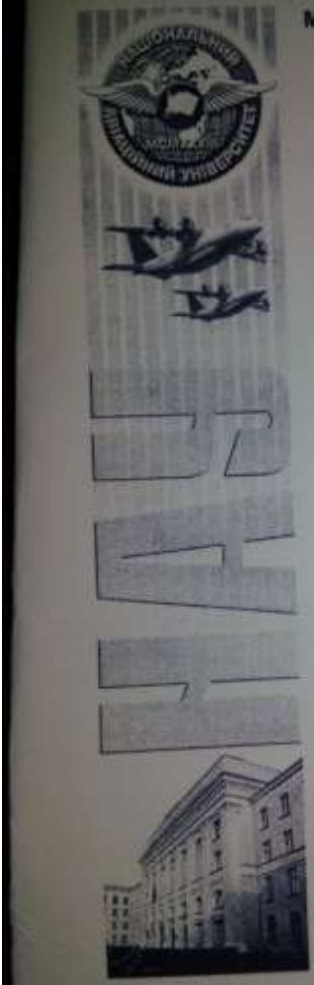
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет



НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Методичні рекомендації до виконання домашнього завдання для студентів напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

VIVERE!
VINCERE!
CREARE!

Київ 2015

УДК [002:004.056.5]:340.11 (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.С.Ільєнко*

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

Нормативно-правове забезпечення інформаційної безпеки: методичні вказівки до виконання домашнього завдання/ уклад.: О.К.Юдін, М.Г. Луцький, А.В.Чунарьова, О.Л.Яковенко. – К.: НАУ, 2014. – 20 с.

Містить методичні рекомендації до виконання домашнього завдання.

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

Зміст

Вступ

Методичні вказівки з дисципліни «Нормативно-правове забезпечення інформаційною безпекою», є складовою частиною професійної підготовки фахівців за напрямом 6.170101 «Безпека інформаційних і комунікаційних систем» – навчальний посібник для виконання домашнього завдання з цієї дисципліни.

Домашнє завдання — це засіб, передбачений навчальним планом як складова підготовки студентів до складання диференційного заліку. Основна мета домашнього завдання — закріпити знання, здобуті студентами під час аудиторних занять, а також самостійно опанувати теоретичні питання з фахових дисциплін та набути навичок практичного застосування знань під час розв'язання конкретних завдань. Домашнє завдання виконується з метою закріплення, поглиблення та узагальнення теоретичних знань, набутих студентами під час вивчення дисципліни, розвитку навичок їх практичного застосування, самостійного та комплексного розв'язання конкретних фахових завдань с сфері інформаційної безпеки та методів її забезпечення. Робота має також за мету навчити користуватися національними стандартами та нормативними документами, та іншими матеріалами, які фахівець використовує під час своєї професійної діяльності в сфері забезпечення захисту інформації.

Основним завданням домашнього завдання є вивчення теоретичних та практичних основ розробки технічного завдання на створення комплексних систем захисту інформації в автоматизованих системах організацій та установ на базі національних нормативних документів та стандартів.

Знання та вміння, здобуті під час вивчення цієї дисципліни, будуть використані як базові для опанування переважної більшості дисциплін професійної та практичної підготовки фахівців напряму 6.170101 «Безпека інформаційних і комунікаційних систем», серед яких «Безпека інформаційно-комунікаційні системи та мережі», «Теорія інформації та кодування», «Технології програмування», «Прикладна криптографія», «Захист програмного забезпечення», «Комплексні системи захисту інформації», «Організаційне забезпечення захисту інформації», «Управління інформаційною безпекою».

Мета та завдання домашнього завдання

Мета домашнього завдання – розробка технічного завдання щодо створення комплексної системи захисту інформації автоматизованої системи (АС) на базі національних стандартів та нормативних документів.

Завдання домашнього завдання:

1. розробка плану захисту інформаційної системи;
2. визначення завдання захисту інформації в АС;
3. визначення класу АС;
4. проведення класифікації інформації, що обробляється в АС;
5. опис компонентів АС та технології обробки інформації;
6. розробка структурно-логічної схеми автоматизованої системи;
7. опис загальної характеристики АС установи і умов її функціонування;
8. побудова моделі загроз інформації в АС;
9. побудова моделі порушника щодо інформації в АС;
10. розробка політики безпеки інформації в АС.

