УТВЕРЖДАЮ
Начальник управления
дополнительного образования
и международной
деятельности
_____/ Ю. С. Топорова

«02» апреля 2021

АННОТАЦИЯ

рабочей программы дисциплины

«Основы кибербезопасности и киберугроз для противодействия преступлениям с использованием информационно-коммуникационных технологий»

Учебная дисциплина входит в состав дополнительной профессиональной программы - программы повышения квалификации «Основы кибербезопасности и киберугроз для противодействия преступлениям с использованием информационно-коммуникационных технологий».

Количество часов: 52

Форма контроля: зачет

Содержание:

Дисциплина включает 12 разделов.

1. Уязвимости современных компьютерных систем
   В данном разделе слушатель познакомится с основными понятиями информационной безопасности: угрозы, уязвимости, атаки. Будут рассмотрены особенности современных киберсистем и кибератак. Кроме того, слушатель получит возможность проследить во времени основные этапы развития методов и средств защиты компьютерной информации.
2. Основы криптографии
   В данной теме будут рассмотрены основные методы защиты информации на основе криптографических преобразований данных: шифрование - способ обеспечения секретности данных, контроль целостности - проверка неизменности данных, неотказуемость - проверка авторства.
3. Методы проверки подлинности
   В данном разделе слушатель познакомится с основными этапами, которые должен пройти пользователь, прежде чем получить доступ к информационным ресурсам: идентификация, аутентификация, авторизация. Будут рассмотрены методы проверки подлинности

пользователей от простых паролей до сложных биометрических систем. Не останутся без внимания и методы проверки подлинности информационной системы при дистанционном доступе к ней.

4. Системы обнаружения вторжений
   В данном разделе слушатели познакомятся со средствами автоматического реагирования на выявленные кибератаки, а также методами сбора и анализа информации на основе которых они функционируют. Будут рассмотрены особенности функционирования различных видов подобных систем.
5. Межсетевое экранирование
   В данном разделе слушатели познакомятся с принципами и технологиями ограничения информационных потоков на границе между безопасной внутренней частью и потенциально враждебной внешней частью информационной системы. В числе прочих будут рассмотрены и персональные межсетевые экраны, которые защищают от внешних угроз только один компьютер или любое другое устройство.
6. Виртуальные частные сети
   В данном разделе будет рассмотрены технологии обеспечения защищенного взаимодействия между отдельными компьютерами или сегментами корпоративной информационной системы через недоверенное информационное пространство, например через Интернет или сеть провайдера, где любые переданные данные могут быть перехвачены или искажены злоумышленником
7. Анализ защищенности
   В данном разделе будут рассмотрены этапы проведения мероприятий по проверке информационных систем на наличие в них уязвимостей, а также методы и средства автоматического поиска уязвимостей. Такие средства могут быть использованы как для проведения атаки на систему, так и для своевременного устранения обнаруженных недостатков.
8. Антивирусные средства защиты информации
   В данном разделе будет дана классификация вредоносных компьютерных программ, будут рассмотрены различные методы их обнаружения, а также состав и принципы работы антивирусных средств.
9. Системы предотвращения утечек информации
   Системы предотвращения утечек информации - единственный класс средств защиты информации, который позволяет выявлять превышение полномочий разрешенными пользователями. В данной теме слушатели узнают о принципах работы подобных систем, основных каналах утечки информации и методах их обнаружения.
10. Виртуализация информационных систем
    В данном разделе слушатели познакомятся с технологией виртуализации - представлением "физического" компьютера или

сервера в виде программного образа, позволяющим сделать информационную инфраструктуру более управляемой и экономичной. Также будут рассмотрены угрозы информационной безопасности, связанные с использованием виртуальных систем.

11. Безопасное восстановление информационных систем

Современные информационные системы должны продолжать обслуживание пользователей даже в случае возникновения неисправностей. В данной теме будут рассмотрены основные подходы, которые применяются для обеспечения бесперебойной работы информационной системы, а также методы выявления и устранения неисправностей без прерывания ее работы.

12. Управление информационной инфраструктурой

Функционирование информационной системы крупной организации невозможно без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого компьютера или другого устройства и управляет их программным обеспечением. В данном разделе слушатель познакомится с видами, особенностями построения и функционирования таких систем.