Введение в цифровую безопасность

Олег Серов (Access Now)

Угроза цифровой безопасности - что это такое?

Угроза - это потенциально возможное событие, которое может подвергнуть опасности ***целостность***, ***доступность*** или ***конфиденциальность*** ваших данных.

Важно выстроить четкое представление, **что конкретно** вам нужно защитить и **от кого именно.**

Построение **модели угроз** поможет лучше понять те риски, с которыми вы можете столкнуться и оценить возможность их возникновения.

Актуальные угрозы безопасности - 2021

- Угрозы, связанные с участием в массовых мероприятиях
- Угрозы, связанные с признанием иноагентом
- Угрозы, связанные с просветительской деятельностью

С чего начать моделирование угроз

1. Что я хочу защитить?
2. От кого мне нужно это защитить?
3. Что случится плохого если мне не удастся это защитить?
4. Какова вероятность того, что мне придется это защищать?
5. На что я готов пойти, чтобы предотвратить потенциальные последствия

Составляем персональную матрицу угроз

- **объект** - что защищаем
- **угроза** - от чего защищаем
- **противник** - от кого исходит угроза
- **уязвимости** - обстоятельства, увеличивающие риск того, что объект будет скомпрометирован противниками
- **потенциал** - возможности и ресурсы, которыми вы обладаете для увеличения уровня своей безопасности
- **необходимый потенциал** - практики, используемые для увеличения уровня безопасности

Структура матрицы угроз

Угрозы (заполните их в первую очередь!)	**Противники**	**Уязвимости**	**Ущерб**	**Имеющийся потенциал**	**Необходимый потенциал**
Пример: Изъятие устройств при пересечении границы	*Пограничная/таможенная служба*	*Изъятие важных, критичных файлов*	*Время для восстановления информации, санкции со стороны государства*	*Резервная копия файлов на отдельном носителе*	*Парольная защита устройств и чувствительных файлов; безопасное удаление информации*

Политика и протокол безопасности

Политика безопасности - документ, содержащий базовые правила, принципы и практики безопасности.

Протокол безопасности (кризисный протокол) - документ, определяющий последовательность действий в критической ситуации

Желательно иметь в виде документа

- Максимальная конкретность и простота содержания
- Учет актуальной информации об угрозах