Завдання на виконання домашнього завдання

Комплексні системи захисту інформації (КСЗІ) в автоматизованих системах організацій та установ повинні створюватися згідно до вимог національних стандартів та нормативних документів [8-15].

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі. Встановлений порядок є обов'язковим для всіх суб'єктів системи технічного захисту інформації (ТЗІ) в Україні незалежно від їхньої організаційно-правової форми та форми власності, в АС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в АС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати, як рекомендації. Порядок створення КСЗІ в АС розглядається, як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт.

Студентам належить на основі наданого індивідуального завдання розробити ТЗ на КСЗІ. В загальному технічне завдання на КСЗІ повинно містити такі основні підрозділи:

1. загальні відомості;
2. мета і призначення комплексної системи захисту інформації;
3. загальна характеристика автоматизованої системи та умов її функціонування;
4. вимоги до комплексної системи захисту інформації.

Далі викладемо основні вимоги до розділів технічного завдання на КСЗІ, які повинні бути враховані в домашньому завданні.

1. Підрозділ «Загальні відомості»

В підрозділі зазначають:

– повне найменування КСЗІ та її умовне позначення;

– шифр теми і реквізити договору;

– найменування підприємств-розробників і замовника (користувача) КСЗІ та їх реквізити;

– перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи;

– планові терміни початку і закінчення роботи із створення КСЗІ;

– відомості про джерела і порядок фінансування робіт;

– порядок оформлення і подання замовнику результатів робіт із створення КСЗІ, з виготовлення і налагодження окремих засобів (технічних, програмних, інформаційних) і програмно-технічних (програмно-методичних) комплексів системи.

2. Підрозділ «Мета і призначення комплексної системи захисту інформації»

Вказується мета розробки КСЗІ в АС, функціональне призначення і особливості застосування. Необхідно зазначати, на підставі яких нормативно-правових актів, інших нормативних документів регламентується порядок захисту інформації в АС.

3. Підрозділ «Загальна характеристика автоматизованої системи і умов її функціонування»

В підрозділі рекомендується зазначити такі моменти, які впливають на безпеку інформації під час її оброблення в АС та на загальні вимоги до реалізації системи захисту інформації (СЗІ):

– загальну структурну схему і склад операційного середовища (О)С АС, а саме перелік і склад устаткування, технічних і програмних засобів, їх зв'язки, особливості конфігурації і архітектури, особливості підключення до локальних або глобальних мереж тощо;

– технічні характеристики каналів зв'язку, а саме пропускну спроможність, типи кабельних ліній, види зв'язку з віддаленими сегментами АС і користувачами і т. ін.;

– характеристики інформації, що обробляється, а саме категорії інформації, вищий гриф секретності і т. ін.;

– характеристики персоналу, а саме кількість користувачів і категорій користувачів, форми допуску тощо;

– характеристики фізичного середовища, а саме наявність категорованих приміщень, територіальне розміщення компонентів АС, їх фізичні параметри, вплив на них чинників навколишнього середовища, захищеність від засобів технічної розвідки і т.п.;

– загальну технічну характеристику АС, а саме обсяги

основних інформаційних масивів і потоків, швидкість обміну інформацією і продуктивність системи під час розв'язання функціональних завдань, тривалість процедури підготовки АС до роботи після подачі живлення на її компоненти, тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності і живучості і т. ін.;

– особливості функціонування АС, а саме надання машинного часу або устаткування в оренду стороннім організаціям, цілодобовий режим роботи без відключення живлення тощо;

– особливості реалізованих або припустимих заходів організаційних, фізичних та інших заходів захисту саме режимні заходи в приміщеннях і на території, охорона, сигналізація, протипожежна охорона і т. ін.;

– інші чинники, що впливають на безпеку оброблюваної інформації;

– потенційні загрози інформації, а саме способи здійснення НСД, можливі технічні канали витоку інформації і умови їх формування, стихійні лиха і т. ін., а також можливі наслідки їх реалізації;

– клас АС згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу».

4. Підрозділ «Вимоги до комплексної системи захисту інформації»

4.1. Підрозділ «Вимоги до комплексної системи захисту інформації в АС в частині захисту від несанкціонованого доступу»

Вимоги до комплексної системи захисту інформації в АС в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу». Згідно з цим документом в процесі оцінки захищеності АС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій. Відповідно, в ТЗ на КСЗІ повинні бути зазначені вимоги обох видів.

Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Повинен бути вказаний рівень гарантій, що передбачається досягти.

