МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ
УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

О.А. БАЛТОВСЬКИЙ
В.Г. ПЯДИШЕВ
А.В. ФОРОС

Навчально-методичні рекомендації до вивчення навчальної дисципліни

БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ

Розроблено для підготовки фахівців освітнього ступеня «магістр» освітньо-професійної програми « Кримінальний аналіз» спеціальність 124 «Системний аналіз»

м. Одеса 2024

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА КРИМІНАЛЬНОГО АНАЛІЗУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

О.А. БАЛТОВСЬКИЙ, А.В. ФОРОС, В.Г. ПЯДИШЕВ

Навчально-методичні рекомендації до вивчення навчальної дисципліни

«БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ»

Розроблено для підготовки фахівців освітнього ступеня «магістр»
освітньо-професійної програми «Кримінальний аналіз»
спеціальність 124 «Системний аналіз»

2024 рік

Схвалено та рекомендовано до друку кафедри кримінального аналізу та інформаційних технологій.
Протокол № 3 від 30 вересня 2024 року

Авторський колектив:
Балтовський О.О. – доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій ОДУВС;
Форос Г.В. – кандидат юридичних наук, доцент, завідувачка кафедри кримінального аналізу та інформаційних технологій ОДУВС;
Пядишев В.Г. – доктор юридичних наук, професор, професор кафедри кримінального аналізу та інформаційних технологій ОДУВС

Безпека технічних систем: навчально-методичні матеріали / уклад. О.А. Балтовський, А.В. Форос, В.Г. Пядишев. — Одеса: ОДУВС, 2024. — 36с.

Навчально-методичні рекомендації створено для забезпечення системного підходу до вивчення дисципліни «Безпека технічних систем». Матеріал охоплює ключові аспекти організації захисту інформації в технічних системах, які є невід'ємною складовою сучасного суспільства. Розроблені матеріали, спрямовані на формування знань і навичок аналізу, оцінювання та протидії загрозам, які виникають в процесі експлуатації технічних систем.

Розглядаються поняття інформаційних ресурсів, їх значення у забезпеченні економічної, соціальної та технічної стабільності. Значна увага приділяється характеристикам властивостей інформації та сучасним підходам до її обробки, зберігання та використання.

Навчально-методичні рекомендації сприяють розвитку у здобувачів вищої освіти критичного мислення, системного аналізу технічних загроз та практичних навичок у галузі інформаційної безпеки. Матеріал адаптовано для використання як у рамках лекційних та практичних занять, так і для самостійної роботи здобувачів вищої освіти.

ЗМІСТ

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Метою викладання дисципліни є формування теоретичних знань та практичних навичок, необхідних для створення умов, що запобігають розголошенню, витоку і неправомірному оволодінню конфіденційною інформацією у технічних системах (ТС), а також запобігають протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.

Задачі вивчення дисципліни полягають у тому, щоб ознайомити слухачів із законодавчим, адміністративним, організаційним і інженерно-технічним рівнями забезпечення захисту ТС, особливостями криптографічного і стеганографічного захисту, навчити їх реалізовувати практично правила політики безпеки.

В результаті вивчення дисципліни магістр повинен:

Знати:

– основні концептуальні положення системи захисту ТС;

– класифікацію загроз конфіденційній інформації;

– умови, що сприяють неправомірному оволодінню конфіденційною інформацією;

– особливості законодавчого рівня забезпечення інформаційної безпеки у ТС:

– особливості адміністративних методів захисту інформації у ТС;

– особливості організаційних заходів щодо захисту інформації у ТС;

– особливості інженерно-технічного рівня захисту інформації у ТС;

– основні поняття криптографічного і стеганографічного захисту інформації у ТС;

– зміст правил автентифікації інформації і користувачів у ТС;

– правила захисту від шкідливого програмного забезпечення у ТС;

Уміти:

– визначати загрози конфіденційній інформації;

– застосовувати положення правових актів для забезпечення інформаційної безпеки ТС;

– розробляти основні положення політики безпеки і програму її реалізації;

– реєструвати порушення режиму безпеки і складати звіти;

– створювати захист інформації за допомогою паролів, а також криптографічний і стеганографічний захист;

– захищати ТС від шкідливого програмного забезпечення;

– користуватись науковою та довідковою літературою за напрямком дисципліни;

знаходити раціональні методи розв'язання практичних задач.

Перелік компетентностей, формування яких забезпечує вивчення навчальної дисципліни (з ОПП).

Загальні компетентності: ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК5. Здатність розробляти проекти та управляти ними.

Спеціальні компетентності: СК1. Здатність інтегрувати знання та здійснювати системні дослідження, застосовувати методи математичного та

інформаційного моделювання складних систем та процесів різної природи. СК2. Здатність проектувати архітектуру інформаційних систем. СК3. Здатність розробляти системи підтримки прийняття рішень та рекомендаційні системи. СК4. Здатність оцінювати ризики, розробляти алгоритми управління ризиками в складних системах різної природи. СК5. Здатність моделювати, прогнозувати та проектувати складні системи і процеси на основі методів та інструментальних засобів системного аналізу. СК7. Здатність управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів. СК10. Здатність до самоосвіти та професійного розвитку.

