Условия эффективности многофакторной аутентификации

Всегда ли многофакторная аутентификация эффективна?

Аутентификация в системах ДБО для юр лиц в 2009-2010гг

Аутентификация при выводе сотрудников на «удаленку» в 2020г

Важно проанализировать наиболее вероятные сценарии проведения кибератаки

3 Этап новой Методики оценки угроз безопасности информации ФСТЭК от 05.02.2021

Социальная инженерия – бич нашего времени

Фактор знания (Пароль, ПИН-код, кодовое слово)

Фактор владения (Смарт-карта, USB-токен, смартфон)

Фактор свойства субъекта (отпечаток пальца, face ID, голос и т.д.)

Атаки на процедуру аутентификации

Кража аутентификаторов и аутентификация в системе с устройства злоумышленника

Получение контроля над устройством пользователя и проведение аутентификации с него

Аутентификация легального пользователя под внешним воздействием

Задачи процедуры аутентификации

Как убедиться, что с нового устройства аутентифицируется легальный пользователь?

Как убедиться, что доверенное устройство находится в руках владельца?

Как понять, что пользователь не находится под внешним воздействием?

Мониторинг процесса аутентификации пользователя

Мониторинг и анализ окружения пользователя (анализ устройства, геолокация, репутация IP

Мониторинг поведения самого пользователя и выявление аномалий

Корреляция событий в целях выявления паттернов, характерных для проведения кибератак

Повышение эффективности многофакторной аутентификации

Анализ сценариев кибератак

Мониторинг процесса аутентификации

Постоянное совершенствование подсистемы аутентификации

Спасибо за внимание!

Скородумов Анатолий Валентинович

E-mail: skorodumov@mail.ru