Опису послуг має передувати опис політики безпеки інформації, яку повинен реалізувати комплекс засобів захисту ОС АС.

Опис політики безпеки має включати в себе опис:

– об'єктів (елементів ресурсів) ОС;

– принципів керування доступом користувачів до інформації (довірче і/або адміністративне керування доступом);

– правил розмежування інформаційних потоків;

– правил маркірування носіїв інформації;

– основних атрибутів доступу користувачів, процесів і пасивних об'єктів;

– правил розмежування доступу користувачів і процесів до пасивних об'єктів;

– правил адміністрування КЗЗ і реєстрації дій користувачів;

– інші загальні моменти політики безпеки, які вважає за потрібне описати розробник ТЗ.

Вимоги до послуг безпеки мають бути викладені і згруповані в тому порядку і стилі, в якому вони подані в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу». В розділі мають бути викладені вимоги до реалізації послуг забезпечення: конфіденційності, цілісності, доступності, спостереженості.

Для кожної включеної до розділу послуги має бути визначений рівень послуги, який передбачається реалізувати. Має бути описана політика даної послуги: визначення об'єктів, до яких застосовується дана послуга, і правил (в тому числі, що застосовуються за замовчуванням), відповідно до яких повинні функціонувати механізми, що реалізують послугу. Відповідно до особливостей розроблюваної АС мають бути конкретизовані всі

вимоги, що викладені в Критеріях для відповідного рівня кожної послуги. У разі, якщо передбачається реалізувати послуги безпеки, їх також необхідно описати, дотримуючись, по можливості, стилю, прийнятого для опису інших послуг.

Вимоги до гарантій також мають бути викладені і згруповані в тому порядку і стилі, як вони подані в Критеріях. Це передбачає включення вимог:

– до архітектури КЗЗ (додатково до загальних вимог до архітектури на даному етапі бажано визначити основні модулі (підсистеми), з яких повинен складатися КЗЗ);

– до середовища розробки (організації процесу розробки і системи керування конфігурацією);

– до гарантій проектування (етапності розробки і проектної документації);

– до середовища функціонування;

– до експлуатаційної документації;

– до випробувань комплексу засобів захисту.

Всі вимоги повинні відповідати належному рівню гарантій.

Функціональний профіль захищеності заданий студентам в індивідуальному завданні.

4.2. Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами

Мають бути сформульовані загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера АС і т. ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами.

Мають бути вказані вимоги до розмірів зони безпеки інформації, необхідні величини показників захищеності, що враховують реальний рівень завадостійкості системи.

Далі наведемо приклади окремих фрагментів ТЗ на КСЗІ.

– оформлення загальних відомостей ТЗ (приклад 1);

– вихідні дані для розроблення та оформлення технічного завдання на створення комплексу ТЗІ (приклад 2);

– загальна характеристика та вимоги до КЗЗ АС 02 (приклад 3).

Приклад 1. ***Приклад оформлення загальних відомостей ТЗ.***

1. Найменування КЗЗ і його умовне позначення.

Комплекс засобів захисту інформації автоматизованої системи класу 2 (далі — КЗЗ АС 02).

2. Шифр ТЗ.

Шифр: «КЗЗ АС 02».

3. Найменування замовника та його реквізити.

Замовник: Інститут комп'ютерних інформаційних технологій.

Юридична адреса: м. Київ, просп. Космонавта Комарова, 1.

4. Найменування виконавця та його реквізити.

Виконавець: Інститут новітніх технологій.

Юридична адреса: м. Київ, просп. Космонавта Комарова, 1.

5. Відомості про джерела й порядок фінансування робіт.

Фінансування робіт проводиться безкоштовно згідно з договором Замовника та Організатора.

6. Порядок оформлення й подання результатів робіт.

Роботи з розроблення КЗЗ АС 02 вважаються завершеними за умови впровадження системи, атестації та отримання позитивного експертного висновку на КЗЗ АС 02 [15].

Приклад 2. ***Вихідні дані для розроблення та оформлення технічного завдання на створення комплексу ТЗІ.***

1. Характеристика автоматизованої системи.

Згідно з НД ТЗІ 2.5-005-99 АС 02 належить до АС класу «2». До складу апаратного забезпечення АС 02 входить: 15 персональних комп'ютерів; 3 сервери : поштовий, файловий, баз даних; свіч; міжмережевий екран (до складу пристроїв можуть висуватися відокремлені вимоги та стандарти, наприклад — взаємодія та конфігурування серверного простору, їх опис тощо).

