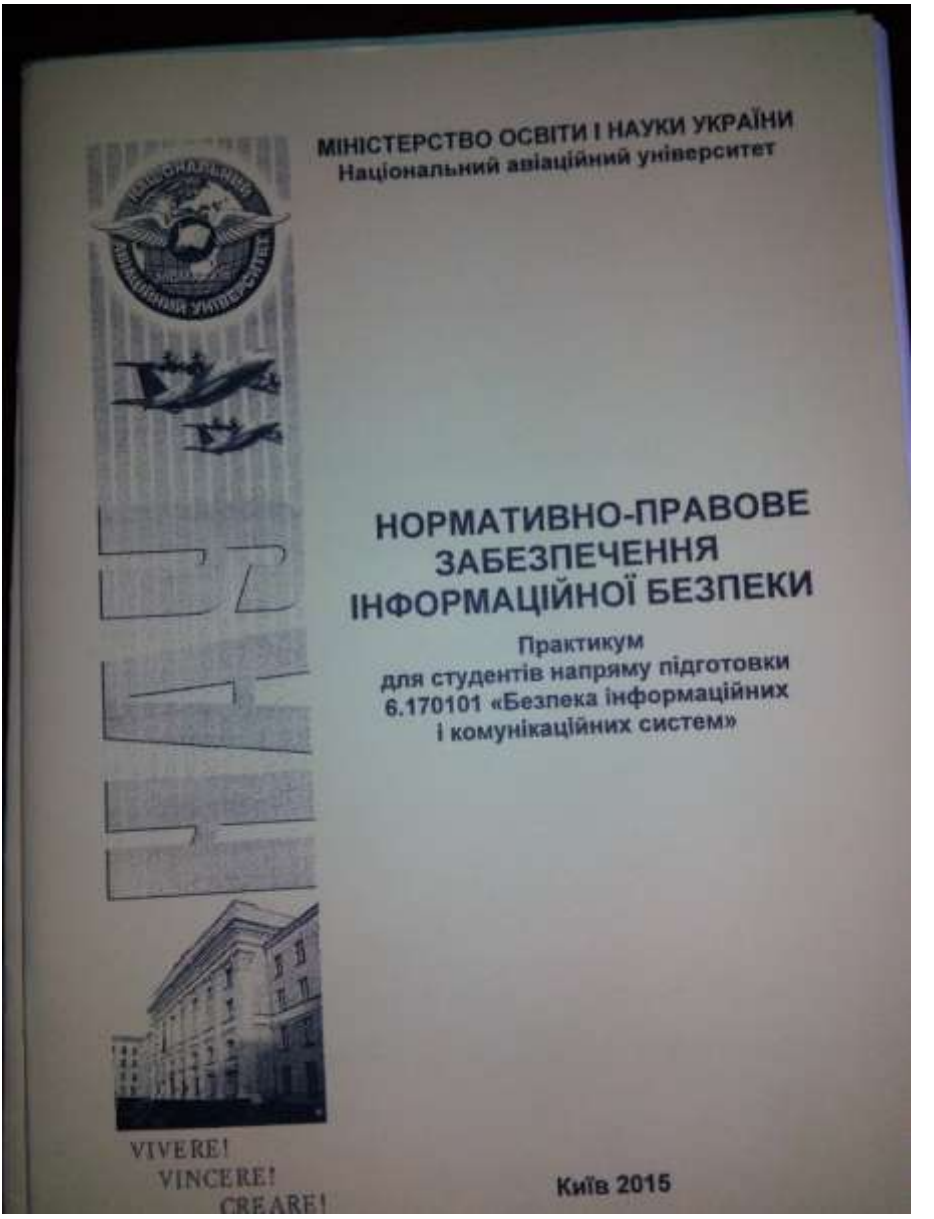
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет
НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Практикум
для студентів напряму підготовки
6.170101 «Безпека інформаційних
і комунікаційних систем»
VIVERE!
VINCERE!
CREARE!
Київ 2015

УДК 34:002 (076.5)
ББК Х 401.114р
Н 832

Укладачі: доктор техн. наук *Юдін О.К.,* доктор техн. наук *Луцький М.Г.,* кандидат техн. наук *Чунарьова А.В., Яковенко О.Л.,*
Рецензент: *канд. техн. наук С.О.Гнатюк*

Затверджено на засіданні методично-редакційної ради Національного авіаційного університету (протокол № 3/14 від 17.04.2014)

Нормативно-правове забезпечення інформаційної безпеки: ***лабораторний практикум / уклад.: О.К.Юдін, М.Г. Луцький, А.В.Чунарьова, О.Л.Яковенко. – К.: НАУ, 2015. – 32 с.***

Містить методичні рекомендації, теоретичний матеріал, практичні завдання до виконання лабораторної роботи студентів.

Для студентів напряму 6.170101 «Безпека інформаційних і комунікаційних систем».

Зміст

ВСТУП

Лабораторний практикум з дисципліни «Нормативно-правове забезпечення інформаційної безпеки», що є складовою частиною професійної підготовки фахівців за напрямом 6.170101 «Безпека інформаційних і комунікаційних систем», – навчальний посібник щодо виконання лабораторних робіт з цієї дисципліни для студентів інституту комп'ютерних інформаційних технологій НАУ.

