# Інформаційна безпека

17 годин

| Очікувані результати | Зміст навчання |
|---|---|
| **Основи безпеки інформаційних технологій** | |
| ***Знаннєва складова***<br><br>Знає основні поняття інформаційної безпеки.<br><br>Називає технічні та програмні засоби для несанкціонованого добування інформації.<br><br>Наводить приклади вразливостей та загроз у інформаційних та комунікаційних системах.<br><br>***Діяльнісна складова***<br><br>Використовує програмні засоби для тестування та очищення операційної системи від вірусів та шкідливого програмного забезпечення<br><br>Виконує аналіз рівня захищеності операційної системи<br><br>***Ціннісна складова***<br><br>Дотримується правил мережного спілкування<br><br>Поважає права інших користувачів на конфіденційність збереження даних<br><br>Усвідомлює відповідальність за збереження власних даних | Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій. Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій.<br><br>Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз безпеки та каналів проникнення і несанкціонованого доступу до відомостей та програмного коду:<br><br>● комп'ютерні віруси та шкідливе програмне забезпечення (Malware);<br>● інтернет-шахрайство;<br>● спам-розсилки;<br>● несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем;<br><br>● бот-мережі (botnet);<br>● DDoS-атаки (Distributed |

| | |
|---|---|
| | Denial of Service);<br>● крадіжка коштів;<br>● «крадіжка особистості» (Identity Theft)<br>Основні ненавмисні і навмисні штучні загрози.<br><br>Технічні засоби добування інформації<br><br>Програмні засоби добування інформації |
| **Забезпечення безпеки інформаційних технологій** | |
| ***Знаннєва складова***<br><br>Знає основні методи і засоби захисту інформації<br><br>Пояснює суть технічного та криптографічного захисту інформації.<br><br>Описує процес керування доступом в інформаційних системах<br><br>Називає міжнародні стандарти інформаційної безпеки.<br><br>Наводить приклади видів засобів захисту інформаційних технологій<br><br>***Діяльнісна складова***<br><br>Використовує засоби адміністрування операційної системи для налаштовування прав користувачів щодо доступу до інформаційних ресурсів.<br><br>Створює (змінює) правила, які забезпечують безпеку операційних | Об'єкти захисту. Види заходів протидії загрозам безпеки. Переваги та недоліки різних видів заходів захисту. Основні принципи побудови системи безпеки інформації в автоматизованій системі.<br><br>Правові основи забезпечення безпеки інформаційних технологій. Закони України та інші нормативно-правові акти, що регламентують відносини суб'єктів в інформаційній сфері та захист інформації. Відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем.<br><br>Основні захисні механізми, які реалізуються в рамках різних заходів і засобів захисту.<br><br>Ідентифікація та аутентифікація користувачів.<br><br>Розмежування доступу |

| | |
|---|---|
| системи<br><br>Виконує моніторинг стану безпеки операційної системи за допомогою системних журналів<br><br>***Ціннісна складова***<br><br>Визначає потенційні загрози інформаційній системі<br><br>Дотримується законодавства України, яке регламентує відносини суб'єктів в інформаційній сфері та захист інформації<br><br>Усвідомлює відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем | зареєстрованих користувачів до ресурсів автоматизованих систем. Реєстрація та оперативне оповіщення про події безпеки.<br><br>Криптографічні методи захисту інформації.<br><br>Контроль цілісності програмних і інформаційних ресурсів.<br><br>Виявлення атак.<br><br>Захист периметра комп'ютерних мереж.<br><br>Керування механізмами захисту.<br><br>Міжнародні стандарти інформаційної безпеки |
| **Забезпечення безпеки комп'ютерних систем і мереж** | |
| ***Знаннєва складова***<br><br>Знає критерії, на основі яких здійснюється фільтрація даних в мережах<br><br>Описує можливості, і основні захисні механізми міжмережевих екранів (брандмауерів<br><br>Називає засоби захисту мереж<br><br>Наводить приклади мережевих загроз<br><br>***Діяльнісна складова***<br><br>Створює віртуальні приватні | Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Типова корпоративна мережа. Рівні інформаційної інфраструктури корпоративної мережі. Мережеві загрози, вразливості і атаки. Засоби захисту мереж.<br><br>Призначення, можливості, і основні захисні механізми міжмережевих екранів (брандмауерів). Переваги та недоліки брандмауерів. Основні захисні механізми: фільтрація пакетів, трансляція мережевих адрес, проміжна аутентифікація, відхилення скриптів, перевірка пошти, віртуальні приватні мережі, протидія атакам, націленим на |

| | |
|---|---|
| мережі<br><br>Виконує налаштування засобів системного міжмережевого екрану(брандмауера).<br><br>Використовує засоби моніторингу мережного трафіку<br><br>Виконує конфігурування простих маршрутизаторів<br><br>Виконує резервне копіювання ОС та даних користувачів<br><br>***Ціннісна складова***<br><br>Дотримується правил безпечної роботи в Інтернеті<br><br>Враховує наслідки несанкціонованого доступу до інформаційних систем та корпоративних мереж<br><br>Усвідомлює необхідність резервного збереження даних | порушення роботи мережевих служб, додаткові функції. Політика безпеки при доступі до мережі загального користування.<br><br>Системи аналізу вмісту поштового і веб-трафіку (електронна пошта і HTTP). Політики безпеки, сценарії і варіанти застосування і реагування.<br><br>Віртуальні приватні мережі (VPN). Загрози, пов'язані з використанням VPN.<br><br>Антивірусні засоби захисту. Загальні правила застосування антивірусних засобів в автоматизованих системах. Технології виявлення вірусів. Можливі варіанти розміщення антивірусних засобів. Антивірусний захист, як засіб нейтралізації загроз. |