До складу програмного забезпечення АС 02 входить: операційна система Unix, засіб антивірусного захисту робочих станцій "Eset NOD 4.0", спеціалізований програмний комплекс «Діловодство та документообіг v.5» АС 02. Операційна система Unix, спеціалізований програмний комплекс «Діловодство та

документообіг v.5», засіб антивірусного захисту “Eset NOD4.0” для робочих станцій (РС), повинні мати чинний позитивний експертний висновок Держспецзв’язку України.

2. Характеристика фізичного середовища.

Розробник повинен розробити і впровадити документовані методики з керування конфігурацією комплексу засобів захисту на всіх стадіях життєвого циклу АС. Система управління конфігурацією має забезпечувати управління внесенням змін у програмне забезпечення і документацію.

Програмні засоби слід розробляти з використанням будь-якого із сучасних засобів розробки прикладних програм для середовища операційної системи платформи Unix, в якому використовується добре визначена документована мова програмування.

Керування конфігурацією повинно здійснюватись на основі базових версій, наприклад, версія КЗЗ, яка може бути змінена тільки через формальні процедури зміни.

Елементами КЗЗ, конфігурація яких підлягає керуванню, є програмні засоби, що входять до складу КЗЗ, настройки КЗЗ та документація.

Зміни в елементи конфігурації слід вносити на основі узгоджених організаційних документів у результаті приймання етапів робіт зі створення КСЗІ, проведення випробувань та дослідної експлуатації.

Технічні засоби АС 02 розміщуються у трьох приміщеннях, які знаходяться в межах контрольованої зони та мають пропускний режим згідно зі встановленою системою пропусків та кодів на охоронну систему приміщень.

3. Базові загрози безпеки інформації. Перелік базових потенційних загроз з врахуванням порушення властивостей інформації (К – конфіденційність; Ц – цілісність; Д – доступність; С – спостережуваність) викладений в табл. 1.

4. Характеристика інформації, що обробляється в АС 02.

Інформація, яка обробляється в АС 02, є власністю *Інституту комп’ютерних інформаційних технологій* та поділяється на такі групи:

– технологічна та ключова інформація, до яких висуваються вимоги із забезпечення конфіденційності та цілісності — конфіденційна інформація;

– інформація загального користування — відкрита інформація.

Таблиця 1

Базові потенційні загрози

№ з/п	Потенційні загрози інформації	Наслідки (порушення властивостей інформації)			
		К	Ц	Д	С
1. Загрози об'єктивної природи					
1.1	Стихійні явища (пожежа, аварії)		+	+	
2. Загрози суб'єктивної природи					
2.2	Несанкціоноване перехоплення інформації	+	+	+	+
2.3	Порушення нормальних режимів роботи АС 02		+	+	+
3. Зовнішні загрози		+	+	+	+
3.1	Несанкціоноване перехоплення інформації за рахунок витоку інформації та побічного електромагнітного випромінювання та наведень	+			
3.2	Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу	+			

5. Характеристики середовища користувачів.

За рівнем повноважень доступу до інформації співробітники та користувачі, що мають доступ до інформаційних ресурсів системи, підрозділяються на такі категорії: АБ — адміністратор безпеки; АС — системний адміністратор; АД — адміністратор баз даних; ОП — оператор; КС — користувач системи [15].

Приклад 3. ***Загальна характеристика та вимоги до комплексу засобів захисту (КЗЗ) АС 02.***

Мета створення КЗЗ АС 02

Метою створення КЗЗ АС 02 є виявлення та протидія загрозам безпеці інформації з обмеженим доступом (ІзОД), що обробляється та зберігається в автоматизованій інформаційній системі КЗЗ АС 02 повинна створюватися відповідно до вимог із захисту інформації від НСД та технічного захисту інформації. КЗЗ

АС 02 є комплексом програмних і технічних засобів та організаційних заходів (рис. 1).

1. Призначення КЗЗ АС 02.

1.1. Функції КЗЗ АС 02.