Курс «Нормативно правове забезпечення інформаційної безпеки» має за мету надати студентам знання та основні поняття з основ нормативно-правового забезпечення інформаційної безпеки держави, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство. Завдання методичних вказівок – визначити основні терміни, поняття та категорії нормативно-правового забезпечення інформаційної безпеки на рівні тлумачення та відтворення, для їх практичного застосування та втілення у процесі фахової діяльності майбутнього спеціаліста з інформаційної безпеки. Студенти повинні навчитися вільно орієнтуватися в питаннях нормативно-правового забезпечення інформаційної безпеки держави; характеризувати основні властивості нормативної-правової бази забезпечення інформаційної безпеки; здійснювати класифікацію нормативно-правових актів України; самостійно визначати місце нормативно-правового забезпечення інформаційної безпеки в загальній системі інформаційної безпеки; самостійно давати характеристику стану законодавчої бази у сфері нормативно-правового забезпечення інформаційної безпеки; самостійно вирішувати складні нормативно-правові питання щодо організації інформаційної безпеки підпорядкованої структури в межах чинного законодавства; роз'яснювати та характеризувати основні поняття конституції України, та її розділів і норми стосовно інформатизації та захисту інформації. Знання та вміння, отримані під час вивчення даної дисципліни, будуть використані як базові для опанування переважної більшості дисциплін професійної та практичної підготовки фахівця напряму 6.170101 «Безпека інформаційних і комунікаційних систем», серед яких «Інформаційно-комунікаційні системи та мережі», «Теорія інформації та кодування», «Технології програмування», «Прикладна криптологія», «Захист програмного забезпечення».

МОДУЛЬ №1 «Загальна нормативно-правова база інформаційної безпеки. Основні поняття та положення»

Лабораторна робота №1

Тема — *основні положення інформаційної безпеки держави. Система нормативно-правового та організаційного управління інформаційною безпекою.*

Мета — *вивчення основних понять інформаційної безпеки держави та базових напрямів нормативно-правового та організаційного управління інформаційною безпекою.*

Основні завдання:

1. вивчення поняття інформаційної безпеки, а також визначення об'єктів та суб'єктів інформаційної діяльності, що підлягають захисту;
2. уведення визначення інформаційної системи та її властивостей, як об'єктів захисту інформації;
3. вивчення базових понять і основних напрямів захисту інформаційної системи та її ресурсів;
4. визначення основних категорій, які регулюють нормативно-правовий порядок забезпечення інформаційної безпеки держави.

Основні теоретичні відомості

За останні роки в Україні реалізовано комплекс заходів щодо удосконалення та забезпечення інформаційної безпеки. Розробляється та впроваджується сучасна база правового забезпечення галузі. Прийнято Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», низку інших законів, створюються механізми їх реалізації, готуються законопроекти, що регламентують суспільні відносини в інформаційній сфері.

Здійснюються певні заходи щодо забезпечення захисту інформації в органах державної влади, на підприємствах, в установах і організаціях усіх форм власності.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Основні поняття інформаційної безпеки держави;

2. Інформаційна система, як об’єкт захисту;
3. Нормативно-правове забезпечення інформаційної безпеки.

Запитання для самоперевірки

1. Наведіть визначення інформаційної безпеки.
2. Назвіть об’єкти інформаційної безпеки.
3. Визначте інтереси держави в інформаційній сфері.
4. Що розуміють під загрозою інформаційним ресурсам?
5. Назвіть основні напрями забезпечення безпеки інформації.
6. Назвіть основні характеристики інформаційної системи.
7. Які існують базові принципи захисту інформаційних систем?
8. Які рівні захисту інформаційних систем вам відомі?

Лабораторна робота №2

Тема — *основні поняття загально-законодавчого забезпечення інформаційної безпеки*

Мета — *вивчення основних понять та принципів загально-законодавчого забезпечення захисту інформації.*

Основні завдання:

1. вивчення основних положень Конституції України, як основного закону держави, введення поняття конституційного законодавства та його ролі в становленні і існування суспільства;

2. вивчення основних положень та принципів закону України «Про власність».

3. вивчення основних положень та принципів закону України «Про авторське право та суміжні права»;

4. вивчення правових аспектів формування та порядку діяльності системи органів державної влади;

5. вивчення основних засад ліцензування видів господарської діяльності в сфері технічного захисту інформації;

6. вивчення основних завдань та положень державного комітету України по стандартизації, метрології та сертифікації;

7. вивчення основних положень та принципів закону України «Про підприємництво», як основного закону забезпечення підприємницької діяльності в сфері інформатизації держави;

Основні теоретичні відомості

До законодавчої бази держави концептуального рівня, яка уособлює загальні засади галузі інформатизації країни, суспільства та безпосередньо інформаційної безпеки, належать норми великої кількості законодавчих і нормативно-правових актів, починаючи з Конституції України, Законів України «Про інформацію», «Про державну таємницю» і закінчуючи системою концепцій, програмних

документів з питань соціально-економічного розвитку України.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Конституційне законодавство;
2. Закон України «Про власність»;
3. Закон України « Про авторське право та суміжні права»;
4. Система центральних органів виконавчої влади;
5. Закон України «Про ліцензування певних видів господарської діяльності»;
6. Стандартизація, метрологія та сертифікація;
7. Закон України «Про підприємництво»;
8. Електронний документообіг.

Запитання для самоперевірки

1. Дайте визначення поняття права власності.
2. Охарактеризуйте об'єкти права виключної власності народу України.
3. Назвіть суб’єкти авторського та суміжного права.
4. Що являється об’єктом авторського права.
5. Охарактеризуйте особисті немайнові та майнові права автора на твір.
6. Порядок захисту авторського права і суміжних прав.
7. Система центральних органів виконавчої влади.
8. Які види господарської діяльності підлягають ліцензуванню ?

Лабораторна робота №3

Тема — *захист інтересів держави в інформаційній сфері.*

Мета — *вивчення основних понять та принципів захисту інформаційних ресурсів держави.*

Основні завдання:

1. вивчення основних заходів щодо захисту інформаційних ресурсів держави, орган державного управління в сфері захисту інформації;
2. вивчення основних понять організації і реалізації державної політики у сфері захисту інформаційних ресурсів;

3. вивчення основних положень та розділів Концепції національної безпеки України як основи державної політики в різних сферах суспільного життя;

4. вивчення основних положень та розділів Концепції інформаційної безпеки як основи формування політики в галузі забезпечення інформаційної безпеки України;

5. вивчення основних положень та понять Закону України «Про державну таємницю».

Основні теоретичні відомості

Сучасні організації та підприємства дедалі ширше впроваджують корпоративні інформаційно-комунікаційні системи та мережі (ІКСМ) у свою діяльність. Новітні інформаційно-комунікаційні технології об'єднали корпоративні мережі в глобальне інформаційне середовище.

