



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ «ВОСХОД»

Риски при массовом переходе на удалённую работу

Андрей Пьянченко

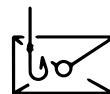
Руководитель департамента ИБ НИИ Восход

Изменение периметра защищаемого объекта!!!



Проблемы доступности корпоративных ресурсов

- качества интернет соединения
- увеличения нагрузки на каналы
- увеличения нагрузки на сервисы



Фишинг



Компрометация корпоративной почты



Увеличение хакерских атак на корпоративную сеть



Утечка конфиденциальной информации учреждения ввиду отсутствия на рабочем месте сотрудника необходимых мер и механизмов защиты информации

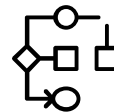
Переход (особенно в условиях спешки) на незащищенные внешние сервисы организации коллективной работы (системы ВКС, хранилища и т.д.) что может повлечь утечку конфиденциальной информации и/или неправомерный доступ к рабочему месту сотрудника

Какие ИБ-решения должны быть внедрены в компании, чтобы обеспечить безопасность?

- защита периметра сети и межсетевых взаимодействий
- средства обнаружения атак
- защищенный удаленный доступ сотрудников к внутренним ресурсам
- система фильтрации электронной почты
- система фильтрации веб-трафика
- средства защиты от несанкционированного доступа
- подсистема антивирусной защиты
- системы юридически значимого документооборота
- DLP
- разработать и утвердить регламенты удаленной работы
- провести работу с сотрудниками, в части проведения обучения (лекции и материалы) против социальной инженерии
- организовать техническую поддержку сотрудникам, в т.ч. обеспечение необходимыми СЗИ



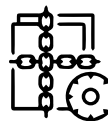
ОПРЕДЕЛИТЬ ПРИЕМЛЕМЫЕ
РИСКИ ДЛЯ ОРГАНИЗАЦИИ



ПРОИЗВЕСТИ ПЕРЕНАСТРОЙКУ
ИМЕЮЩИХСЯ СЗИ,
ЕСЛИ ЭТО ВОЗМОЖНО



ПРОВЕСТИ АНАЛИЗ
СИСТЕМЫ ИБ



ВНЕДРЕНИЕ НОВЫХ СЗИ



ОПРЕДЕЛИТЬ ИБ-СЕРВИСЫ,
НУЖДАЮЩИЕСЯ В МОДЕРНИЗАЦИИ



**СЕРВИС УПРАВЛЕНИЯ СОБЫТИЯМИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**



**СЕРВИС ЗАЩИТЫ
ОТ DDOS-АТАК**



**СЕРВИС ОБЛАЧНОЙ
ЭЛЕКТРОННОЙ ПОДПИСИ**



- определить минимально необходимое количество сотрудников, присутствие которых необходимо на объекте информатизации
- определить перечень сотрудников, которым необходимо предоставить права удаленного администрирования информационных ресурсов организации
- определить перечень ресурсов организации доступ, к которым возможен посредством удаленного подключения
- определить перечень сотрудников, которым необходимо предоставить удаленный доступ к информационным ресурсам организации
- разработать и утвердить регламент удаленной работы ИБ-службы (довести до каждого сотрудника важность соблюдения требований);
- организовать защищенный доступ сотрудников к ресурсам организации, с применением технологий TLS ГОСТ или VPN ГОСТ;
- при необходимости обеспечить сотрудников, которым необходимо организовать удаленный защищенный доступ с применением технологии VPN ГОСТ, портативными компьютерами с предустановленными СЗИ и СКЗИ.

