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 Прикладна математика
Компонент освітньої програми	Вибірковий
Загальна кількість кредитів та кількість годин для вивчення дисципліни	3 кредитів / 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.

Після вивчення дисципліни «Захист інформації» у здобувачів освіти формуються такі **компетентності:**

К02. Здатність застосовувати знання у практичних ситуаціях.

К05. Здатність вчитися і оволодівати сучасними знаннями.

К06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

К08. Здатність діяти на основі етичних міркувань.

К13. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.

К16. Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами.

К17. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К20. Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.

В результаті виконання програми дисципліни передбачаються наступні **програмні результати:**

ПР01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

ПР02. Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності.

ПР04. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.

ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Очікувані результати навчання:

у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати:

- концепцію забезпечення кібербезпеки.
- загальновідомі ризики безпеці інформаційних систем що застосовують мережеві технології чи бази даних.
- відомі засоби забезпечення інформаційної безпеки комп'ютерних систем.
- міжнародні стандарти з безпеки та оцінювання безпеки інформаційних технологій.
- нормативно-правові акти України що врегульовують заходи забезпечення кібербезпеки.
- методи руйнування інформації та засоби протидії їм.

вміти:

- здійснювати швидкий пошук та як поверхневий так і глибокий аналіз ново виявлених кіберзагроз, визначати ступінь вразливості розроблюваної/обслуговуваної системи до них та визначати і застосовувати засоби протидії
- визначати доцільність та обмеження застосування нормативно-правових документів що врегульовують принципи та методи забезпечення безпеки програмних систем
- коректно описувати та документувати особливості роботи розроблюваних програмних комплексів, встановлювати правила та обмеження покликані мінімізувати ризики їх компрометації
- знижувати ризики безпеці інформаційних систем що виникають при використанні мережевих технологій та баз даних
- підбирати оптимальний набір програмних, апаратних та нормативних засобів для забезпечення належного рівня захисту баз даних та інформаційних систем в цілому.

Результати навчання для дисципліни передбачають:

- розуміння меж відповідальності за невживання заходів протидії відомим кіберзагрозам та наслідки для фізичних та юридичних осіб що користуються розроблюваним/підтримуваним програмним продуктом.
- усвідомлення вагомості функції розробника програмного забезпечення як першої лінії протидії кіберзагрозам, а також недопустимість розголошення інсайдерської інформації про структуру та принципи функціонування розроблюваних програмних продуктів.
- здатність до аналізу вразливостей інформаційних систем.
- здатність до побудови комплексного захисту інформаційних систем.
- здатність розробляти як індивідуальні так і колективні проекти з забезпечення кібербезпеки інформаційних систем.

1. 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.