Результати навчання: РН 1 Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері системного аналізу та інформаційних технологій і є основою для оригінального мислення та проведення досліджень. РН 2 Будувати та досліджувати моделі складних систем і процесів застосовуючи методи системного аналізу, математичного, комп'ютерного та інформаційного моделювання. РН 3 Застосовувати методи розкриття невизначеностей в задачах системного аналізу, розкривати ситуаційні невизначеності та невизначеності в задачах взаємодії, протидії та конфлікту стратегій, знаходити компроміс при розкритті концептуальної невизначеності. РН 4 Розробляти та застосовувати методи, алгоритми та інструменти прогнозування розвитку складних систем і процесів різної природи. РН 6 Застосовувати методи машинного навчання та інтелектуального аналізу даних, математичний апарат нечіткої логіки, теорії ігор та розподіленого штучного інтелекту для розв'язання складних задач системного аналізу. РН 7 Розробляти інтелектуальні системи в умовах слабо структурованих даних різної природи. РН 8 Здійснювати ідентифікацію та оцінювання параметрів математичних моделей об'єктів керування. РН 9 Розробляти та застосовувати моделі, методи та алгоритми прийняття рішень в умовах конфлікту, нечіткої інформації, невизначеності та ризиків. РН 13. Розробляти та застосовувати методи, алгоритми та інструменти прогнозування кримінального аналізу при оцінки процесів різної природи.

Міждисциплінарні зв'язки: курс «Безпека технічних систем» викладається в магістратурі, тому що успішне її вивчання базується на застосуванні слухачами знань суспільних і спеціальних дисциплін («Системний аналіз та прогнозування ризиків», «Системи підтримки прийняття рішень», «Теорія та проектування інформаційних систем», «Програмні методи та засоби алгоритмізації процесів», «Інформаційна та кібернетична безпека».

2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна</td><td>заочна</td></tr>
<tr><td rowspan="2">Кількість кредитів – 3</td><td>Галузь знань 12 «Інформаційні технології»</td><td colspan="2" rowspan="2">Обов'язкова</td></tr>
<tr><td rowspan="5">Спеціальність 124 «Системний аналіз»</td></tr>
<tr><td rowspan="4">Загальна кількість годин – 90</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>-</td><td>1-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>-</td><td>1-й, 2-й</td></tr>
<tr><td rowspan="8">Освітній ступінь: магістр</td><td colspan="2">Лекції</td></tr>
<tr><td>-</td><td>6 год.</td></tr>
<tr><td colspan="2">Семінарські</td></tr>
<tr><td>-</td><td>10 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>-</td><td>74 год.</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">Залік</td></tr>
</table>

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин				
	заочна форма				
	усього	у тому числі			
		л	с	п	с.р.
1	2	3	4	5	6
Тема № 1. Інформація – найбільш цінній ресурс сучасного суспільства.	29	2	2	-	24
Тема № 2. Загроза інформації.	32	2	4	-	26
Тема № 3. Сучасна постановка завдання захисту в технічних системах.	29	2	4	-	24
Усього годин на навчальну дисципліну	90	6	10	-	74

Навчальна дисципліна «**Безпека технічних систем**» вивчається протягом двох семестрів. Тематичним планом передбачено проведення семінарських/практичних занять з усіх тем курсу. На семінарські (практичні) заняття виносяться питання, передбачені тематичним планом. Заняття

проводяться під керівництвом викладача з використанням різних форм та методів контролю знань слухачів: просте опитування, вільна дискусія, обговорення доповідей, семінарських ситуацій, самостійне створення алгоритмів обчислювальних процесів та під наглядом викладача. При підготовці слухачі повинні звернути увагу, по-перше, на ретельне конспектування лекцій; по-друге, на самостійне вивчення наукових праць, перелік яких надається в планах семінарських/практичних занять. При висвітленні питань теми дозволяється користуватись особистим конспектом для цитування наукових джерел. Наприкінці семінарського (практичного) заняття викладач оцінює виступи та самостійну практичну роботу окремих слухачів і рівень підготовки групи в цілому, визначає питання, які потребують більш глибокого вивчення під час самостійної роботи. Завершується вивчення навчальної дисципліни «Безпека технічних систем» складанням заліку, до якого допускаються ті слухачі, які активно працювали над освоєнням матеріалу курсу та не мають академічних заборгованостей.

Тематичним планом передбачено проведення семінарських занять з усіх тем курсу. На семінари виносяться питання, передбачені тематичним планом. Семінари проводяться під керівництвом викладача з використанням різних форм та методів контролю знань слухачів: просте опитування, вільна дискусія, обговорення практичних ситуацій тощо. При підготовці слухачі повинні звернути увагу, по-перше, на ретельне конспектування лекції; по-друге, новітніх законодавчих актів та наукових праць, перелік яких надається в планах семінарських занять. При висвітленні питань теми дозволяється користуватись особистим конспектом для цитування окремих положень законодавчих актів або наукових джерел. Наприкінці семінарського заняття викладач оцінює виступи окремих слухачів і рівень підготовки групи в цілому, визначає питання, які потребують більш глибокого вивчення під час самостійної роботи.

Програма навчальної дисципліни

Тема № 1. Інформація – найбільш цінній ресурс сучасного суспільства

Поняття про інформаційні революції. Інформатизація суспільства. Інформаційне суспільство. Інформаційні ресурси. Інформаційна технологія. Інформаційні процеси. Властивості інформації.

