МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

«**ЗАТВЕРДЖУЮ**»
Голова Вченої ради ЧДТУ
_____/_____
«_____» _____ 20___ р.

ПРОГРАМА
навчальної дисципліни

«ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ»

шифр (за ОПП) – ОПП-8

підготовки здобувачів освітнього ступеня «бакалавр»

напряму підготовки – 6.170103 «Управління інформаційною безпекою»

2017 рік

РОЗРОБЛЕНО ТА ВНЕСЕНО КАФЕДРОЮ:
Інформаційної безпеки та комп’ютерної інженерії

Протокол засідання кафедри № __ від _____ 20 __ р.

РОЗРОБНИКИ ПРОГРАМИ: Рудницький В.М., д.т.н., проф. кафедри інформаційної безпеки та комп'ютерної інженерії, Стабецька Т.А., асистент кафедри інформаційної безпеки та комп'ютерної інженерії

Обговорено та рекомендовано до затвердження методичною комісією факультету інформаційних технологій і систем

«____» _____ 20___ р., протокол №__

ПОГОДЖЕНО

Навчально-методичний відділ _____ /_____/
підпис *ПІБ*

«____» _____20___ р.

ВСТУП

Програма навчальної дисципліни «Організаційне забезпечення захисту інформації» складена відповідно до освітньо-професійної програми підготовки здобувачів освітнього ступеня «бакалавр» напряму підготовки – *6.170103 «Управління інформаційною безпекою».*

Предметом вивчення навчальної дисципліни *«*Організаційне забезпечення захисту інформації*»* є забезпечення формування знань та вмінь, визначених освітньо-кваліфікаційною характеристикою, за сукупністю й рівнями їхньої сформованості, необхідними для вирішення професійних завдань.

Міждисциплінарні зв'язки: начальна дисципліна *«*Організаційне забезпечення захисту інформації*»* тісно пов'язана з такими дисциплінами, як «Система охорони державної таємниці», «Основи технічного захисту інформації», «Управління персоналом», «Методи та засоби захисту інформації», «Інформаційна безпека держави».

Мета викладання навчальної дисципліни полягає в ознайомленні студентів з організаційними основами забезпечення інформаційної безпеки об'єктів інформатизації, принципами системного підходу до вирішення цієї задачі, архітектурною побудовою та проектуванням систем захисту інформації, організаційно-правовим забезпеченням робіт з захисту інформації.

Завдання вивчення навчальної дисципліни:

Головне завдання дисципліни – надати студентам знання та основні поняття з основ організації забезпечення захисту інформації. Визначити основні методи та засоби забезпечення інформаційної безпеки, стратегії захисту інформації, моделювання систем та процесів захисту інформації. Розвивати у студентів прагнення творчого відношення до задач забезпечення захищеності інформації в інформаційних системах та мережах.

Результати навчання: згідно з вимогами освітньо-професійної програми, після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

Знати:

- правовий статус інформації;
- поняття інформації, як виду власності;
- класифікацію інформації;
- основні види представлення інформації;
- класифікацію та зміст можливих загроз інформації

- поняття та зміст інформації з обмеженим доступом;
- системи захисту інформації з обмеженим доступом;
- поняття охорони державної таємниці;
- вимоги та задачі забезпечення інформаційної безпеки;
- основні нормативні документи із захисту інформації;
- організаційно-правове забезпечення робіт з захисту інформації;
- правила, методи та засоби побудови системи інформаційної безпеки на підприємствах та організаціях;
- організаційні заходи захисту інформації в автоматизованих системах.

Уміти:

- визначати організаційно-правові основи захисту інформації з обмеженим доступом та особливості захисту певних видів інформації;

- визначати правові основи захисту комерційної таємниці, міжнародно-правові основи захисту інформації з обмеженим доступом, а також правовий статус та зміст інформації з обмеженим доступом про особу.

- аналізувати нормативно-правову базу в області ОЗЗІ;
- оцінювати збитки внаслідок реалізації загроз інформаційним ресурсам;
- створювати модель системи об'єктів захисту;
- складати окремі моделі загроз та порушників;
- оцінювати ризики для інформаційних ресурсів;
- розробляти політику безпеки організації;
- складати відповідні документи ОЗЗІ.

Досвід:

- здатність контролю безпеки процесів розробки та підтримки, а також адміністрування доступу до інформації з обмеженим доступом на об’єктах інформаційної діяльності.

- управління та контроль доступу в автоматизованих системах; моніторинг систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою.

На вивчення навчальної дисципліни відводиться 108 годин та 3 кредити ЄКТС.

1. Інформаційний обсяг навчальної дисципліни

Тема 1.1. *Основні положення щодо організації системи захисту інформації.*

Основи забезпечення інформаційної безпеки. Сучасна постановка проблеми захисту інформації. Основні форми прояву інформації та їх властивості. Інформаційна безпека та її забезпечення. Умови безпеки інформації. Державна політика і система ОЗЗІ в Україні. Нормативно-правова база України у сфері ОЗЗІ.

Тема 1.2. *Визначення інформаційних ресурсів, що підлягають захисту.*

Державна таємниця і конфіденційна інформація, що є власністю держави. Недержавна конфіденційна і відкрита інформація, що потребує захисту. Дослідження структури і умов функціонування інформаційної системи організації. Модель системи об'єктів захисту

Тема 1.3. *Концепція побудови системи безпеки підприємства*

Загальна характеристика організаційних методів захисту інформації. Вимоги до побудови системи безпеки підприємства. Концептуальна модель інформаційної безпеки. Види об’єктів захисту. Класифікація загроз інформаційної безпеки та види каналів витоку інформації на підприємстві. Основні напрямки організаційного захисту інформації на підприємстві.