Концепція інформаційно-комунікаційних мереж є логічним результатом розвитку інформаційних технологій та їх упровадження в усі сфери діяльності сучасного суспільства. Для забезпечення захисту інформаційних ресурсів держави в мережах передавання даних, проведення єдиної державної політики у сфері захисту інформації та підвищення рівня захисту державних інформаційних ресурсів, було вперше створено ***орган державного управління*** — *Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України* (*ДСТЗІ СБУ; натепер базові функції покладено на Державну службу спеціального зв'язку та захисту інформації — Держспецзв'язок)*.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Заходи захисту інформаційних ресурсів держави;
2. Державна політика у сфері захисту інформаційних ресурсів;
3. Концепція національної безпеки України;
4. Концепція та доктрина інформаційної безпеки;
5. Закон України «Про державну таємницю».

Запитання для самоперевірки

1. Які ви знаєте заходи щодо забезпечення інформаційної безпеки

держави?

3. Як забезпечується інформаційна безпека України?

4. Що являє собою орган державного управління у сфері захисту інформації?

6. Наведіть особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя.

7. Які існують загрози інформаційній безпеці України?

8. Наведіть джерела загроз інформаційній безпеці України.

9. Які головні принципи забезпечення національної безпеки?

Лабораторна робота №4

Тема — *сфера інформатизації*

Мета — *вивчення основних положень та розділів законодавчих документів в сфері інформатизації.*

Основні завдання:

1. вивчення основних положень та понять Закону України "Про інформацію", проведення класифікації інформації як головного об'єкта захисту за правовим режимом доступу, визначення переліку інформації, що має обмежений доступ;

2. вивчення основних положень та розділів Закону України «Про Концепцію Національної програми інформатизації»;

3. вивчення основних положень та розділів Закону України «Про Національну програму інформатизації».

Основні теоретичні відомості

Інформатизацію держави і суспільства можна розглядати як формування і реалізацію глобального процесу активного впровадження й широкомасштабного використання інформаційних ресурсів. У процесі інформатизації відбувається перетворення традиційних технологічних методів і засобів виробництва та способів існування суспільства в новий — постіндустріальний. Основою процесу інформатизації є використання новітніх наукоємних технологій. Підґрунтям існування загальнонаціональної системи інформаційних ресурсів держави стають інформаційно-комунікаційні системи та мережі, інтегровані бази даних та бази знань, експертні системи якісного прийняття рішень і т. ін.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта

завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Закон України "Про інформацію";
2. Закон України «Про Концепцію Національної програми інформатизації»;
3. Закон України «Про Національну програму інформатизації».

Запитання для самоперевірки

1. Розкрийте поняття інформаційних відносин.
2. Проведіть класифікацію інформації за правовим режимом доступу.
3. Яка наступає відповідальність за порушення і неправильне встановлення режимів доступу до інформації?
4. Основні положення Закону України "Про науково-технічну діяльність ".
5. Назвіть Загальні положення щодо розвитку інформатизації та науково-технічної діяльності в Україні.
6. Правові основи розвитку та діяльності галузі інформатизації та науково-технічної діяльності Україні.

Лабораторна робота №5

Тема — *сфера науково-технічної діяльності*

Мета — *вивчення основних положень та розділів законодавчих документів в сфері науково-технічної діяльності,науково-технічної експертизи, а також загальних засад формування, виконання та коригування програми науково-технічного розвитку України.*

Основні завдання:

1. введення поняття науково-технічна інформація та науково-технічна діяльність;
2. визначити мету та задачі науково-технічної діяльності;
3. визначити нормативно-правові основи та порядок проведення науково-технічної експертизи;
4. вивчення основних заходів щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні;
5. вивчення порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади.

Основні теоретичні відомості

Науково-технічна інформація охоплює отримувані в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності результати, зафіксовані у формі, яка забезпечує їх відтворення, використання та

поширення. Науково-технічна інформація є суспільним надбанням, необхідною умовою продуктивної інтелектуальної діяльності, зокрема наукової і технічної творчості. Інформаційна продукція та послуги органів науково-технічної інформації, а також підприємств, установ, організацій, окремих громадян, які провадять науково-інформаційну діяльність, можуть бути об'єктами товарних відносин, що регулюються чинним законодавством.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Науково-технічна інформація;
2. Наукова та науково-технічна діяльність;
2. Наукова та науково-технічна експертиза;
3. Розвиток національної складової глобальної інформаційної мережі Інтернет;
4. Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади.

Запитання для самоперевірки

1. Дайте визначення науково-технічній інформації.
2. Назвіть основи правового режим науково-технічну інформації.
3. Охарактеризуйте національну систему науково-технічної інформації.
4. Назвіть основні завдання наукової і науково-технічної експертизи.
5. Охарактеризуйте основні принципи та етапи наукової і науково-технічної експертизи.
6. Назвіть форми наукової і науково-технічної експертизи.
7. Основні заходи щодо розвитку національної складової глобальної інформаційної мережі.
8. Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади.

Лабораторна робота №6

Тема — *сфера зв'язку та радіочастотного ресурсу держави.*

Мета — *вивчення основних положень та розділів концептуальних документів у сфері зв'язку (конфіденційного*

зв'язку), телекомунікацій та радіочастотного ресурсу.

Основні завдання:

1. вивчення правових, економічних і організаційних основ діяльності в галузі зв'язку;
2. визначення мети та завдання впровадження Єдиної системи національного зв'язку;
3. вивчення основних положень та організаційних засад системи радіочастотного ресурсу та його розподілу за Законом України «Про радіочастотний ресурс України»;
4. визначення основних складових національної системи конфіденційного зв'язку; розкриття основних напрямів системи надання послуг конфіденційного зв'язку;
5. вивчення сфери телекомунікацій, захист інформаційних ресурсів, вимоги та правила.

