Рівненський державний гуманітарний університет
факультет математики та інформатики
Кафедра інформаційних технологій та моделювання

АНОТАЦІЯ

Назва дисципліни / освітнього компонента	Основи кібербезпеки
Освітня програма	Інженерія програмного забезпечення Комп'ютерні науки
Компонент освітньої програми	Вибірковий
Загальна кількість кредитів та кількість годин для вивчення дисципліни	3 кредити / 90 годин
Вид підсумкового контролю з	залік
Мова викладання	українська
Викладач	кандидат юридичних наук, доцент кафедри Інформаційно-комунікаційних технологій та методики викладання інформатики Кіндрат П.В.
CV викладача на сайті кафедри	https://iktmvi.rshu.edu.ua/pro-kafedru/teachers/teacher/kindrat-pavlo-vadymovych.html
E-mail викладача	pavlo.kindrat@rshu.edu.ua

Мета та завдання навчальної дисципліни

Мета вивчення дисципліни «Основи кібербезпеки» полягає у формуванні у майбутніх спеціалістів знань, умінь та навичок в сфері комплексного захисту інформації в інформаційно-телекомунікаційних системах від основних загроз здійснення несанкціонованого доступу до інформації та руйнування інформації.

Завданнями вивчення дисципліни «Основи кібербезпеки» є дослідження принципів та методів безпечної роботи в комп'ютерних системах та мережах, ознайомлення з програмами, призначеними для захисту інформації та її носіїв, засвоєння правил налаштування програмного забезпечення, набуття знань і навичок використання технологій для побудови системи кібербезпеки.

Згідно з освітньо-професійною програмою навчальна дисципліна «Основи кібербезпеки» має забезпечити формування у здобувачів вищої освіти наступних компетентностей.

Програма навчальної дисципліни

Змістовий модуль 1. ***Стандарти кібербезпеки***

Тема 1. Концепція кібербезпеки. Загрози та ризики. Основні положення системи захисту інформації (СЗІ). Вимоги безпеки СЗІ. Умови безпеки СЗІ. Види забезпечення безпеки СЗІ. Концептуальна модель інформаційної безпеки, її основні компоненти. Інформаційна безпека. Загрози інформації та їх прояви. Класифікація загроз. Дії, які призводять до неправомірного оволодіння інформацією з обмеженим доступом.

Тема 2. Міжнародні стандарти з безпеки та оцінювання безпеки інформаційних технологій. Стандарт ISO/IEC 15408. Зміст, структура, область застосування та недоліки стандарту. Розроблення IT-продукту та його кваліфікаційний аналіз. Специфікації функцій захисту. Заявка на відповідність профілю захисту. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації». Структура й основний зміст стандарту. Оцінювання й оброблення ризиків. Організація забезпечення безпеки інформації. Управління інцидентами безпеки інформації. Стандарт безпеки ISO/IEC 17799. Розподіл відповідальності стосовно забезпечення безпеки.Безпека носіїв даних. Контроль доступу в ОС. Використання системних утиліт. Порівняння підходів за ISO 17799 і BSI. Оцінювання ефективності існуючої системи захисту ІС на основі стандарту.

Тема 3. Законодавство України в області захисту інформації. Система нормативно-правових документів в Україні, що регламентують питання захисту інформації. Структура законодавства України в області захисту інформації. Конфіденційна інформація. Основні параметри комерційної таємниці. Правові норми забезпечення безпеки і захисту інформації на конкретному підприємстві

Змістовий модуль 2. ***Методи та засоби захисту інформації в інформаційно-телекомунікаційних системах***

Тема 4. Несанкціонований доступ до інформації: способи здійснення та протидії. Способи здійснення несанкціонованого доступу (НСД). Модель способів НСД до джерел інформації. Основні задачі НСД. Класифікація загроз безпеки ІТС. Причини випадкових дій. Умисні загрози. Інсайдер. Основні канали НСД. Перехоплення паролів. Маскарад. Незаконне використання привілеїв. Шкідливі програми. Градації доступу до інформації. Напрями реалізації порушником інформаційних загроз в ІТС. Методи реалізації загроз НСД.

Тема 5. Технічні канали витоку інформації: аналіз загроз та методів протидії. Спостереження за об'єктом. Характеристика технічних каналів витоку акустичної інформації. Допоміжні технічні засоби і системи (ДТЗС). Контрольована зона (КЗ). Межа КЗ. Об’єкт інформатизації, як об’єкт розвідки. Технічний канал витоку інформації (ТКВІ). Технічні засоби розвідки (ТЗР). Спеціальні технічні засоби (СТЗ). Класифікація ТКВІ в ІТС. Електромагнітні канали витоку інформації. Причини виникнення електромагнітних каналах витоку інформації. Паразитне електромагнітне випромінювання ТЗОІ. Електричні канали витоку інформації (ЕКВІ). Виток інформації за рахунок наведень. Спеціально створювані технічні канали витоку інформації. Виток інформації створений шляхом високочастотного опромінення. Закладні пристрої. Класифікація апаратних закладних пристроїв.

Тема 6. Методи руйнування інформації та способи мінімізації пов’язаних ризиків. Умисна силова електромагнітна дія. Методи руйнування інформації. Завади. Навмисні силові впливи. Шкідливе програмне забезпечення (ШПЗ). Програмне заглушення обчислювальних систем (ПрЗ ОС). Методи заглушення ОС процедурними і декларативними ПрЗ. Загальні рекомендації з ТЗІ з обмеженим доступом від витоку каналами ПЕМВН. Організаційні заходи. Технічні заходи. Порядок контролю за станом ТЗІ.