математической модели надежной и безопасной корпоративной сети использована реальная сеть предприятия ООО «АйТиЭл». На ее примере рассмотрены аспекты технической надежности топологии сети, а также аспекты информационной безопасности корпоративной сети предприятия. Будет выбран комплекс средств по организации средств защиты. Для самого предприятия ООО «АйТиЭл» данная разработка будет важным шагом по автоматизации процесса производства и по защите конфиденциальной информации от злоумышленников. Кроме того, данная модель может быть использована для определения степени защищенности любого предприятия, а также для организации подсистемы защиты информации на предприятии. Задача оценки эффективности контрмер является не менее сложной, чем оценка рисков. Причина в том, что оценка эффективности комплексной подсистемы безопасности, включающей контрмеры разных уровней (административные, организационные, программно-технические), в конкретной информационной

системе – методологически чрезвычайно сложная задача. По этой причине обычно используются упрощенные, качественные оценки эффективности контрмер. Примером является следующая таблица типичных значений эффективности контрмер, применяемых в методе анализа рисков RiskWatch. Таким образом, анализ и управление информационными рисками позволяет обеспечить экономически оправданную безопасность компании.

Слайд 13

Таким образом, Цель работы достигнута.

Спасибо за внимание! Доклад окончен.