Основні теоретичні відомості

Основна функція ІКСМ або інформаційних систем передавання даних в умовах функціонування інтегрованих інформаційних комплексів полягає в організації оперативного і надійного обміну інформацією між абонентами (користувачами) національних інформаційних ресурсів та їх власниками. Головний показник ефективності інформаційно-комунікаційних мереж — час доставляння інформації та її кількість. Ці чинники залежать від ряду факторів: структури мережі зв'язку, пропускної здатності інформаційної мережі зв'язку, способів з'єднання каналів зв'язку між взаємодіючими абонентами, протоколів інформаційного обміну, методів доступу абонентів до середовища передавання, методів маршрутизації пакетів тощо. Унаслідок інтенсивного збільшення кількості користувачів інформаційних систем та їх ресурсів сучасні технології потребують оперативного створення сучасних каналів зв'язку, що відповідають міжнародним вимогам та стандартам, а також розроблення відповідної законодавчої бази.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Правові, економічні і організаційні основи діяльності в галузі

зв'язку;

2. Концепція розвитку зв’язку в державі;

3. Радіочастотний ресурс та система його розподілу.

Запитання для самоперевірки

1. Наведіть організаційно-правові засади та заходи розвитку зв’язку в Україні.

2. У чому полягають порядок та умови надання послуг зв’язку в мережах загального користування?

3. Якою є відповідальність підприємств і об’єднань зв’язку перед споживачами послуг?

4. У чому полягає порядок використання радіочастотного ресурсу і радіоелектронних засобів?

5. Охарактеризуйте управління і регулювання в системі зв’язку.

6. У чому полягає повноваження Українського державного центру радіочастот та нагляду за зв’язком?

7. Що таке державний нагляд за використанням радіочастотного ресурсу?

Лабораторна робота №7

Тема — *сфера конфіденційного зв’язку.*

Мета — *вивчення основних положень та розділів концептуальних документів у сфері конфіденційного зв’язку.*

Основні завдання:

1. визначення основних складових національної системи конфіденційного зв’язку; розкриття основних напрямів системи надання послуг конфіденційного зв’язку;

2. вивчення сфери телекомунікації, захист інформаційних ресурсів, вимоги, правила.

Основні теоретичні відомості

Послуги конфіденційного зв’язку в Національній системі конфіденційного зв’язку (НСКЗ) надаються споживачам з установленими рівнями якості конфіденційного зв’язку відповідно до нормативних документів, прийнятих Держспецзв’язком України.

Послуги конфіденційного зв'язку в НСКЗ надаються споживачам з встановленими рівнями якості конфіденційного зв'язку відповідно до нормативних документів та законодавчих актів. Безпека оброблення конфіденційної інформації забезпечується операторами зв’язку шляхом комплексного використання криптографічних і технічних засобів захисту інформації та здійснення організаційно-правових, інженерно-технічних заходів, спрямованих на запобігання

розголошенню конфіденційної інформації.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Національна система конфіденційного зв'язку;
2. Система надання послуг конфіденційного зв'язку;
3. Сфера телекомунікації, захист інформаційних ресурсів, вимоги, правила.

Запитання для самоперевірки

1. Розкрийте поняття національної системи конфіденційного зв'язку та її складових.
2. Яким є порядок забезпечення безпеки обробки конфіденційної інформації?
3. Визначте умови надання послуг конфіденційного зв'язку.
4. Висвітліть телекомунікації як невід'ємну частину виробничої та соціальної інфраструктури України.
5. Які основні принципи діяльності у сфері телекомунікацій, надання телекомунікаційних послуг на території України ви знаєте?
6. Розкрийте суть захисту інформаційних ресурсів в телекомунікаційних системах.
7. Наведіть основні умови та вимоги до систем захисту інформації.
8. Розкрийте питання КСЗІ в телекомунікаційних системах, а також висвітліть порядок розроблення та впровадження КСЗІ.

Лабораторна робота №8

Тема — *технічний захист інформації. Державна політика у сфері захисту технічного захисту інформації.*

Мета — *вивчення основних положень та розділів концептуальних нормативно-правових документів у сфері ТЗІ в Україні.*

Основні завдання:

1. вивчення основних положень та розділів Концепції технічного захисту як основи державної політики у сфері захисту інформації інженерно-технічними заходами;
2. вивчення основних розділів Положення про технічний захист

інформації в Україні, що визначає порядок організації ТЗІ в Україні;

3. вивчення основних розділів Положення про контроль за функціонуванням системи технічного захисту інформації, що визначає правові та організаційні засади контролю за функціонуванням системи технічного захисту інформації України.

Основні теоретичні відомості

Захист інформаційних ресурсів у мережах передавання даних, проведення єдиної державної політики у сфері захисту інформації та підвищення рівня захисту державних інформаційних ресурсів в інформаційних і телекомунікаційних системах, забезпечення інформаційної безпеки об'єктів інформаційної діяльності, організацію діяльності державної системи технічного захисту інформації на міжрегіональному, регіональному, галузевому рівнях виконує ***орган державного управління*** *— Держспецзв'язок України.*

Одними з ключових напрямів державної політики у сфері інформаційної безпеки є ТЗІ та КЗІ.

Традиційно ТЗІ можна поділити на два великі класи виконуваних завдань із захисту інформації: захист інформації від несанкціонованого доступу та захист інформації від її витоку технічними каналами.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Концепція технічного захисту інформації в Україні;
2. Основні засади технічного захисту інформації в Україні.;
3. Контроль за функціонуванням системи технічного захисту інформації.

Запитання для самоперевірки

1. Яка концепція технічного захисту інформації в Україні?
2. Наведіть основні загрози безпеці інформації.
4. Охарактеризуйте систему ТЗІ держави.
5. Наведіть принципи формування і проведення державної політики у сфері ТЗІ.
6. Охарактеризуйте основні напрями державної політики у сфері ТЗІ.

7. Які організаційні та правові засади технічного захисту інформації в Україні?

8. Наведіть суб'єкти системи ТЗІ.

9. Охарактеризуйте основні завдання Департаменту.

10. Який контроль за функціонуванням системи ТЗІ?