Інформація як об'єкт юридичного захисту. Основні принципи засекречування інформації. Організаційно-правове забезпечення ІБ. Визначення основних принципів віднесення відомостей, що мають конфіденційний характер, до інформації, що захищається. Визначення інформації, що захищається. Основні принципи засекречування інформації.

Можливі шляхи отримання конфіденційної інформації. Економічне шпигунство. Підкуп.- це найпростіший та ефективний спосіб отримання конфіденційної інформації. Впровадження "Своїх" людей до складу персоналу конкуруючої фірми. Знімання інформації з ПЕОМ багатьма способами. Спостереження. Прослуховування і підслуховування

Джерела конфіденційної інформації в інформаційних системах, виток з яких призводить до неправомірного оволодіння конфіденційною інформацією.

Розуміння безпеки ІС. Розуміння загрози безпеці інформації. Характери впливів на керовану систему: випадкові та невипадкові. Поняття про хакерів або комп'ютерних піратів. Поняття системного підходу для захисту інформації.

Семінарське заняття № 1- 2 години

Учбові питання:

1. Класифікація и зміст можливий загроза інформації.
2. Можливі шляхи отримання конфіденційної інформації.
3. Джерела конфіденційної інформації в інформаційних системах, что приводити до неправомірного оволодіння конфіденційною інформацією в інформаційних системах
4. Інформація як об'єкт юридичного захисту. Основні принципи засекречування інформації.
5. Державна система правової забезпечення захисту інформації в Україні.

Тестування по темі № 1–15 хвилин.

Методичні рекомендації

Розпочинаючи самостійну роботу з вивчення теми та підготовки до семінарського заняття, необхідно:

- ознайомитись із планом семінарського заняття, питаннями, що належать до цієї теми;
- потрібно опрацювати конспект лекції з даної теми, звернувши, при цьому при вивченні теми слід зазначити, загальні органи, що забезпечують національну безпеку, цілі, завдання, а також національні інтереси в інформаційній сфері.;
- опрацювати рекомендовану для вивчення теми літературу, законспектувати окремі положення, що стосуються питань теми, або зробити нотатки, групуючи їх за певними ознаками;
- рекомендується зробити у робочому зошиті план відповіді на кожне питання, яке виноситься на розгляд під час семінарського заняття;
- для більш глибокого вивчення теми бажано підготувати реферат на одну з наведених вище тем;
- самостійно розглянути наступні питання:

Пріоритетні напрямки в області захисту інформації, а також тенденції розвитку інформаційної політики держав і відомств. Поняття державної таємниці та правове забезпечення захисту інформації

Визначити загальнометодологічні принципи теорії інформаційної безпеки та комплексність.

Зазначити загальні етапи розвитку інформаційної безпеки, а саме системи безпеки ресурсу, етапи розвиненою захисту (поступове усвідомлення необхідності комплексування цілей захисту, розширення арсеналу використовуваних засобів захисту, стали об'єднуватися в функціональні самостійні системи захисту) та етап комплексного захисту а також вимоги до системи захисту інформації.

Зазначити показники інформації, а саме важливість, повнота,

адекватність, релевантність, толерантність.

Перерахувати методи порушення конфіденційності, цілісності та доступності інформації.

Визначити класи каналів несанкціонованого отримання інформації: 1) безпосередньо з об'єкта; 2) з каналів відображення інформації; 3) отримання по зовнішніх каналах; 4) підключення до каналів отримання інформації.

Причини порушення цілісності інформації: суб'єктивні навмисні, суб'єктивні ненавмисні, об'єктивні ненавмисні.

Завдання для самостійної роботи.

Тема №1: Інформація – найбільш цінний ресурс сучасного суспільства

Задача:

Компанія планує розробити маркетингову стратегію для нового продукту. У процесі підготовки маркетологи мають обмежений доступ до трьох типів інформації:

- Статистичні дані щодо цільової аудиторії (актуальність: висока, достовірність: середня).
- Аналітичні звіти конкурентів (актуальність: середня, достовірність: висока).
- Соціологічні опитування (актуальність: висока, достовірність: низька).

Запитування:

- Яку з цих інформаційних категорій слід вважати пріоритетною для формування стратегії?
- Обґрунтуйте свій вибір.

Питання для самостійної підготовки:

1. Види загроз.
2. Характер походження загроз.
3. Класи каналів несанкціонованого отримання інформації;
4. Джерела появи загроз.
5. Причини порушення цілісності інформації.
6. Потенційно можливі злочинні дії.
7. Визначити клас захисту інформації.

Контрольні питання:

1. Назвіть джерело організації конфіденційного документообігу ІС який призводить до інформаційної витоку.
2. Які присутні шляху отримання конфіденційної інформації?
3. Хто здійснює на підприємстві облік, реєстрацію та зберіганняконфіденційних документів?
4. Чим представлена державна система правового забезпечення захистуінформації.

Тестові завдання.

Тема №1: Інформація – найбільш цінний ресурс сучасного суспільства

1. Що є основною характеристикою інформації як ресурсу?

A. Відновлюваність

B. Актуальність

C. Постійність

D. Доступність

2. Який вид інформації є найбільш стратегічно прибутковим для компаній?

A. Відкрита інформація з публічних джерел

B. Персональні дані

C. Інтелектуальна власність

D. Статистичні дані клієнтів

3. Який ресурс найбільше впливає на розвиток інформаційного суспільства?