Тема 1.4. *Дії по захисту інформації*

Характеристика захисних дій. Розголошення інформації, яка захищається. Способи запобігання розголошення інформації, яка захищається. Протидія несанкціонованому доступу до інформації.

Тема 1.5. *Організаційне забезпечення безпеки інформації обмеженого доступу.*

Державна таємниця та порядок віднесення до неї інформації. Захист державної таємниці. Організація режиму секретності, його особливості та зміст. Комерційна таємниця та порядок її визначення. Організація робіт з інформацією, яка є комерційною таємницею.

Тема 1.6. *Організація та функції служби безпеки підприємства*

Організаційна структура служби безпеки. Організація внутрішньооб’єктного режиму на підприємстві. Організація охорони об’єктів підприємства. Організація та забезпечення за захисту комерційної таємниці на підприємстві. Організація інженерно-технічної безпеки. Організація безпеки функціонування інформаційних систем. Проведення – аналітико-розвідувальної роботи.

Тема 1.7. *Організація інформаційно-аналітичної роботи*

Цілі та задачі інформаційно-аналітичної роботи. Направлення і методи аналітичної роботи. Етапи виконання інформаційно-аналітичних досліджень виробничих ситуацій. Методи виконання аналітичних досліджень.

Тема 1.8. *Забезпечення безпеки інформації на найбільш вразливих напрямках діяльності підприємства*

Захист інформації під час проведення засідань та переговорів. Захист інформації під час роботи з відвідувачами. Організація захисту інформації у кадровій службі. Організація роботи з документами.

Тема 1.9. *Організація роботи з персоналом підприємства*

Підбір та підготовка кадрів. Перевірка персоналу на благонадійність. Укладання контрактів та домовленостей про секретність. Особливості звільнення співробітників, які володіють конфіденційною інформацією.

2. Рекомендована література

Основна:

1. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.
2. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – К.: «МК-Прес», 2005. – 432 с.
3. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.
4. Мельников В.П. Информационная безопасность и защита информации. – М.: «Академия», 2008. – 336 с.
5. Дудатьєв А.В. Інформаційна безпека. Навчальний посібник. – Вінниця: УНІВАР-Сум-Вінниця, 2009. – 240 с.
6. Садердинов А.А. Информационная безопасность предприятия. – М.: «Дашков и К», 2005. – 336 с.
7. Лужецький В.А. Захист персональних даних. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 487 с.
8. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: Известия, 1997. – 246 с.

9. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

10. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / Інститут проблем національної безпеки; Національна академія Служби безпеки України. – К.: 2004. – 472 с.

11. Сѐмкин С.К. Основы информационной безопасности объектов обработки информации: Научно-практическое пособие. – Орел: Труд, 2000. – 164 с.

12. Диев С.А. Организация и современные методы защиты информации. – М.: Банковская Академия, 2007. – 420 с.

13. Корнеев И.К. Защита информации в офисе. – М.: ТК Велби, 2008. – 336 с.

14. Ярочкин В.И. Информационная безопасность. – М.: Акад. проект; Гаудеамус, 2004. – 544 с.

15. Исаев Л.М. Правовые основы информационной безопасности. – М.:

МИЭМП, 2008. – 40 с.

16. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. – М.: Российск. гос. гуманит. ун-т, 2002. – 399 с.

17. Аверченков В.И., Рытов М.Ю. Организационная защита информации. – Брянск: БГТУ, 2005. – 184 с.

18. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Навч. посібник. – Вінниця: ВНТУ, 2009. – 268 с.

Додаткова:

1. Сѐмкин С.А., Сѐмкин А.И. Основы правового обеспечения информационной безопасности. – Орел: Навигатор-технологии, 2003. – 98 с.

2. Ярочкин В.И. Безопасность информационных систем. – М.: Ось-89, 1996. 126 с.

3. Шиверский А.А. Защита информации: проблемы теории и практики. – М.: Юность, 1996. – 268 с.

4. Мельников В.В. Защита информации в компьютерных системах – М.: Финансы и статистика; Электроинформ, 1997. – 188 с.

5. Бармен С. Разработка правил информационной безопасности. – М.: «Вильямс», 2002. – 208 с.

6. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.

7. Лазарев К.А. Информация и безопасность. Композиционная технология информационного моделирования сложных объектов принятия решений. – М.:

Московский городской центр НТИ, 1997. – 164 с._ Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.

4. Форма підсумкового контролю успішності навчання

Денна форма навчання – підсумковий модульний контроль, екзамен в кінці 7 семестру.

5. Засоби діагностики успішності навчання

Оцінювання студентів проводяться згідно тематики вивчення дисципліни. Ці заходи мають на меті поглибити та закріпити знання, отримані студентами на лекціях, лабораторних роботах та в процесі самостійної роботи над навчальною та науковою літературою, рекомендованою викладачем, а також виробити у тих, хто навчається, уміння пошуку, узагальнення та викладання навчального матеріалу.

Підсумкові бали (оцінки) за кожне заняття вносяться викладачем до журналу занять навчальної групи. Одержані ними оцінки за окремі заняття враховуються при визначенні підсумкової оцінки (рейтингу) з даної навчальної дисципліни. Проводиться поточний контроль (усне та письмове опитування), виконання лабораторних завдань, підсумковий письмовий тест, екзамен в кінці 7 семестру.