Лабораторна робота №9

Тема — *технічний захист інформації. Сертифікація та експертиза засобів ТЗІ*

Мета — *вивчення основних положень та розділів концептуальних нормативно-правових документів в сфері проведення державної експертизи, сертифікації засобів ТЗІ.*

Основні завдання:

1. вивчення нормативно-правових основ, задач та порядку проведення державної експертизи в сфері технічного захисту інформації;

2. вивчення основних понять та порядку проведення сертифікації засобів забезпечення технічного захисту інформації загального призначення;

3. вивчення порядку проведення та організації ліцензування господарської діяльності у галузі технічного захисту інформації;

4. вивчення вимог та порядку організації захисту, що обробляється засобом КРТ;

Основні теоретичні відомості

Загальне керівництво сертифікаційною діяльністю у сфері захисту інформації, організація і координація робіт із сертифікації здійснюються національним органом із сертифікації — Державним комітетом України з питань технічного регулювання та споживчої політики та Держспецзв'язку. Сертифікацію здійснюють винятково органи сертифікації, які призначені та/або вповноважені в установленому порядку для виконання робіт із сертифікації в системі і мають відповідну акредитацію.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань.

Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Порядок проведення державної експертизи в сфері технічного захисту інформації;
2. Сертифікація засобів забезпечення технічного захисту інформації загального призначення;
3. Порядок ліцензування господарської діяльності у галузі технічного захисту інформації;
4. Створення та порядок проведення атестації комплексів технічного захисту інформації;
5. Засоби копіювально-розмножувальної техніки;
6. Організації проектування і проектної документації для будівництва

Запитання для самоперевірки

1. Як проводиться державна експертиза у сфері технічного захисту інформації?
2. Яких типів буває експертиза у сфері ТЗІ?
3. Який порядок організації та проведення експертизи?
4. Охарактеризуйте порядок надання експертного висновку та атестата.
5. Яка основна мета і завдання сертифікації засобів забезпечення ТЗІ загального призначення?
6. Охарактеризуйте порядок проведення робіт із сертифікації.
7. Які види робіт з ТЗІ підлягають ліцензуванню?
8. Охарактеризуйте підготовчі роботи зі створення комплексів ТЗІ.
9. Охарактеризуйте етапи створення комплексу ТЗІ.

*МОДУЛЬ №2 «***Спеціалізована нормативно-правова база інформаційної безпеки***»*

Лабораторна робота №1

Тема — *сфера криптографічного захисту інформації.*

Мета — *вивчення основних положень та розділів нормативно-правових документів, стандартів у сфері КЗІ.*

Основні завдання:

1. вивчення нормативно-правових основ здійснення КЗІ в Україні;
2. вивчення основних положень та розділів Закону України «Про електронний цифровий підпис»;
3. вивчення нормативно-правових основ та порядку розроблення, виготовлення та експлуатації засобів КЗІ інформації;
4. вивчення нормативно-правових основ, змісту та порядку проведення сертифікації засобів КЗІ.

Основні теоретичні відомості

Сучасний етап розвитку держави характеризується стрімким розвитком кіберзлочинності та її реалізацією в усі сфери діяльності суспільства. Дедалі частіше об'єктом злочинних посягань стає інформація в усіх її формах та безпосередньо її властивостей: конфіденційності, доступності, цілісності.

Основними напрямами використання криптографічних методів захисту інформації стали передавання конфіденційних даних каналами зв'язку, встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому (закритому) вигляді. Системи криптографічного захисту інформації є базовою складовою інформаційної безпеки держави, а отже, і національної безпеки в цілому.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Здійснення криптографічного захисту інформації в Україні;
2. Закон України «Про електронний цифровий підпис»;
3. Розроблення, виготовлення та експлуатація засобів криптографічного захисту конфіденційної інформації;
4. Сертифікація засобів криптографічного захисту інформації.

Запитання для самоперевірки

1. Який порядок здійснення КЗІ в Україні?
2. У чому полягає правовий статус та який порядок використання ЕЦП?
3. Який порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації?
4. Які засоби належать до засобів криптографічного захисту конфіденційної інформації?
5. Які відомості включають до технічного завдання на розроблення криптографічного захисту конфіденційної інформації?
6. Що включає в себе порядок проведення сертифікації засобів криптографічного захисту інформації?

Лабораторна робота №2

Тема — *захист інформації в автоматизованих системах. Загальні положення та визначення.*

Мета — *вивчення основних положень та розділів концептуальних, нормативно-правових документів у сфері захисту інформації в автоматизованих системах.*

Основні завдання:

1. вивчення основних положень та розділів Закону України «Про захист інформації в автоматизованих системах»;
2. вивчення нормативно-правових основ організації служби захисту інформації в АС;
3. вивчення основних завдань та структури служби захисту інформації в АС.

Основні теоретичні відомості

Захисту підлягає будь-яка інформація в АС. Необхідність організації процесу захисту визначається власником інформаційних ресурсів або чинним законодавством. Об'єктом захисту інформації в АС є права власників цієї інформації та власників АС, права користувача. Суб'єктами відносин, пов'язаних з обробленням інформації в АС, є: власники інформації; власники системи; користувачі; уповноважений орган у сфері захисту інформації в системах. У державних установах і організаціях можуть створюватись підрозділи або служби щодо організації роботи, пов'язаної із захистом інформації, підтриманням рівня захисту інформаційних ресурсів в АС і відповідають за ефективність системи захисту згідно з вимогами закону.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Закон України "Про захист інформації в автоматизованих системах";
2. Служба захисту інформації в АС.

Запитання для самоперевірки

1. Охарактеризуйте основи регулювання правових відносин щодо захисту інформації в автоматизованих системах.

2. Назвіть суб'єкти відносин, пов'язаних з обробленням інформації в АС.

4. Назвіть способи забезпечення захисту інформації в АС.

5. Який порядок організації захисту в АС?

6. Розкрийте поняття «служба захисту інформації в АС».

7. Назвіть основні завдання СЗІ.

8. Охарактеризуйте функції СЗІ під час створення та експлуатації КСЗІ.