A. Людські ресурси

B. Технології передачі даних

C. Матеріальні ресурси

D. Природні ресурси

4. Що не є властивістю інформації?

A. Динамічність

B. Актуальність

C. Виснажуваність

D. Достовірність

5. Що є основною перевагою інформації як ресурсу?

A. Низька вартість створення

B. Можливість багаторазового використання

C. Легкість зберігання

D. Непотреба в захисті

Тема № 2. Загрози інформації

Класифікація та зміст можливих загроз інформації. Класифікація загроз безпеці інформації. Види загроз. Походження загроз. Причини виникнення загроз. Класифікація каналів витоку інформації. Канали витоку інформації 1-го класу, 2-го класу, 3-го класу, 4-го класу, 5-го класу, 6-го класу,

Види загроз інформаційнім системам. Поняття про готовність, надійність і конфіденційність системи. Класифікація загроз за природою виникнення, а також за орієнтацією. Фактори, що призводить до інформаційних втрат і до різних видів збитків. Промислове шпигунство.

Причини порушення цілісності інформації. Суб’єктивні (навмисні та ненавмисні) та об’єктивні. Класифікація каналів несанкціонованого отримання

інформації.

Види, втрати, збитки, пов'язані з інформаційнім обміном. Втрати, пов'язані з матеріальними збитками. Втрати, пов'язані з персоналом, обслуговуванням мережі і витрати на відновлення інформації, пов'язані з поновленням роботи мережі по збору, зберігання, обробки і контролю даних. Експлуатаційні втрати. Збитки, пов'язані зі зловживаннями. Інформаційні інфекції. Втрати інформації. Зміна інформації. Нещирість. Маскарад. Перехоплення інформації. Вторгнення в інформаційну систему. Прийоми проникнення. Модель порушника інформаційних систем.

Семінарське заняття № 2- 4 години

Учбові питання:

1. Сучасна постановка задачі захисту інформації.
2. Сутність, необхідність, шлях та умови переходу до інтенсивних засобів захисту інформації.
3. Класифікація каналів несанкціонованого отримання інформації.

Тестування по темі № 2–15 хвилин.

Методичні рекомендації

Розпочинаючи самостійну роботу з вивчення теми та підготовки до семінарського заняття, необхідно:

- ознайомитись із планом семінарського заняття, питаннями, що належать до цієї теми;
- потрібно опрацювати конспект лекції з даної теми, звернувши, при цьому при вивченні теми слід зазначити, загальні органи, що забезпечують національну безпеку, цілі, завдання, а також національні інтереси в інформаційній сфері.;
- опрацювати рекомендовану для вивчення теми літературу, законспектувати окремі положення, що стосуються питань теми, або зробити нотатки, групуючи їх за певними ознаками;
- рекомендується зробити у робочому зошиті план відповіді на кожне питання, яке виноситься на розгляд під час семінарського заняття;
- для більш глибокого вивчення теми бажано підготувати реферат на одну з наведених вище тем;
- самостійно розглянути наступні питання:

Потенційно можливі злочинні дій в автоматизованих системах обробки даних. Функції захисту інформації: 4 функції. Стратегії захисту інформації: оборонна стратегія, наступальна стратегія, упереджувана стратегія.

Завдання управління інформаційною безпекою. Архітектура управління інформаційною безпекою КІС. Глобальна та локальні політики безпеки. Функціонування системи управління інформаційною безпекою КІС.

Завдання для самостійної роботи.

Тема №2: Загроза інформації

Задача:

Фінансова організація отримала сигнал про можливе кібератаку на їх серверах. Відділ Фахівці відділу безпеки дали наступні загрози:

- Розширення шкідливого програмного забезпечення через корпоративну електронну пошту.
- Несанкціонований доступ до бази даних клієнтів.
- Фішингові атаки на співробітників.

Запитування:

- Яка загроза є найбільш критичною для організації?
- Які дії слід виконати для мінімізації цієї загрози?

Питання для самостійної підготовки:

1. Охарактеризуйте основні функції захисту інформації.
2. Перерахувати основні вимоги до моделі захисту.
3. Основні підходи щодо організації моделі порушника.
4. Класифікація автоматизованих систем і вимог щодо захисту інформації.

Контрольні питання:

1. Назвіть основну мету для реалізації завдання щодо захисту інформації.
2. Які присутні канали по несанкціонованому зніманню інформації.
3. Охарактеризувати причину порушення цілісності інформації.
4. Підходи для організації системи захисту інформації.
5. Які присутні стратегії захисту інформації.

Тестові завдання.

Тема №2: Загроза інформації

1. Що є основним призначенням рибальських атак?

A. Злам системи безпеки

B. Перевантаження серверів

C. Викрадання конфіденційних даних

D. Зміна структури даних

2. Який із наведених прикладів не є загрозою інформаційної безпеці?

A. Несанкціонований доступ

B. Резервне копіювання даних

C. Кіберзлочинність

D. Розповсюдження шкідливого ПЗ

3. Який тип атаки спрямований на тимчасове виведення системи з ладу?

A. DoS-атака

B. Фішинг

C. Соціальна інженерія

D. SQL-ін'єкція

4. Яка з цих загроз пов'язана з фізичним доступом до інформаційних систем?

