КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОЙ ЛИЧНОСТИ

Цель курса - совершенствование имеющихся и получение новых компетенций в сфере кибербезопасности и защиты данных, получение навыков по оцениванию возможных угроз и защиты информации.

Содержание курса:

№ п/п	Наименование темы	Содержание
1	Текущий ландшафт киберугроз	Понятие информационной безопасности. Конфиденциальность, целостность, доступность. Понятие Кибербезопасности. Связь кибербезопасности и реальной жизни человека. Различные направления в области кибербезопасноти. Текущий ландшафт киберугроз. Примеры популярных инцидентов кибербезопасности. Почему возникают инциденты кибербезопасности. Как специалисты кибербезопасности ищут ошибки в работе программного обеспечения.
2	Базовые приемы работы злоумышленников	Социальная инженерия. Фишинг. Трояны. Вирусы-шифровальщики. Бэкдоры и бот-неты. Распределенные атаки отказа в обслуживании. Вредоносное программное обеспечение. Поддельные окна идентификации и аутентификации.
3	Базовые правила безопасной работы в сети Интернет	Безопасные и небезопасные соединения в сети Интернет. Безопасное использование общественных точек доступа Wi-Fi. Безопасная передача конфиденциальной информации. Ограничения по публикованию личной информации в сети Интернет. Настройки приватности различных сервисов. Подозрительные ссылки. Недоверенные источники приложений и файлов. Безопасное использование банковских карт при оплате в сети Интернет. Безопасное использование общественных компьютеров. Политика безопасности.
4	Базовые приемы безопасной работы с электронной почтой	Электронная почта как канал распросранения угроз. Рабочая и личная почта. Безопасность и надежность паролей. Многофакторная аутентификация. Факторы аутентификации.

		Контрольные вопросы и ответы. Спам-фильтры. Черные списки исходящих адресов. Подделка адреса отправителя. Подозрительные ссылки. Режим ограниченного доступа к документам.
5	Социальная инженерия	Что такое социальная инженерия. Основной метод противодействия социальной инженерии. Омографические атаки. Домены и поддомены. Сертификаты сайтов. Как работают спам-фильтры. Звонки и СМС от мошенников. Как мошенниками формируется профиль жертвы. Безопасность при сделках в сети Интернет.
6	Ошибки пользователей при использовании корпоративных ресурсов.	Статитистика. Примеры ошибок. Принцип наименьших привилегий. Аудит привилегий. Как минимизировать риски ошибок пользователей. Резервное копирование. Различные подходы. Доступ к резервным копиям.
7	Модуль 7. Безопасное применение электронной цифровой подписи	Что такое электронная цифровая подпись (ЭЦП). Зачем нужна ЭЦП. Функции ЭЦП. Три вида ЭЦП. Что такое удостоверяющий центр. Обязанности удостоверяющих центров. Из чего состоит ЭЦП. Открытый и закрытый ключ ЭЦП. Принцип работы ЭЦП. Правила работы с ЭЦП. Что делать в случае утери ЭЦП.
8	Безопасность при удаленном доступе	Зачем нужен удаленный доступ. Угрозы применения удаленного доступа. Личные и корпоративные устройства. VPN-соединения. Правила безопасного использования. Безопасность домашних сетей. Использование централизованных хранилищ. Настройки безопасности домашнего роутера. Безопасная работа с сервисами видеоконференций.