Лабораторна робота №3

Тема — *захист інформації в автоматизованих системах. План захисту інформації.*

Мета — *вивчення основних положень та розділів плану захисту інформації в автоматизованих системах.*

Основні завдання:

1. вивчення методики створення та організації плану захисту інформації в АС;
2. визначення процедури класифікації інформації та опису компонентів АС;
3. побудова моделі загроз та порушника;
4. принципи реалізації політики безпеки в АС.

Основні теоретичні відомості

План захисту інформації в АС є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу АС

План захисту інформації в АС розробляється на підставі виконаного аналізу технології оброблення інформації, аналізу ризиків,сформульованої політики безпеки інформації. План захисту визначає і документально закріплює об'єкт захисту інформації в АС, основні завдання захисту, загальні правила оброблення інформації в АС, мету побудови та функціонування КСЗІ, заходи щодо захисту інформації. План захисту має фіксувати на певний момент часу склад АС, перелік оброблюваних відомостей, технологію оброблення інформації, склад комплексу засобів захисту інформації, склад необхідної документації та ін..

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта

завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Методичні рекомендації щодо захисту інформації в АС;.
2. Опис програмно-апаратного забезпечення та класифікація інформації;
3. Побудова моделі загроз;
4. Побудова моделі порушника;
5. Порядок розробки політики безпеки інформації в АС.

Запитання для самоперевірки

1. Охарактеризуйте основні складові плану захисту інформації в АС.
2. Опишіть компоненти АС та технології обробки інформації.
3. Розкрийте поняття моделі загроз.
4. Назвіть основні загрози для інформації в АС.
5. Наведіть способи здійснення загроз в АС.
6. Розкрийте поняття моделі порушника.
7. Проведіть класифікацію порушників інформації в АС.
8. Охарактеризуйте політику безпеки інформації в АС.

Лабораторна робота №4

Тема — *захист інформації в автоматизованих системах. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.*

Мета — *вивчення основних положень процедури класифікації АС та порядку вибору профілю захищеності.*

Основні завдання:

1. вивчення особливостей проведення класифікації АС;
2. вивчення особливостей визначення підкласів АС;
3. вивчення особливостей порядку вибору функціональних профілів захищеності залежно від накладених умов;

Основні теоретичні відомості

Автоматизована система являє собою організаційно-технічну систему, що об’єднує операційні системи (ОС), фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу комплексу засобів захисту (КЗЗ) залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми.

Стандартні функціональні профілі будуються на підставі існуючих вимог до захисту певної інформації від певних загроз і відомих натепер функціональних послуг, що дозволяють

протистояти цим загрозам і забезпечувати виконання поставлених вимог.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Класифікація автоматизованих систем;
2. Підкласи автоматизованих систем;
3. Поняття функціонального профілю захищеності.

Запитання для самоперевірки

1. Проведіть класифікацію АС.
2. Проведіть класифікацію підкласів АС.
3. Що таке функціональний профіль захищеності?
4. Назвіть семантику функціонального профілю захищеності.
5. Назвіть стандартні функціональні профілі захищеності для АС класу 1.
6. Назвіть стандартні функціональні профілі захищеності для АС класу 2.
7. Назвіть стандартні функціональні профілі захищеності для АС класу 3.

Лабораторна робота №5

Тема — *захист інформації в автоматизованих системах. Технічне завдання зі створення комплексної системи захисту інформації в автоматизованій системі* **.**

Мета — *вивчення основних положень та розділів концептуальних, нормативно-правових документів у сфері захисту інформації в автоматизованих системах.*

Основні завдання:

1. вивчення вимог до розроблення ТЗ зі створення КСЗІ в АС;
2. вивчення вимог до захисту інформації від НСД під час оброблення в АС класу 2 і встановлення мінімально необхідного переліку функціональних послуг безпеки та рівнів їх реалізації в комплексах засобів захисту інформації.

Основні теоретичні відомості

Технічне завдання зі створення комплексної системи захисту інформації (КСЗІ) в АС є базовим організаційно-технічним

документом для виконання робіт із забезпечення захисту інформації в системі.

Технічне завдання зі створення КСЗІ розробляється у разі потреби в розробленні або модернізації КСЗІ існуючої АС. Технічне завдання зі створення КСЗІ потрібно розробляти з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об'єднання в єдину систему необхідних заходів і засобів захисту від різноманітних загроз безпеки інформації на всіх етапах життєвого циклу АС.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Технічне завдання на створення комплексної системи захисту інформації в автоматизованій системі;
2. Порядок розроблення, зміст та основні складові ТЗ;
3. Вимоги до комплексної системи захисту інформації.

Запитання для самоперевірки

1. Назвіть загальні вимоги до розробки технічного завдання на створення КСЗІ в АС
2. Назвіть порядок розроблення технічного завдання.
3. Перелічіть вимоги до комплексної системи захисту інформації.
4. Назвіть зміст технічного завдання.
5. Перелічіть основні роботи етапу формування технічного завдання.
6. Перелічіть вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу.
7. Перелічіть вимоги до складу проектної та експлуатаційної документації.
8. Охарактеризуйте порядок проведення випробувань комплексної системи захисту інформації.

Лабораторна робота №6

Тема — *захист інформації в комп'ютерних системах та мережах.*

Мета — *вивчення основних положень та розділів нормативно-правових, концептуальних документів у сфері захисту інформації в комп'ютерних системах та мережах.*

Основні завдання:

1. вивчення нормативно-правових основ та загальних положень щодо захисту інформації в КС;

2. вивчення загальних критеріїв оцінювання захищеності інформації від несанкціонованого доступу, оброблюваної в КСМ;

3. вивчення вимог до порядку створення, впровадження, супроводження та модернізації засобів ТЗІ від несанкціонованого доступу в КСМ.

Основні теоретичні відомості

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і потребують захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів. Захист інформації, що обробляється в ІКСМ, полягає в створенні та підтриманні в дієздатному стані системи заходів як технічних так і нетехнічних, що дають змогу запобігти або ускладнити можливість реалізації загроз, а також зменшити потенційні збитки.