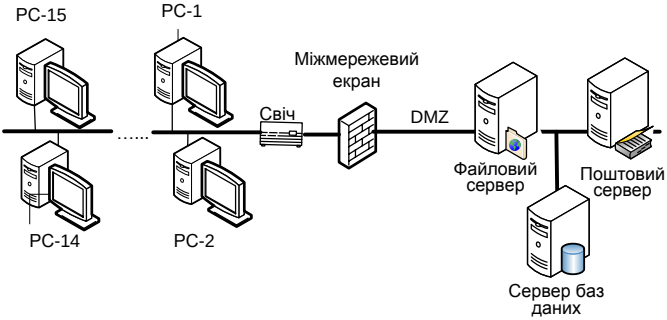


Рис. 1. Функціональна схема АС 02

КЗЗ АС 02 повинна забезпечувати виконання таких функцій:

— розмежування та контроль доступу до інформаційних ресурсів системи користувачів, операторів, адміністраторів та адміністраторів безпеки АС;

— реєстрацію даних про події та інциденти, що відбуваються в системі і мають відношення до безпеки інформації;

— забезпечення цілісності та унеможливлення несанкціонованої модифікації інформаційних ресурсів за умов реалізації процесів стандартного, спеціалізованого та прикладного ПЗ;

— тощо.

1.2. Вимоги до складу КЗЗ АС 02.

КЗЗ складається з комплексу технічних засобів (КТЗ) та програмного стандартного (штатного) і спеціалізованого програмного забезпечення.

Склад ПЗ АС 02:

– штатна операційна система платформи Unix (має позитивний експертний висновок);

– засоби антивірусного захисту для робочих місць “Eset NOD 4.0” (ліцензована та має позитивний експертний висновок);

– спеціалізований програмний комплекс «Діловодство та документообіг v.5» (має позитивний експертний висновок).

– тощо.

1.3. Вимоги та функції складових КЗЗ АС 02.

Штатний КЗЗ операційної системи повинен реалізовувати такі функції:

— авторизоване розмежування та контроль доступу до інформаційних ресурсів системи користувачів, операторів, адміністраторів та адміністраторів безпеки АС;

— реєстрацію даних про події та інциденти, що відбуваються в системі і мають відношення до безпеки інформації;

— виявлення уразливостей в АС 02 та її процесах;

— тощо.

Спеціалізований програмний комплекс «Діловодство та документообіг» реалізує такі функції:

— розмежування та контроль доступу до інформаційних ресурсів програмного комплексу «Діловодство та документообіг»;

— реєстрацію даних про події та інциденти при організації і проведенні робіт з автоматизованою системою діловодства та документообігу;

— організацію та контроль баз даних при організації і проведенні робіт з автоматизованого діловодства та документообігу;

— тощо.

1.4. Вимоги та функції засобів антивірусного захисту.

Засоби антивірусного захисту повинні реалізовувати такі функції:

– захист файлової системи, додатків, утилітів;

– захист штатного ПЗ платформи Unix;

– захист спеціалізованого ПЗ;

– ведення журналу аудиту антивірусного захисту серверного простору та робочих станцій;

– тощо.

1.5. Вимоги та функції КЗЗ оператора АС 02.

Вимоги до оператора АС 02: наявність диплому про вищу освіту за фахом та сертифікати про підвищення кваліфікації по роботі з антивірусним ПЗ “Eset NOD 4.0”.

Функції оператора КЗЗ а АС 02:

– ідентифікація та автентифікація користувачів, операторів АС 02;

– реєстрація даних про події та інциденти, які відбулися

відносно до КЗЗ;

– унеможливлення несанкціонованого доступу до інформаційних ресурсів КЗЗ;

– тощо.

1.6. Вимоги та функції КЗЗ системного адміністратора АС 02.

Вимоги до адміністратора АС 02: наявність диплому про вищу освіту за фахом, сертифікати про підвищення кваліфікації по роботі зі штатним ПЗ платформи Unix та антивірусним ПЗ "Eset NOD 4.0".

Системний адміністратор КЗЗ АС 02 повинен реалізовувати такі функції:

– автоматизоване розмежування та контроль доступу до інформаційних ресурсів АС 02;

– реєстрація інцидентів, що мають відношення до безпеки інформації;

– захист інформаційних ресурсів програмного забезпечення КЗЗ;

1.7. Вимоги та функції КЗЗ адміністратора баз даних АС 02.

Вимоги до адміністратора баз даних АС 02: наявність диплому про вищу освіту за фахом, сертифікати про підвищення кваліфікації по роботі зі спеціальним та прикладним ПЗ (SQL, Java тощо), антивірусним ПЗ "Eset NOD 4.0".

