ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

Государственное автономное профессиональное образовательное учреждение города Москвы

«ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ № 8 имени дважды Героя Советского Союза И.Ф. Павлова»

(ГАПОУ ПК № 8 им. И.Ф. Павлова)

Выполнил: Студент группы 53 ПИ

Оринич Виталий Валерьевич

Руководитель работы: Преображенская О.В.

- Угроза безопасности информации – возможность возникновения такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение физической целостности, логической структуры, несанкционированная модификация информации, несанкционированное получение информации, несанкционированное размножение информации.

Классификация угроз безопасности информации

При пассивном вторжении (перехвате информации) нарушитель только наблюдает за прохождением информации. При активном вторжении – стремится изменить информацию, передаваемую в сообщении. Случайные угрозы – это сбои аппаратуры, ошибки в ПО, ошибки в работе обслуживающего персонала... Преднамеренные угрозы связаны с целенаправленными действиями нарушителя.

- Стихийные бедствия;
- Сбои и отказы оборудования;
- Ошибки эксплуатации;
- Преднамеренные действия нарушителей и злоумышленников.
- Разглашение информации работниками

Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы	Программа резервного копирования Macrium Reflect
Заражение компьютера вирусами;	Антивирус «Dr.Web», на сервере установлен UserGate
Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем	Установлены источники бесперебойного питания. (позволяют сохранить данные и завершить работу ПК.)
Несанкционированный доступ в помещения учреждения для совершения кражи или других действий в не рабочее время;	На данном предприятии дежурит охранник. Рекомендуется так же установка охранно-пожарной сигнализации, с возложением на охранника обязанностей вызова милиции или пожарной службы при срабатывании сигнализации.
Нарушение конфиденциальности при почтовой пересылке в электронном виде отчетности;	Обеспечивается программными продуктами Система «СТЭК-Траст»,ViPNet [Деловая почта], которые поддерживают шифрование.

Программно-аппаратные средства, реализованные на предприятии:

Использование систем управления доступом (защита от несанкционированной загрузки персонального компьютера, ограничение доступа к внутренним ресурсам).

Использование антивирусных средств.

Программно-аппаратные меры позволят уменьшить риск таких угроз как нарушение доступности информации, и вероятность возникновения уязвимостей ошибки, сбои и отказы. Выявлены следующие возможные меры защиты: Использование неавторизованных USB устройств представляет угрозу корпоративным сетям и данным.

Кроме доступа к USB портам существует спектр потенциально опасных устройств: дисководы, CD-ROM, а также FireWire, инфракрасные, принтерные (LPT) и модемные (COM) порты, WiFi и Bluetooth адаптеры.

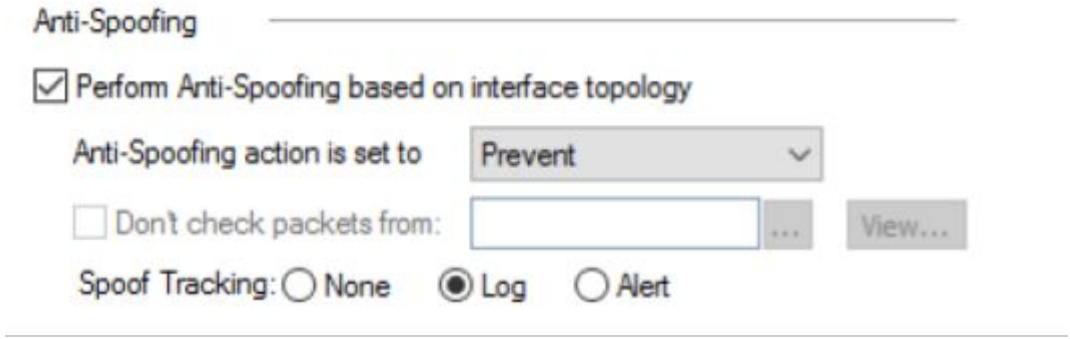
- Защита общей локальной сети с помощью маршрутизатора:
- периодический тест системы для избежания несанкционированного доступа
- настройка устанавливаемого оборудования и шифровка записей
- защита всех подключаемых устройств к сети
- создание общей защищенной локальной сети предприятия

1. Использование систем управления доступом (защита от несанкционированной загрузки персонального компьютера, ограничение доступа к внутренним ресурсам).
2. Регистрация, хранение и обработка сведений о событиях, имеющих отношение к безопасности системы.
3. Использование антивирусных средств.

Для защиты локальной сети используется маршрутизатор и встраиваемые протоколы защиты.

enable secret	Задать пароль для привилегированного доступа.
service password-encryption	Обеспечить минимальную защиту для паролей в конфигурации.
no service tcp-small-servers no service udp-small-servers	Избегать использования простых сервисов для DoS и других атак.
no service finger	Избегать распространения информации о пользователях.
no cdp running no cdp enable	Избегать распространения информации об этом маршрутизаторе на соседние устройства.
ntp disable	Предотвратить атаки на сервис NTP.

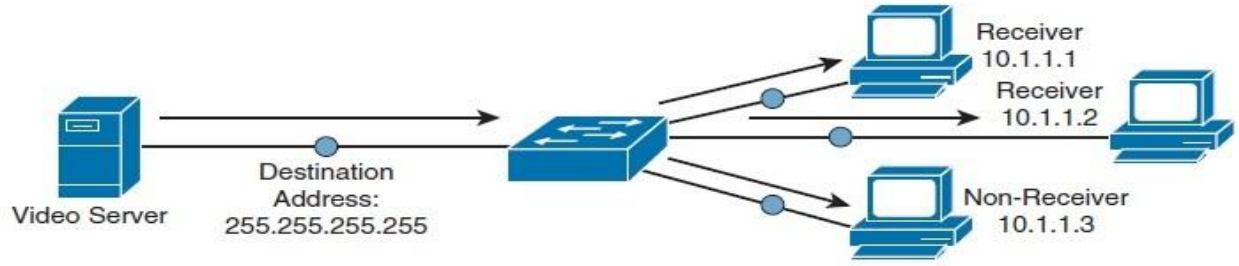
Anti-spoofing:
Множество сетевых атак проводятся с подмененными IP-адресами источника атаки, что снижает риск для атакующего быть замеченным.
Система защиты от спуфинга (anti-spoofing) должна быть использована на каждой точке, где существует возможность подобной атаки, обычно устанавливают данную защиту на границах сети, между большими блоками адресов или между доменами сетевого администрирования.



Для атаки типа "smurf" обычно используется IP directed broadcasts.

IP directed broadcast - это пакет, который посылается на адрес broadcast подсети, к которой посылающая машина напрямую не подключена.

Согласно архитектуре протокола, IP только последний маршрутизатор в цепочке, тот который напрямую подсоединен к подсети-назначения, может идентифицировать directed broadcast.



Название должности	Штат	Заработная плата
Начальник СБ	1	40000
Зам. Директора по кадрам	1	20000
Бухгалтер	4	10000
IT специалист	1	10000

В нашем случае затраты по заработной плате персонала, работающего с составлением различных положений и регламентов исходя из трудоемкости ведения данных работ составят:
Рзп= (40000*58+20000*116+4*10000*16+10000*116)*1,34/176 = 49032 руб.

Наименование	Стоимость с НДС	Количество	Итого
Программно-аппаратное направление защиты			
Cisco WAP 121	4750р	1	4750
Лицензия на антивирус Dr. Web	1550	14	21700
Маршрутизатор Cisco C881-K9	24500	1	24500
Итого:			50950

Рит-персонала = (10000*60*1,34)/176= 4569 руб.
Руст = = 46410 руб.

Спасибо за внимание