**2. Обрыв канала связи (Интернет)**

Стоит учесть, что резервный канал может не всегда справляться с полной нагрузкой основного канала.

**3. Внешняя атака на Информационную Систему**

Дополнительные риски:

* Фишинг: сотрудники могут стать жертвой фишинговых атак и раскрыть конфиденциальные данные.
* DDoS-атаки: могут быть направлены на серверы, что приведет к отказу в обслуживании.
* Вредоносное ПО: может быть загружено на компьютеры сотрудников через электронную почту или сайты.
* Кража учетных данных: могут быть украдены логины и пароли сотрудников.
* Несанкционированный доступ: злоумышленники могут получить доступ к системе через уязвимости в VPN или RDP.
* Кража конфиденциальной информации: злоумышленники могут попытаться украсть конфиденциальные данные с корпоративных ресурсов.
* Обход антивируса: злоумышленники могут использовать новые виды вредоносных программ, которые обходят защиту антивируса.
* Кража данных: злоумышленники могут попытаться украсть данные с FTP-сервера.

Решение проблем:

3.1. В случае атаки на Информационную систему пакеты будут отклонятся сетевым экранам с оповещением на почту об угрозе

Важно не только отклонять пакеты, но и анализировать атаки для предотвращения будущих попыток. (IDS/IPS системы, анализ сетевых пакетов, для сайта WAF).

3.2. В случае попыток входа через ВПН или RDP после ввода определенного количества неудачных попыток учетная запись пользователя блокируется на определенное время согласно политикам безопасности

Помимо блокировки учетной записи, стоит ввести двухфакторную аутентификацию.

Важно применять разные правила блокировки для разных групп пользователей. (Ролевая модель).

3.4. В случае обнаружения антивирусной программой в системе зараженного файла или вирусной активности, антивирусная защита удаляет зараженный файл, блокирует вирусную активность в системе, сообщая об инциденте.

Важно регулярно обновлять антивирусную программу и проводить сканирование системы на наличие вредоносных программ. Настроить политики. Запретить на МЭ для АВПО отправлять данные из нашей ИС. (отправлять файлы только для анализа, только через сайт АВПО)

Дополнительный риск:

Ложные срабатывания: АВПО может ошибочно определить некоторые безопасные файлы как вредоносные. (отключить удаление файлов, оставить для последующего анализа)

3.6. На серверах и рабочих станциях установлена и настроена Антивирусная защита с единым сервером администрирования антивирусом

АВПО установлено не на всех хостах в ИС (информационная система)

3.5. В случае попыток доступа по FTP с неразрешенных IP адресов пакеты буду отклоняться

Важно использовать безопасные протоколы FTP, такие как SFTP или FTPS.

**4. Ограничение доступа к серверному и сетевому оборудованию:**

Важен физический доступ к оборудованию. Нужно организовать пропускной режим и видеонаблюдение.

Дополнительные риски:

* Несанкционированный доступ: злоумышленники могут получить доступ к оборудованию и изменить его конфигурацию.
* Физическое повреждение: оборудование может быть повреждено в результате несчастных случаев или саботажа.

**5. Потеря данных из-за сбоя или вируса:**

Регулярное создание резервных копий данных и проверка их работоспособности.

Дополнительные риски:

* Потеря критических данных: Может привести к остановке работы.
* Повреждение данных: в результате атаки вредоносного ПО или сбоя в работе программного обеспечения данные могут быть повреждены.

**6. Сбой в Информационной Системе:**

Регулярно создавать резервные копии данных и проверять их работоспособность.

Дополнительные риски:

* Остановка работы серверов: может привести к нарушению работы приложений.
* Потеря данных: может произойти в результате сбоя в работе жестких дисков или системы RAID.

**Не учтены риски, связанные с внутренним нарушителем (внутренние атаки) и утечкой конфиденциальной информации:**

* Несанкционированный доступ: сотрудники могут получить доступ к конфиденциальной информации без разрешения.
* Неправомерное использование информации: сотрудники могут использовать конфиденциальную информацию в собственных целях.
* Утечка информации: сотрудники могут передать конфиденциальную информацию третьим лицам.

**Дополнительно:**

* Необходимо разработать и внедрить строгую политику безопасности, которая регламентирует доступ к системам и данным. Описать сценарии реагирования для различных ситуаций.
* Ввести обучение сотрудников: сотрудники должны быть обучены основам информационной безопасности и правилам работы с конфиденциальными данными.
* Внедрить системы мониторинга и анализа: важно мониторить систему на наличие угроз, действий, организовать сбор событий информационной безопасности и проводить регулярный анализ безопасности.