Адміністратор баз даних КЗЗ АС 02 повинен реалізовувати такі функції:

– контроль цілісності баз даних та знань та їх каталогів;

– управління доступом до баз даних та знань;

– резервне копіювання баз даних та її відновлення з резервної копії;

– введення журналу аудиту доступу до баз даних;

1.8. Опис політики безпеки інформації, що повинен реалізувати КЗЗ АС 02.

Відповідно до функціонального призначення, місця розміщення і виду подання програмно-інформаційні ресурси можна поділити на види, що наведені в табл. 2.

1.8.1. Вимоги до адміністратора безпеки АС 02.

На адміністратора безпеки покладається виконання таких функцій:

– загальне адміністрування системою захисту, повний

контроль списків доступу згідно зі встановленою політикою безпеки;

Таблиця 2.

Програмно-інформаційні ресурси КЗЗ АС 02

Умовне позначення	Найменування ресурсу	Ступінь обмеження доступу
{СПЗ01_КЗЗ}	Інформація про спеціалізоване ПЗ, яке використовується адміністратором безпеки АС 02	Відкритий
{І_ЖР}	Інформація журналів реєстрації подій та інцидентів	Конфіденційний
{К_ВІ}	Каталоги різних форматів, які містять відкриту інформацію	Відкритий
{ІД}	Особисті ключі та ідентифікатори персоналу АС 02	Конфіденційний

– адміністрування системи доступу до інформації з РС або віддалено;

– налаштування і моніторинг процесів і ресурсів операційної системи Unix.

Адміністратор безпеки повинен мати можливість контролювати всі пов’язані з безпекою події, оперативно коригувати список контрольованих подій безпеки, переглядати їх та заносити в архів. Права доступу визначають правомірність виконання користувачем конкретних дій з ресурсами (табл. 3).

Кожен співробітник категорії ОП АС 02 повинен мати право запускати лише робочу станцію оператора АС 02 і обробляти інформацію лише із застосуванням функцій, що надаються оператору АС 02. Співробітники категорії ОП АС 02 не повинні мати можливість інсталювати, налагоджувати, активізувати виконання або модифікувати стандартне та спеціальне ПЗ.

Програмно-апаратні засоби захисту, які входять до складу КЗЗ АС 02, повинні мати відповідним чином оформлені документи:

ліцензії, експертні висновки, сертифікати, допуски до експлуатації тощо.

Таблиця 3

Таблиця розподілу прав доступу співробітників до інформаційних ресурсів КЗЗ АС 02

Співробітник	Читання	Модифікація	Створення	Видалення
АБ	{ТІ_КЗЗ} {СПЗ01_ КЗЗ} {І_ЖР}	{К_ВІ}	{К_ВІ}	{К_ВІ}
ОП	{СПЗ01_ КЗЗ} {К_ВІ} {ІД}	{К_ВІ}	{К_ВІ}	{К_ВІ}

2. Вимоги до реалізації послуг безпеки в частині захисту від НСД.

Визначення функціонального профілю захищеності і рівня гарантій.

КЗЗ АС 02 має забезпечувати реалізацію такого функціонального профілю захищеності інформації, як:

{КА-1, ЦА-2, ДР-2, ДВ-2, НР-2, НИ-3, НО-2, НЦ-2, Г-2}.

Семантику наведеного профілю обрано відповідно до НД ТЗІ 2.5-004-99.

2.1. Вимоги до реалізації послуг забезпечення конфіденційності.

Мінімальна адміністративна конфіденційність (КА-1)

Політика мінімальної адміністративної конфіденційності належить до таких об'єктів: {ТІ_КЗЗ}, {СПЗ01_КЗЗ}. Права доступу до {ТІ_КЗЗ}, {СПЗ01_КЗЗ} повинні встановлюватися в момент їх ініціалізації. КЗЗ має здійснювати керування доступом до {ТІ_КЗЗ} на підставі атрибутів доступу користувачів. КЗЗ повинен надавати можливість АБ визначати конкретних користувачів і/або групи користувачів, які можуть мати доступ до

{СПЗ01_КЗЗ}.

2.2. Вимоги до реалізації послуг забезпечення цілісності.

Базова адміністративна цілісність (ЦА-2)

Політика базової адміністративної цілісності стосується користувачів АС 02 всіх категорій таких об'єктів, як: {СПЗ01_КЗЗ}.

