Практическое занятие № 2

Тема: Защита кроссплатформенных программных систем от угроз проникновения противника. Методы обнаружения и противодействия угрозам отечественным кросс-платформенным информационным системам в современной геополитической обстановке.

Литература:

1. А. Бирюков. Информационная безопасность. Защита и нападение. Москва, 2024.
2. А. Белоус, В. Солодуха. Мир электроники. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. Москва, Техносфера, 2021.
3. Д. Безсонов. Методы информационно-психологического влияния, применяемые украинскими подразделениями информационно-психологических операций против участников СВО, их родственников и других граждан. Москва, 2023.

Вопросы:

1. Расскажите об основных типах уязвимостей в программном обеспечении –при *проектировании*, *реализации* и *эксплуатации*. Приведите примеры. Назовите средства централизованного управления защитой от уязвимостей ПО.

2. Как происходят кибератаки в *виртуальной* среде? Расскажите о сетевых угрозах и средствах защиты: *Security Code vGate, Docker, Kubernetes.*

3. Охарактеризуйте принцип работы *облачных технологий* и *облачных вычислений*. Что представляют собой Центры обработки данных – ЦОД?

4. Назовите общие требования к безопасности облачных систем – *сетевой* и *серверной* частям облака, безопасности хранения персональных данных и приложений. Расскажите о системах контроля безопасности облачных систем – *мониторинга* и *аудита*.

5. Как осуществляется построение системы защиты информации в корпоративной сети? Расскажите об организации защиты от вирусов (по *сигнатурам*, по *аномалиям* в трафике, с помощью *эмуляций*, по методу *белого списка*, по *эвристическому анализу* и др.).

6. Назовите проблемы эффективного использования *антивирусного* ПО. Как, по Вашему мнению, нужно правильно построить архитектуру антивирусной защиты?

7. Дайте характеристику принципам работы межсетевых экранов. Аппаратные и программные средства межсетевых экранов. Расскажите о *Next Generation FireWall*.

8. Назовите средства *обнаружения* и *предотвращения вторжений*, и утечек информации. *Web Application FireWall*. Мониторинг событий информационной безопасности. *SIEM*-системы. *DLP*-системы, принципы работы и возможности настройки.

9. Расскажите об *иммунном подходе* к защите информационных систем. Почему цифровые иммунные системы являются перспективными инструментами сетевой защиты? KasperskyOS – первая российская ОС с кибериммунитетом. Киберфизические иммунные системы. Биометрическая система кибербезопасности *DarkTrace*.

10. Угрозы *кибершпионажа* противника, способы его осуществления. Методы *кибер*разведки и *киберконтр*разведки. Стратегическая *кибер*разведка как управление рисками. Требования к специалистам по кибербезопасности в области *кибер*разведки.

11. Концепции, стандарты и методы обеспечения *кибербезопасности критических инфраструктур*. Особенности *цифровизации* промышленности, энергетики, коммуникаций.

12. *Информационная война* и методы *информационно-политического* влияния на сознание граждан, применяемые противником. Принципы выявления *фейков*.

13. Самостоятельное изучение самой свежей научной литературы (научных статей, монографий, учебников 2021 – 2024 годов издания) по теме занятия.