A. Фішинг
B. Втрата обладнання
C. Вірусні атаки
D. Перехоплення даних

5. Що збільшує є причиною витоку даних?

A. Фізична крадіжка серверів
B. Людський фактор
C. Мережеві атаки
D. Недоліки програмного забезпечення

Тема № 3. Сучасна постановка завдання захисту в технічних системах

Сучасна постановка задачі захисту інформації. Поняття про комплексність захисту інформації. Поширення поняття «таємниця». Інструментальна комплексність Сучасне коло цілей захисту. Поняття «захист від інформації». Поняття про «біопотенцер».

Основні принципи засекречування інформації. Законність засекречування інформації. Обґрунтованість засекречування інформації. Своєчасність засекречування інформації. Підпорядкованість відомчих заходів по засекречування інформації загальнодержавним інтересам. Принципові аспекти розсекречення інформації/

Державна система правового забезпечення захисту інформації в Україні. Доктрина інформаційної безпеки України стосовно основних положеннь правового забезпечення захисту інформації. Роль Служби з технічного та експортного контролю України щодо загальної організація і координація робіт в країні по захисту інформації, що обробляється технічними засобами. Права СБУ (та її зовнішньої розвідки) стосовно організації захисту інформації в Україні. Роль Державної системи забезпечення інформаційної безпеки. Структура нормативної бази з питань інформаційної безпеки. Найважливіші відповідні закони України.

Сутність, необхідність, шлях та умови переходу до інтенсивних засобів захисту інформації. Протиставлення інтенсивного та екстенсивного способів. Основні положення уніфікованої концепції, практична реалізація яких означає перехід до інтенсивних способів захисту інформації. Структурований опис середовища захисту. Всебічний кількісний аналіз ступеня уразливості інформації на об'єкті. Науково обґрунтоване визначення необхідного рівня захисту. Єдина уніфікована методологія. Безперервна експертиза.

Семінарське заняття № 3- 4 години

Учбові питання:

1. Причини порушення цілісності інформації.
2. Види загроза інформаційнім системам.

3. Види втрата, збитки, пов'язані з інформаційнім обміном.
Тестування по темі № 3–15 хвилин.

Методичні рекомендації

Розпочинаючи самостійну роботу з вивчення теми та підготовки до семінарського заняття, необхідно:

- ознайомитись із планом семінарського заняття, питаннями, що належать до цієї теми;
- потрібно опрацювати конспект лекції з даної теми, звернувши, при цьому при вивченні теми слід зазначити, загальні органи, що забезпечують національну безпеку, цілі, завдання, а також національні інтереси в інформаційній сфері.;
- опрацювати рекомендовану для вивчення теми літературу, законспектувати окремі положення, що стосуються питань теми, або зробити нотатки, групуючи їх за певними ознаками;
- рекомендується зробити у робочому зошиті план відповіді на кожне питання, яке виноситься на розгляд під час семінарського заняття;
- для більш глибокого вивчення теми бажано підготувати реферат на одну з наведених вище тем;
- самостійно розглянути наступні питання:

Три методологічних підходу до оцінки вразливості інформації: емпіричний, теоретичний і теоретіко-емпіріческій. Модель витрат. Модель захисту - модель системи з повним перекриттям. Послідовність рішення задачі захисту інформації. Фундаментальних вимоги, яким повинні задовольняти ті обчислювальні системи, які використовуються для обробки конфіденційної інформації. Класифікація автоматизованих систем і вимог щодо захисту інформації. Фактори, що впливають на необхідний рівень захисту інформації. Поняття і цілі управління. Цілі управління. Планування діяльності. Контроль діяльності.

Завдання для самостійної роботи.

Тема №3: Сучасна постановка завдання захисту в технічних системах

Задача:

Підприємство використовує автоматизовану систему управління виробничими процесами. Інженери виявили такі якісь загрози:

- Перехоплення даних, що передаються між вузлами систем.
- Відмова в обслуговуванні через перезавантаження мережі.
- Несанкціонована модифікація алгоритмів управління.

Запитування:

- Яку з цих загроз слід розглядати як пріоритетну для рішення?
- Які технології захисту слід впровадити для її усунення?

Питання для самостійної підготовки:

1. Охарактеризуйте основні функції захисту інформації.
2. Перерахувати основні вимоги до моделі захисту.

3. Основні підходи щодо організації моделі порушника.

4. Класифікація автоматизованих систем і вимог щодо захисту інформації.

Контрольні питання для повторення матеріалу:

1. Назвіть основну мету для реалізації завдання щодо захисту інформації.
2. Які присутні канали по несанкціонованому зніманню інформації.
3. Охарактеризувати причину порушення цілісності інформації.
4. Підходи для організації системи захисту інформації.
5. Які присутні стратегії захисту інформації.

Тестові завдання.