Чимало проблем забезпечення захисту інформації в ІКСМ можна вирішити організаційними заходами. Проте з розвитком інформаційних технологій спостерігається тенденція зростання потреби в застосуванні технічних заходів і засобів захисту.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Загальні положення захисту інформації в комп’ютерних системах;

2. Критерії оцінювання захищеності інформаційних систем від несанкціонованого доступу;

3. Створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

Запитання для самоперевірки

1. Назвіть основні напрями захисту інформації від НСД у комп’ютерних системах.

2. Які ви знаєте основні принципи забезпечення захисту інформації?

3. Що розуміють під безперервним захистом?

4. Наведіть основні принципи реалізації програмно-технічних засобів.

5. Назвіть критерії оцінювання захищеності інформаційних систем від НСД.

6. Проведіть класифікацію критеріїв конфіденційності, цілісності, доступності та спостережуваності.

Лабораторна робота №7

Тема — *порядок організації захисту інформації на програмно-керованих АТС.*

Мета — *вивчення основних положень та розділів нормативно-правових документів у сфері захисту інформації на програмно-керованих АТС.*

Основні завдання:

1. вивчення нормативно-правових засад та загальних положень захисту інформації на програмно-керованих АТС;

2. вивчення методики оцінювання захищеності інформації, що циркулює на програмно-керованих АТС;

3. вивчення специфікації функціональних послуг захисту інформаційних ресурсів АТС та рівнів стійкості механізмів захисту інформації під час реалізації послуг захисту;

4. вивчення гарантій захисту інформації, що циркулює на програмно-керованих АТС загального користування;

5. вивчення нормативно-правових основ та розділів порядку виконання робіт з позиції технічного захисту інформації на програмно-керованих АТС загального користування.

Основні теоретичні відомості

Об’єктом технічного захисту на програмно-керованих автоматизованих телефонних станціях (АТС), а також на відомчих, корпоративних АТС є конфіденційна та відкрита важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих системах. Мета технічного захисту інформації (ТЗІ) на програмно-керованих АТС загального користування, а також на відомчих, корпоративних АТС — запобігання за допомогою інженерно-технічних заходів здійсненню загроз інформаційним ресурсам.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання

відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Загальні положення захисту інформації на програмно-керованих АТС.;
2. Оцінювання захищеності інформації, що циркулює на програмно-керованих АТС;
3. Функціональні послуги захисту на програмно-керованих АТС;
4. Гарантії захисту інформації на програмно-керованих АТС загального користування;
5. Порядок виконання робіт, спрямованих на технічний захист інформації на програмно-керованих АТС загального користування.

Запитання для самоперевірки

1. Назвіть основні принципи ТЗІ на АТС.
2. Охарактеризуйте структуру програмно-керованих АТС із позицій технічного захисту інформації.
3. Проведіть класифікацію порушників на програмно-керовані АТС щодо впливу на її компоненти.
4. Назвіть види забезпечення систем ТЗІ на АТС.
5. Охарактеризуйте основні дані для оцінювання якості документованості процесу створення системи ТЗІ.
6. Назвіть аспекти оцінювання захищеності інформації в середовищі створення та експлуатаційному середовищі оцінюваної АТС.
7. Охарактеризуйте специфікації функціональних послуг захисту на програмно-керованих АТС.

Лабораторна робота №8

Тема — *критерії безпеки інформаційних технологій*

Мета — *ознайомлення з основоположними критеріями та вимогами оцінки захисту інформації.*

Основні завдання:

1. визначення основних вимог та критеріїв оцінки безпеки інформаційних технологій;
2. визначення переліку базових критеріїв інформаційних технологій;
3. вивчення основних правил побудови системи забезпечення інформаційної безпеки організації.

Основні теоретичні відомості

Одними з найбільш важливих нормативно-технічних документів, які стимулюють розвиток захищених інформаційних систем, мереж і засобів є документи, що стандартизують вимоги та критерії оцінки безпеки.

Стандарти інформаційної безпеки — це стандарти забезпечення захисту, призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації захищених систем оброблення інформації.

Стандарт забезпечення захисту звичайно містять опис послідовності оцінок, які необхідно виконати, щоб вважати дану характеристику безпеки підтвердженою з точки зору атестації захисту або множину характеристик безпеки, які повинна забезпечити система захисту, щоб її можна було використовувати в даному конкретному режимі забезпечення безпеки або у відповідності до загальної стратегії захисту.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати, яких навичок та знань набули студенти під час виконання індивідуальних завдань. Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Загальні відомості про вимоги та критерії оцінки безпеки інформаційних технологій;
2. Основні положення загальних критеріїв безпеки інформаційних технологій;
3. Функціональні вимоги до засобів захисту;
4. Вимоги гарантій засобів захисту.

Запитання для самоперевірки

1. Назвіть стандарти інформаційної безпеки у хронологічному порядку.
2. Охарактеризуйте мету та призначення критеріїв безпеки комп’ютерних систем.
3. Охарактеризуйте потенційні загрози безпеці та типові завдання захисту відповідно до загальних критеріїв безпеки інформаційних технологій.
4. Що розуміють під поняттям «продукт інформаційних

технологій»?

5. Що включають в себе функціональні вимоги безпеки?
6. Охарактеризуйте структуру функціональних вимог безпеки.

Лабораторна робота №9

Тема — *міжнародні стандарти та рекомендації в галузі забезпечення інформаційної безпеки.*

Мета — *ознайомлення з основоположними міжнародними стандартами, що регламентують порядок створення та експлуатації комплексних систем захисту інформації та найбільш вживаними методиками оцінювання ризику.*

Основні завдання:

1. визначення основних недоліків законодавчої системи України в галузі захисту інформації;
2. визначення переліку базових міжнародних стандартів у сфері інформаційної безпеки;
3. вивчення основних етапів процедури розроблення, створення, експлуатації та підтримання комплексної системи захисту інформації на базі міжнародного стандарту ISO 27001;
4. ознайомлення з практичними рекомендаціями стандарту ISO 27002 з питань організації системи захисту інформації;
5. вивчення методики кількісної оцінки ризику.

