Практическое занятие № 1

Тема: Основные направления обеспечения кибербезопасности. Уязвимости в системах киберзащиты. Защита кроссплатформенных программных системы от проникновения противника. Новые угрозы информационным системам в России 2020-х годов, методы их поиска, обнаружения и противодействия.

Литература:

1. Н. Скабцов. Аудит безопасности информационных систем. 2018.
2. А. Бирюков. Информационная безопасность. Защита и нападение. 2024.
3. А. Белоус, В. Солодуха. Мир электроники. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. 2021.
4. К. Хэднеги. Искусство обмана. Социальная инженерия в мошеннических схемах. 2020.
5. Д. Безсонов. Методы информационно-психологического влияния, применяемые украинскими подразделениями информационно-психологических операций против участников СВО, их родственников и других граждан. 2023.

Вопросы:

1. Какие угрозы российским информационным системам возникают в нынешней геополитической ситуации? Перечислите виды современных кибератак.

2. Какова классификация сетевых кибератак по уровням иерархической модели OSI? Перечислите атаки на физическом, канальном, сетевом, транспортном и др. уровнях.

3. Расскажите об атаках на беспроводные устройства, Wi-Fi, Bluetooth и др.

4. Какие средства защиты от сетевых кибератак различного рода Вам известны? Как минимизировать угрозу кибератак на Ваш компьютер? Ноутбук? Смартфон?

5. Расскажите об угрозе киберпреступности и кибертерроризма. Что представляет собой кибероружие, каковы концепции, методы и средства его применения?

6. Дайте характеристику типовым уязвимостям в системах киберзащиты – в микросхемах, в криптографических алгоритмах, в шифровальном оборудовании, в программном обеспечении информационных систем, в автомобилях, в авиации и др.

7. Назовите методы выявления программных уязвимостей – сертификационные испытания, тестирование безопасности кода, статистический анализ и др.

8. Расскажите об антивирусных программах и проактивной вирусной защите.

9. Как обезопасить от различных киберугроз учреждения и организации гражданского назначения? Как защитить от различных угроз объекты критической инфраструктуры?

10. Как обезопасить разрабатываемое Вами импортозамещающее программное обеспечение? Как защитить свои сетевые ресурсы от различных киберугроз?

11. Расскажите о методах социальной инженерии. Какие виды фишинговых атак Вам известны? Перечислите их. Какие методы борьбы с ними Вы можете предложить?

12. Расскажите о методах информационно-психологического влияния противника на российских граждан. Борьба с деструктивным контентом в сети Интернет – на Web-сайтах, в социальных сетях, в Телеграм-каналах, в мессенджерах и др.

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