Тема №3: Сучасна постановка завдання захисту в технічних системах

1. Яке основне завдання в захисті технічних систем?
A. Захист від фізичних загроз
B. Запобігання збоям у роботі апаратного забезпечення
C. Забезпечення конфіденційності, цілісності та доступності даних
D. Оптимізація енергоспоживання

2. Що з зазначеного не є сучасною технологією захисту?
A. Антивірусне програмне забезпечення
B. Двофакторна автентифікація
C. Аналогові замки для серверів
D. Системи виявлення вторгнення (IDS)

3. Що з переліченого індивідуально до превентивних заходів захисту?
A. Аналіз систем логів
B. Використання фаєрволів
C. Відновлення даних після атаки
D. Аналіз зловмисного ПЗ

4. Яке з наведених рішень забезпечує захист від перехоплення даних?
A. Шифрування
B. Резервне копіювання
C. Антивірусна перевірка
D. Додаткова система живлення

5. Що є головною перевагою багатофакторної автентифікації?
A. Зменшення вартості захисту
B. Забезпечення високого рівня конфіденційності
C. Простота у використанні
D. Автоматичне відновлення паролів

4. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Навчальним планом передбачено індивідуальне навчальне завдання для здобувачів вищої освіти денної форми навчання у вигляді мультимедійних презентацій або наукових рефератів за визначеною тематикою.

Реферати виконуються на основі самостійного вивчення рекомендованої літератури і законодавства, перелік яких не обмежує ініціативи здобувача вищої освіти і його можливостей у використанні більш широкого кола наукових досліджень. До літератури відносяться: першоджерела; підручники і навчальні посібники; наукові дослідження (монографії, наукові статті та ін.)

Тема обирається кожним здобувачем самостійно з переліку запропонованих. Обрані теми не повинні повторюватися в групі.

Представлення презентації повинно мати усне супроводження, яке базується на нормах чинного законодавства, а також спеціальної літератури. Презентація повинна бути оформлена лаконічно, відповідно до чинного законодавства, розкривати зміст обраної теми. Мінімальна кількість слайдів – 15, включаючи титульну сторінку та план. При створенні презентації необхідно використовувати схеми, таблиці, ефекти анімації тощо.

Форма педагогічного контролю – оцінювання представленої презентації або наукового реферату під час проведення семінарського заняття.

5. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

Система оцінювання передбачає накопичення 100 балів із кожної навчальної дисципліни, які перераховуються в національну шкалу та шкалу оцінювання ЄКТС.

Оцінювання результатів вивчення навчальної дисципліни у формі заліку.

Підсумковий контроль у формі заліку проводиться після проведення всіх видів занять передбачених робочою навчальною програмою відповідної освітньої компоненти.

Оцінювання здійснюється за результатами накопичених балів з аудиторної та самостійної робіт.

Результати навчання з аудиторної роботи обчислюються за таким алгоритмом:

- результат аудиторної роботи визначається, як середній бал помножений на коефіцієнт 16 та заокруглюється до цілого балу за математичними правилами (до 0,4 включно – до попереднього цілого числа, 0,5 і більше – до наступного цілого числа);

- середній бал дорівнює сумі усіх одержаних позитивних оцінок (балів) поділених на відповідну кількість, при цьому:

а. мінімальна кількість оцінок має складати не менше 1/3 (33 %) від загальної можливої кількості занять (семінарських, практичних, лабораторних) передбачених робочою навчальною програмою навчальної дисципліни. Якщо 1/3 (33 %) від кількості занять складає дробове число, то до розрахунку береться наступне ціле число;

б. якщо кількість отриманих оцінок менша за 1/3 (33 %), то кожна недостаюча оцінка враховується, як «нуль» балів;

в. кількість позитивних оцінок, які перевищують визначену мінімальнодопустиму («додаткових») враховуються з коефіцієнтом 0,5, такий коефіцієнт застосовується з метою мотивування здобувачів вищої освіти до покращення результатів оцінювання за аудиторну роботу;

г. невідпрацьовані «незадовільні» оцінки та пропущені заняття враховуються як «нуль» балів;

д. відпрацювання усіх «незадовільних» оцінок та пропущених занять не є обов'язковим.

У випадку, якщо за результатами оцінювання аудиторної роботи сума накопичувальних балів перевищує 80, то здобувачу вищої освіти нараховується максимально допустимий результат – 80 балів.

Формула розрахунку:

$$РАР = \frac{СОБ}{МКО + КДО*0,5+КНО} * 16$$

де:

- РАР – результат аудиторної роботи;
- СОБ – сума отриманих оцінок у балах;
- МКО – мінімальна кількість оцінок (1/3 (33 %) від кількості семінарських, практичних, лабораторних занять передбачених робочою навчальною програмою навчальної дисципліни). При цьому, якщо МКО складає дробове число, то до розрахунку береться наступне ціле число;
- КДО – кількість «додаткових» оцінок – оцінок, що перевищують МКО;
- КНО – кількість невідпрацьованих «незадовільних» оцінок та невідпрацьованих пропущених занять.

Загальна кількість балів за самостійну роботу визначається, як сума отриманих балів за виконання видів робіт, передбачених робочою навчальною програмою навчальної дисципліни.

Підсумкова кількість балів отриманих під час складання заліку визначається, як сума отриманих балів за аудиторну (максимум 80 балів) та самостійну роботу (максимум 20 балів.

Поточний контроль		**Підсумковий контроль (ПК)**
Аудиторна робота (РАР) (семінарські/практичні заняття та контрольні заходи)	**Самостійна робота (РСР)**	ЗАЛІК (З)
≤ 80	≤20	
≤ 100		
Підсумкова кількість балів = РАР+РСР ≤ 100		

У разі, якщо здобувач вищої освіти під час складання заліку отримав менше 60 балів – «не зараховано» він ліквідовує академічну заборгованість за

окремим графіком на вище визначених умовах.