Основні теоретичні відомості

Успішний розвиток підприємств, установ і організацій неможливо уявити без використання постійно зростаючих обсягів інформаційних потоків, що передаються або обробляються на базі інтегрованих інформаційно-комунікаційних систем та сучасних інформаційних технологій.

Стандарти сімейства ISO 27000 — це модель системи менеджменту, яка визначає загальну організацію, класифікацію даних,системи доступу, напрями планування, методи забезпечення безпеки, практичні правила та вимоги, відповідальність співробітників, використання оцінювання ризику в контексті інформаційної безпеки підприємств. У процесі впровадження стандарту створюється система менеджменту інформаційної безпеки, мета якої — скорочення матеріальних утрат, пов’язаних з порушенням інформаційної безпеки.

Порядок виконання лабораторної роботи

Кожен студент повинен виконати індивідуальне завдання відповідно до варіанта і зробити висновки на основі проведених теоретичних та практичних досліджень. У висновках слід указати,

яких навичок та знань набули студенти під час виконання індивідуальних завдань.

Порядок вибору варіанта: номер варіанта завдання відповідає порядковому номеру студента в журналі.

Кожному студенту потрібно розглянути наступні питання:

1. Стандарт ISO/IEC 27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги».
2. Стандарт ISO/IEC 27002:2005 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою».
3. Методики кількісної оцінки ризику інформаційної безпеки компанії.

Запитання для самоперевірки

1. У чому полягають основні недоліки системи законодавства України в галузі захисту інформації?
2. Які міжнародні стандарти інформаційної безпеки вам відомі?
3. Визначте мету стандарту ISO/IEC 27001:2005.
4. Наведіть визначення поняття системи менеджменту інформаційної безпеки.
5. З яких основних розділів складається стандарт ISO/IEC 27002:2005?
6. Охарактеризуйте принцип якісної оцінки ризику.
7. Які основні етапи процесу управління ризиками безпеки вам відомі?
8. Які основні цілі аудиту інформаційної безпеки?
9. Опишіть систему методів управління безперервністю бізнесу.
10. Наведіть приклади розрахунку системи ризиків компаній.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. *Information* Security Management — Specification With Guidance for Use : ISO/IEC 27001:2005. — Режим доступу:
http://www.standards.-org/standards/listing/iso_27001.
2. *Information* technology — Security techniques — Code of practice for information security management : ISO/IEC 27002: 2005. — Режим доступу:
http://www.iso.org/iso/catalogue_detail?csnumber=39612.
3. *Information* technology — Security techniques — Information security risk Magement : ISO/IEC 27005: 2008. — Режим доступу:
http://www.iso.org/iso/catalogue_detail?csnumber=42107.
4. *Information* technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems: ISO/IEC 27006: 2007. — Режим доступу:
http://www.iso.org/iso/catalogue_detail?csnumber=42505.
5. *Захист* інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. — [Чинний від 1996.10.10]. — К. : Держстандарт України, 1996. — 20 с.
6. *Захист* інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. — [Чинний від 1997.07.01]. — К. : Держстандарт України, 1997. — 32 с.
7. *Захист* інформації. Технічний захист інформації. Терміни і виз-начення: ДСТУ 3396.2-97. — [Чинний від 1998.01.01]. — К. : Держ-стандарт України, 1998. — 20 с.
8. *Про державну* таємницю: Закон України від 21.01.1994 № 3855-12-ВР // ВВР. —1994. — № 24. — С. 296.
9. *Про захист* інформації в автоматизованих системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.
10. *Про інформацію*: Закон України від 02.10.1995 № 2658-XII-ВР//ВВР. —1992. — № 48. — С. 651.
11. 30. *Про телекомунікації*: Закон України: від 18.11.2003 № 1280-IV-ВР//ВВР. — 2003. — № 12. — С. 155.
12. *Конституція* України: Закон України від 28.06.1996 № 254к/96-ВР// ВВР. — 1996. — № 30. — С. 141.
13. *Технічний* захист інформації на програмно-керованих АТС за-гального користування: НД ТЗІ 1.1-001-99. — [Чинний від 1999.05.28]. — К. : ДСТСЗІ СБУ, 1999. — № 26. — (Нормативний документ системи технічного захисту інформації).
14. *Загальні* положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. — [Чинний від 1999.04.28]. — К.

: ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

15. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

16. *Типове* положення про службу захисту інформації в автоматизованій системі: 1.4-001-2000. — [Чинний від 2000.12.04]. — К. : ДСТСЗІ СБУ, 2000. — № 53.— (Нормативний документ системи технічного захисту інформації).

17. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

18. *Класифікація* автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

19. *Порядок* проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. — [Чинний від 2005.11.08]. — К. : ДСТСЗІ СБУ, 2005. — № 125. — (Нормативний документ системи технічного захисту інформації).

20. *Положення* про державну експертизу у сфері технічного захисту інформації: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. — Режим доступу:
http://zakon2.rada.gov.ua/laws/show/z0820-07.

21. *Положення* про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98. — Режим доступу:
http://zakon2.rada.gov.ua/laws/show/505/98.

Навчальне видання

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Лабораторний практикум
для студентів напряму 6.170101
«Безпека інформаційних і комунікаційних систем»

Укладачі: ЮДІН Олександр Костянтинович
ЛУЦЬКИЙ Максим Георгійович
ЧУНАРЬОВА Анна Вадимівна
ЯКОВЕНКО Олеся Леонідівна

Технічний редактор
Коректор
Комп'ютерна верстка

Підп. до друку _____ Формат 60х84/16. Папір офс.
Офс. друк Ум друк. арк. ___ . Обл.-вид. арк. ____.
Тираж 100 пр. Замовлення № _____. Вид. № __.

Видавництво НАУ
03058. Київ-58, проспект Космонавта Комарова, 1.

Свідоцтво про внесення до Державного реєстру ДК
№ ___ від _____