

Повна назва: Захист інформації в комп'ютерних системах

Статус: Нормативна

Мета: багатоаспектний розгляд означеного поняття захисту інформації в комп'ютерних системах з позицій інтересів користувачів, програмістів, операторів, експлуатаційників, адміністраторів обчислювальних систем.

Обсяг, методики, і технології викладання дисципліни:

Тематичний план дисципліни «Захист інформації в комп'ютерних системах» на бакалавраті спеціальності 123 «Комп'ютерна інженерія» складається з трьох модулів, кожен з яких поєднує в собі відносно окремий самостійний блок дисципліни, який логічно пов'язує кілька навчальних елементів дисципліни за змістом і взаємозв'язками.

Для визначення рівня засвоєння слухачами навчального матеріалу використовуються такі форми та методи навчання:

1) лекційні заняття, на яких викладається теоретичний матеріал, наводяться практичні приклади; заняття проводяться з використанням технічних та програмних засобів;

2) лабораторні заняття, що передбачають підготовку теоретичних та практичних питань з вивчення критеріїв, методів та засобів забезпечення інформаційної безпеки, шляхи запобігання комп'ютерним інцидентам;

3) консультації, які проводяться з метою допомоги студентам у виконанні їх самостійних завдань та роз'яснення окремих розділів теоретичного матеріалу, відпрацювання студентами пропущених занять.

Структура навчальної дисципліни

№ з/п	Назви розділів та тем	Всього годин	За формами занять, годин				
			Аудиторні				Самостійна робота студента
			лекційні	семінарські	практичні	лабораторні	
ЗМІСТОВИЙ МОДУЛЬ 1. Теоретичні засади захисту інформації в комп'ютерних системах							
1	Законодавчі аспекти захисту інформації – міжнародні та державні	16	4			4	8
2	Інформаційна безпека комп'ютерних систем. Шляхи витоку інформації та способи резервування інформації	16	4			4	8
ЗМІСТОВИЙ МОДУЛЬ 2. Програмно-апаратне забезпечення системи безпеки							
3	Комп'ютерні віруси та антивірусні програми	8	2			2	4
4	Загальна характеристика криптології. Шифротехнології. Криптосистеми	16	4			4	8
5	Тема 6. Методи і засоби вбудови скритої службової інформації в аудіо - та відеосигнали. Поняття стеганографії	16	4			4	8

6	Реалізація політики безпеки штатними засобами основних операційних систем, сучасних СУБД та програмно-апаратних комплексів	16	4			4	8
ЗМІСТОВИЙ МОДУЛЬ 3. Безпека сучасних мережевих технологій							
7	Побудова системи захисту корпоративних мереж на основі застосування міжмережевих екранів і VPN рішень. Протокол SSH як засіб шифрування трафіка	16	4			4	8
8	Виявлення і протидія програмним атакам в корпоративних мережах	16	4			4	8
9	Політика безпеки при роботі у відкритих мережах в глобальній мережі Інтернет	12	4			4	4
10	Комплексна система захисту інформації підприємства, організації, установи	12	4			4	4
Всього за 8-й триместр		144	38			38	68

Знання та навички: студенти повинні

знати: міжнародні та державні нормативно-правові засади захисту інформації в комп'ютерних системах;

- основні загрози інформації та можливі шляхи реалізації НСД зловмисником;
 - основні положення по формуванню структури системи захисту інформації на підприємстві (установі, організації);
 - організаційно-методичне забезпечення системи захисту інформації;
 - особливості обробки конфіденційної інформації в автоматизованих системах;
 - основні напрями і складові КСЗІ на об'єктах інформатизації;
 - основи теорії криптографії та криптоаналізу, типи шифрувальних алгоритмів та спеціалізованих програм і характеристики обладнання для техзахисту;
 - основні уразливості механізмів безпеки сучасних операційних систем (ОС), та їх порівняльний аналіз;
 - засоби реалізації атак на протоколи;
 - методи та інструментальні засоби реалізації програмних атак;
 - основи безпечної міжмережевої взаємодії і підключення до глобальних телекомунікаційних мереж.
- термінологію локальних та глобальних мереж;

вміти:

- організувати і забезпечувати захист інформації в приміщеннях з комп'ютерної технікою і каналах зв'язку;

- аналізувати вразливості, створювати моделі загроз в автоматизованій системі;
- організовувати і забезпечувати захист інформації засобами криптографії та антивірусного захисту;
- діагностувати, протидіяти та попереджати атаки на паролі, засоби автоматичної генерації, перехвату та викриття паролів;
- діагностувати, протидіяти та попереджати атаки на служби і протоколи інформаційного обміну; засоби реалізації атак на протоколи;
- організовувати і забезпечувати захист інформації управлінням доступу до ресурсів автоматизованої системи на базі ОС Windows;
- створювати та реалізовувати політики інформаційної безпеки штатними засобами основних операційних систем;
- реалізовувати політики безпеки засобами резервного копіювання, попередження втрати даних і безперебійного живлення;
- створювати типові рішення по захисту корпоративної мережі в умовах несанкціонованого доступу за допомогою спеціальних програмних і технічних засобів, використовуючи процедури дистанційної реєстрації подій, резервування даних на сервері, перевірки захищеності комп'ютера і паролів, контроль змін в системних файлах, систему аутентифікації тощо.

Кількість годин (кількість кредитів ЄКТС): На вивчення навчальної дисципліни відводиться 144 години / 4 кредити ECTS.

Види робіт: Контроль за рівнем засвоєння матеріалу та знань студентів проводиться у таких формах: виконання лабораторних робіт; самостійне опрацювання теоретичного матеріалу, поточне опитування під час лекційних занять; залік.

Протягом триместру здійснюється поточний та підсумковий контроль. Поточний контроль здійснюється під час захисту лабораторних робіт, перевірки самостійної роботи, надання відповідей біля дошки, перевірки виконаних творчо-пошукових завдань. Підсумковий контроль з дисципліни «Захист інформації в комп'ютерних системах» проводиться відповідно до навчального плану у вигляді заліку у 11-му триместрі, в терміни, встановлені графіком навчального процесу та в обсязі навчального матеріалу.

Оцінювання:

Форма контролю	Сума балів за 11-й триместр
Захист лабораторних робіт	55
Опитування на лекційних заняттях	5
Самостійна творчо-пошукова робота	10
Загальна кількість балів за триместр	70
Залік	30
Всього за триместр	100

Викладач:

Журавська Ірина Миколаївна, кандидат технічних наук, доцент кафедри комп'ютерної інженерії ЧНУ ім. Петра Могили. Стаж науково-педагогічної діяльності – 25 років. Кількість виданих наукових праць – біля 50, у т. ч. 3 патенти, 1 навчальний посібник із грифом ЧНУ ім. Петра Могили (2016). В 1994 р. захистила дисертацію на здобуття наукового ступеня кандидата наук зі спеціальності 05.09.12 – напівпровідникові перетворювачі електроенергії у спеціалізованій вченій раді Д 016.30.03 Інституту електродинаміки НАН України (м. Київ). У 2008 р. отримала вчене звання доцента.

Сфера наукових інтересів – передача даних за різними технологіями кабельних та бездротових мереж з урахуванням зовнішніх факторів, інформаційна безпека даних, захист інформації в комп'ютерних мережах, шифрування та стеганографічні перетворення даних.