Такий здобувач повинен покращити результати поточного контролю (відпрацювати пропущені заняття та/або незадовільні оцінки, відпрацювати тему для одержання оцінки, виконати самостійну роботу тощо) до моменту ліквідації академічної заборгованості.

У разі повторного не складання заліку ліквідація академічної заборгованості здійснюється перед комісією без врахування результатів навчання отриманих за результатами аудиторної та самостійної роботи за 100 бальною шкалою. При ліквідації академічної заборгованості перед комісією здобувач вищої освіти може одержати не більше 70 балів.

Здобувач вищої освіти, як додатковий здобуток може отримати додаткові бали, при цьому загальна сума накопичувальних балів не повинна перевищувати 100:

- за наукову роботу в межах навчальної дисципліни до 10-ти балів;
- за проходження тренінгу за тематикою навчальної дисципліни та отриманні сертифікату до 5-ти балів.

З метою підвищення поточного рейтингу успішності здобувач вищої освіти має право перескладати аудиторну та самостійну роботу відповідно до графіка, встановленого науково-педагогічним працівником до підсумкового контролю, і не більше двох пропусків та/або незадовільних оцінок з однієї навчальної дисципліни в один робочий день.

Відсутність здобувача вищої освіти на підсумковому контролі без поважної причини, прирівнюється до незадовільної оцінки. Такий здобувач вищої освіти має право скласти підсумковий контроль під час ліквідації академічної заборгованості, визначеної окремим графіком.

Здобувач вищої освіти зобов’язаний попередити деканат про свою можливу відсутність на підсумковому контролі до його початку. Здобувач вищої освіти, який був відсутній на підсумковому контролі з поважних причин, які підтверджені відповідними документами, за рішенням декана факультету (директора інституту, керівника відділу докторантури та аспірантури) може скласти пропущений підсумковий контроль у визначений час.

Здобувач вищої освіти, який за результатами поточного та підсумкового контролю сумарно накопичив менше 60-ти балів, допускається до повторного перескладання підсумкового контролю після закінчення екзаменаційної сесії, але до початку наступного семестру чи атестації.

Критерії оцінювання знань на заліку

Оцінка «відмінно»/ А – виставляється, якщо здобувач вищої освіти має глибокі і системні знання, вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями; оволодів навиками аналізу, моделювання та адекватного оцінювання ситуації; обізнаний з науковими працями вітчизняних та зарубіжних фахівців в цій галузі; матеріал викладає логічно, послідовно, переконливо і аргументовано.

Оцінка «добре»/ В,С – виставляється, якщо здобувач вищої освіти показав достатній рівень знання курсу; надав правильні, але не зовсім повні визначення термінів; засвоїв основи аналітичного методу; допускає незначні неточності в розкритті окремих теоретичних положень.

Оцінка «задовільно»/ D, E – виставляється, якщо здобувач вищої освіти в цілому засвоїв теоретичний матеріал курсу навчальної дисципліни, але декламує із деякими упущеннями при визначенні основних явищ та процесів; намагається висловити своє ставлення до проблемних питань, хоча і не зовсім аргументовано; вміє аналізувати набуті теоретичні знання і співвідносити їх з конкретними ситуаціями; викладає матеріал непослідовно, неточно, з наявними помилками.

Оцінка «незадовільно»/ FX,F – виставляється, якщо здобувач вищої освіти виявив слабкі (відсутні) знання теоретичного матеріалу навчальної дисципліни; не зміг дати визначення основних категорій та явищ; відсутні знання основних норм і визначень; матеріал викладається непослідовно, нелогічно, фрагментарно та з допущенням помилок.

Оцінка «зараховано» / A, B, C, D, E – виставляється, якщо здобувач вищої освіти виявив достатньо повні знання матеріалу навчальної дисципліни; вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями, дає правильні, хоча і не завжди повні відповіді на оставлені запитання; припускається помилок у розкритті окремих теоретичних положень, норм та визначень.

Оцінка «не зараховано»/ FX,F – виставляється, якщо здобувач вищої освіти виявив слабкі знання; не зміг дати визначення основних термінів та понять; викладає матеріал непослідовно, нелогічно, фрагментарно, неточно, стисло; відсутня переконливість у викладенні матеріалу.

Шкала оцінювання: національна та ECTS

<table>
<tr><th rowspan="2">За внутрішньоюшкалою навчального закладу в балах</th><th colspan="2" rowspan="2">За шкалою ECTS /За національною шкалою</th></tr>
<tr></tr>
<tr><td rowspan="2"></td><td colspan="2">Вноситься до відомості</td></tr>
<tr><td>екзамен</td><td>залік</td></tr>
<tr><td>90 – 100</td><td>A/Відмінно</td><td rowspan="5">A,B,C, D, E /Зараховано</td></tr>
<tr><td>82-89</td><td>B/Добре</td></tr>
<tr><td>74-81</td><td>C/Добре</td></tr>
<tr><td>64-73</td><td>D/Задовільно</td></tr>
<tr><td>60-63</td><td>E/Задовільно</td></tr>
<tr><td rowspan="2">35-59</td><td>FX/Незадовільно</td><td>Не зараховано</td></tr>
<tr><td colspan="2">З можливістю повторного складання</td></tr>
<tr><td rowspan="2">0-34</td><td>F/Незадовільно</td><td>Не зараховано</td></tr>
<tr><td colspan="2">з обов’язковим повторним курсом</td></tr>
</table>

6. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Теорія захисту інформації. Основні напрямки.
2. Забезпечення інформаційної безпеки та спрямування захисту.
3. Комплексність (цільова, інструментальна, структурна, функціональна, тимчасова).

