Опис кредитного модуля (дисципліни)

Назва модуля (дисципліни): Cyber Security of Critical Infrastructure (Кібербезпека критичних інфраструктур)

Код модуля (дисципліни): 122_ 1_1_02, 123_1_1_02
(XXX – код спеціальності, N_N_NN – номер рядка с записом дисципліни в РНП)

Тип модуля (дисципліни): обов'язкова
(обов'язкова, вибіркова)

Форми та методи навчання: лекції, лабораторні роботи, практичні заняття, самостійна робота
лекції, лабораторні заняття, практичні заняття, семінари, курсова робота(проект), самостійна робота.і т.д.

Семестри: 1
Обсяг модуля (дисципліни): кількість годин - 135; кількість кредитів ECTS – 4,5
(всі дані тільки за денною формою навчання).

1 семестр: лекції – 14 год., лабораторні роботи – 14 год., практичні заняння – 7, самостійна робота студентів – 100 год.; кількість кредитів ECTS – 4,5, вид контролю – іспит;
(залік; іспит)

Лектори: д.т.н., доц. Скарга-Бандурова І.С., к.т.н., доц. Кардашук В.С.
(науковий ступінь, наукове звання, П.І.Б.).

Мова навчання: англійська, українська
(українська, англійська, французька, німецька).

Спосіб навчання: аудиторне навчання
(аудиторне навчання, заочне(дистанційне))

Методи і критерії оцінювання

Поточний контроль: експрес-контрольні роботи, опитування на лабораторних заняттях
Експрес-контрольні роботи, тестування, колоквіуми, звіти та захист лабораторних робіт, опитування на практичних, лабораторних і семінарських заняттях, тощо

Оцінювання проводиться протягом семестру за рейтинговою системою.

Необхідні обов'язкові попередні та супутні модулі (дисципліни) (пререквізити і кореквізити): вища математика, дискретна математика, теорія ймовірності, імовірнісні процеси та математична статистика, програмування, розробка та аналіз комп'ютерних алгоритмів

Результати навчання:

В результаті вивчення дисципліни студенти повинні знати:

- способи функціонального представлення системних зв'язків для аналізу їх безпеки і резильєнтності;
- моделі та технології оцінки ризиків великих систем;
- методи аналізу ризиків для різних завдань IT-безпеки;
- статистичні інструменти для складання та аналізу даних для виявлення тенденцій щодо забезпечення безпеки;
- методи оцінки ризику технічної безпеки АСУ ТП.

В результаті вивчення дисципліни студенти повинні вміти:

- використовувати функціональні моделі системних зв'язків для структурного аналізу стійкості і оцінки ризиків систем.
- вибрати відповідний метод аналізу ризиків для різних завдань IT-безпеки.
- підготувати тестові сценарії, призначені для перевірки ефективності систем безпеки і засоби захисту для виявлення, припинення і протидії загрозам.
- використовувати різні статистичні інструменти для складання та аналізу даних з метою виявлення тенденцій щодо забезпечення безпеки та створення звітів для підтримки вимог замовника та/ або пов'язані з дотриманням вимог.
- виконати аналіз ризиків і процес аналізу, пов'язаних з маніпуляціями даних безпеки та управління.
- аналіз АСУ ТП методів оцінки ризику технічної безпеки

короткий опис, що здобувач вищої освіти повинен знати, вміти

Зміст дисципліни:

Критична інфраструктура як об'єкт аналізу безпеки: Визначення критичної інфраструктури та системи систем System of Systems). Класифікація SoS. Характеристика SoS.

Вступ до аналіз ризику структур SoS: Архітектура і атрибути SoS. Взаємозалежність в SoS. Які компоненти SoS знаходяться на кібербезпека ризику. Аналіз аудиту безпеки.

Моделі управління ризиками SoS: Ризик структури управління. Процес аналізу ризику. Оцінка ризиків. Зниження ризику. Управління ризиками Програмне забезпечення.

Огляд моделей для аналізу ризику: Кількісний та якісний аналіз ризиків. Основні поняття, пов'язані із ризиком для безпеки в SoS. Класифікація основних методик аналізу та оцінки ризиків. Кількісний проти якісного аналізу ризику. Поліпшення кількісних ризику. Гібридний аналіз ризиків в SoS.

Комплексні методи оцінювання безпеки та ризиків безпеки. Security-Aware Аналіз небезпек і оцінка ризиків (SAHARA). Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS). Відмова-Attack-Контрзаходи (FACT) Graph. FMVEA. Об'єднаний метод оцінки безпеки та ризиків безпеки.

Аналіз резильєнтності SoS: Основні характеристики резильєнтності. Стійкість, сталість, резильєнтність. Класифікація резильєнтності SoS, що базується на характеристиках відмов. Методи оцінки резильєнтності кибер-систем. Фреймворки оцінки резильєнтності.

Оцінка ризику для цілей тестування. Ризик-тестування на основі систем безпеки критично важливих або критичних для безпеки. Ризик на основі оптимізації процесу тестування. Ризик-орієнтоване планування випробувань, дизайн, приоритезация або вибір. Модель на основі підходів до тестування на основі ризику. Підтримка забезпечення якості шляхом тестування на основі оцінки ризиків (IEC 61508, ISO 26262, Common Criteria).

Показники ризиків у сфері безпеки в промисловості: Системи управління процесом (PCS) проблема оцінки ризику технічної безпеки. Обмін міждоменної інформації (CDIS), в контексті системи управління технологічних процесів (PCS) співтовариство. Моделювання кібер атак. Аналіз ризиків контролю безпеки.

Мережева безпека, аналіз ризиків для мереж управління технологічних процесів: Інфраструктура декомпозиція. Режими і наслідків відмов. Процес специфікації .Режими процесу руйнування

…….

стислий перелік тем з тематичного плану дисципліни

Рекомендована література

1. Norman T.L. Risk analysis and security countermeasure selection / CRC Press, Taylor & Francis Group, 2010.
2. Jones K. Management of Information Security and Risk: Full 2014 programme specification City University London, UK, URL: http://www.city.ac.uk/__data/assets/pdf_file/0005/178691/PSINSR-MSc-Management-of-Information-Security-and-Risk.pdf
3. Giannopoulos G., Filippini R. Risk Assessment and Resilience for Critical Infrastructures, 2012, URL: http://www.moi.gov.cy/moi/cd/cd.nsf/5D9E4DBCF6DBB062C2257A3000294D18/$file/RISK%20ASSESSMENT%20AND%20RESILIENCE%20PROCEEDINGS.pdf
4. Netkachov O., Popov P., Salako K. Quantification of the impact of cyber attack in critical infrastructures / International Conference on Computer Safety, Reliability, and Security. – 2014. – pp. 316-327.