КЗЗ має надавати ОП можливість працювати тільки за допомогою призначеного для цього програмного забезпечення. Доступ до має надаватися КЗЗ лише для ОП на підставі його атрибутів доступу. Доступ до {СПЗ01_КЗЗ} повинен надаватися КЗЗ лише для АБ та АС на підставі їх атрибутів доступу.

2.3. Вимоги до реалізації послуг забезпечення доступності.

Квоти (ДР-2)

Політика послуги стосується користувачів усіх категорій, обсягів ресурсів, що їм необхідні для обробки інформації, а також файлів із системним та спеціальним програмним забезпеченням.

До функцій системного адміністратора входять: інсталяція і налаштування ОС Unix, інсталяція і налаштування засобів антивірусного захисту, інсталяція і налаштування ПК, періодичне оновлення антивірусних баз.

До функцій адміністратора безпеки входять: реєстрація, модифікація і видалення облікових записів, додавання і видалення сертифікатів із файлового сховища та списків відкликаних сертифікатів, перегляд, резервне копіювання і відновлення з резервної копії баз даних захисту [15].

Склад, обсяг і структура домашнього завдання

Робота оформляється у вигляді звіту на аркушах формату А4. Звіт щодо виконання домашнього завдання повинен виконуватися засобами MS Word та містити наступні розділи:

1. титульний аркуш;
2. зміст;
3. вступ;
4. основна частина;
5. заключна частина;
6. список використаної літератури.

Текст набирається шрифтом Times New Roman, 12 пт., міжрядковий інтервал – 1,5; інтервал - 0 пт.; абзацний відступ 1,25 см; вирівнювання за шириною; заголовки 14 пт., напівжирний, вирівнювання за центром. У верхньому колонтитулі вказати прізвище та ініціали студента; у нижньому ліворуч – № варіанту, праворуч – № сторінки.

Загальна кількість сторінок звіту щодо виконання домашнього завдання – 20-25 стр.

Порядок вибору варіанту: номер варіанта домашнього завдання відповідає порядковому номеру студента в навчальній групі.

Методичні рекомендації до розділів домашнього завдання

Пояснювальна записка включає зміст, вступ та розділи, які є необхідними для повного розкриття виконаного домашнього завдання.

У *вступі* (1 – 2 сторінки) коротко викладається зміст задачі, вирішенню якої присвячене домашнє завдання.

У *основній частині* спочатку стисло викладається теоретичний матеріал, який висвітлює основи розробки ТЗ на КСЗІ згідно національних стандартів та нормативних документів. Після викладення теоретичного матеріалу проводиться розробка ТЗ відповідно до варіанту та повинно містити такі основні підрозділи: 1) загальні відомості АС; 2) мета і призначення КСЗІ в АС; 3) загальна характеристика АС та умов її функціонування; 4) вимоги до комплексної системи захисту інформації.

У *заключній частині* повинні бути викладені основні висновки та результати власних досліджень.

Порядок захисту роботи

Кожен студент в обов'язковому порядку захищає контрольну роботу відповідно до термінів згідно графіку самостійної роботи студента.

Вчасне подання роботи на кафедру відповідно до встановленого терміну, розкриття змісту завдання відповідно до встановлених вимог та відповідність друкованого звіту домашнього завдання умовам оформлення враховується при оцінюванні виконання та захисту роботи.

Студенти, що матимуть звіти, однакові за змістовною частиною, до захисту роботи допускатися не будуть.

Список джерел

1. *Захист* інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. — [Чинний від 1996.10.10]. — К. : Держстандарт України, 1996. — 20 с.

2. *Захист* інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. — [Чинний від 1997.07.01]. — К. : Держстандарт України, 1997. — 32 с.

3. *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.

4. *Про інформацію*: Закон України від 02.10.1995 № 2658-XII-ВР//ВВР. —1992. — № 48. — С. 651.

5. *Про захист* інформації в автоматизованих системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.

6. *Про захист* інформації в інформаційно-телекомунікаційних сис-темах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.

7. *Положення* про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 № 1229/99. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/1229/99.

8. *Термінологія* в галузі захисту інформації в комп'ютерних сис-темах 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).

9. *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).

10. *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).

11. *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).

12. *Класифікація* автоматизованих систем і стандартні функціо-нальні 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).

13. *Методичні* вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

14. *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).

15. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

Навчальне видання

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Методичні вказівки до виконання домашнього завдання
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 _____