4. Вимоги до системи захисту інформації.
5. Загрози інформації.
6. Види загроз. Основні порушення.
7. Характер походження загроз.
8. Джерела загроз. Передумови появи загроз.
9. Система захисту інформації.
10. Класи каналів несанкціонованого отримання інформації.
11. Причини порушення цілісності інформації.
12. Методи та моделі оцінки вразливості інформації.
13. Загальна модель впливу на інформацію.
14. Загальна модель процесу порушення фізичної цілісності інформації.
15. Структурована схема потенційно можливих злочинних дій вавтоматизованих системах обробки даних.
16. Методологічні підходи до оцінки вразливості інформації.
17. Модель захисту системи з повним перекриттям.
18. Рекомендації щодо використання моделей оцінки вразливостіінформації.
19. Допущення в моделях оцінки вразливості інформації.
20. Методи визначення вимог до захисту інформації.
21. Фактори, що обумовлюють конкретні вимоги до захисту, зумовлені специфікою автоматизованої обробки інформації.
22. Класифікація вимог до засобів захисту інформації.
23. Вимоги до захисту, які визначаються структурою автоматизованоїсистеми обробки даних.
24. Вимоги до захисту, обумовлюються видом інформації, щозахищається.
25. Вимоги, що обумовлюються взаємодією користувача з комплексом засобів автоматизації.
26. Аналіз існуючих методик визначення вимог до захисту інформації.
27. Стандарт США «Критерії оцінки гарантовано захищених ви- числівників систем в інтересах Міністерства оборони США». Основні положення.
28. Класи захищеності засобів обчислювальної техніки від несанкціонованого доступу.
29. Фактори, що впливають на необхідний рівень захисту інформації.
30. Функції та завдання захисту інформації.
31. Основні положення механізмів безпосереднього захисту і механізми управління механізмами безпосереднього захисту.
32. Методи формування функцій захисту.
33. Події, що виникають при формуванні функцій захисту.
34. Класи задач функцій захисту.
35. Клас задач функцій захисту 1 - зменшення ступеня розпізнаванняоб'єктів.
36. Клас задач функцій захисту 2- захист змісту обробляється, зберігається та передається інформації.
37. Клас задач функцій захисту 3 - захист інформації від інформаційноговпливу.
38. Функції захисту інформації.
39. Стратегії захисту інформації.
40. Способи та засоби захисту інформації.
41. Способи «абсолютної системи захисту».

42. Архітектура систем захисту інформації. Вимоги.
43. Загальнометодологічними принципів архітектури системи захистуінформації.
44. Побудова засобів захисту інформації.
45. Ядро системи захисту інформації.
46. Семирубежная модель захисту.
47. Основні законопроекти в галузі захисту режимів обмеженого доступу до інформації.
48. Що таке інформаційна безпека?
49. Основні принципи державної політики в галузі забезпеченняінформації.
50. Що таке інформація?
51. Що таке інформаційна війна?
52. Інформаційний канал та його складові.
53. Класифікація (загальна) каналів витоку інформації.
54. Електромагнітні канали витоку інформації.
55. Електричні канали витоку інформації. Паразитні зв'язки і наведення.
56. Пристрій прихованого знімання аудіовідеіинформації.
57. Способи та засоби енергетичного приховування акустичногосигналу.
58. Характеристики пасивних засобів несанкціонованого доступу.
59. ДП закладних пристроїв.
60. Класифікація засобів виявлення випромінювань закладних пристроїв.
61. Класифікація засобів виявлення неизлучающих закладок.
62. Апаратура радіоконтролю.
63. Категорії засобів безпеки інформації в мережах.
64. Обов'язки осіб, допущених до відомостей що становлять КТ.

ЛІТЕРАТУРА

Базова

1. Конституція України: Закон України від 28.06.1996. № 254к/96. Дата оновлення: 01.01.2020. URL:. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text . (дата звернення: 14.06.2024).

2. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650). Дата оновлення 21.03.2023. URl: https://zakononline.com.ua/documents/show/151399___591480. (дата звернення: 14.07.2024).

3. Про Національну програму інформатизації: закон України. Документ 2807-IX, чинний, поточна редакція Прийняття від 01.12.2022. Zakon.Rada.Gov.UA. Сайт. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 25.05.2023).

4. Закон України "Про захист інформації в інформаційно-комунікаційних системах" (назва із змінами, внесеними згідно із Законом України від 16.12.2020 р. N 1089-IX) (вводиться в дію з 15 червня 2022 року). Ips.Ligazakon.Net. Сайт. URL: https://ips.ligazakon.net/document/Z008000?an=1 (дата звернення: 14.06.2024).

5. Закон України «Про державну таємницю» (Відомості Верховної Ради України, 1999 р., № 49. Дата оновлення: 13 грудня 2022 року N 2849-IX URl: https://ips.ligazakon.net/document/T385500?an=1 (дата звернення: 14.06.2024).

6. Закон України «Про наукову і науково-технічну експертизу» Закон введено в дію з дня опублікування - 28 лютого 1995 року, крім статті 7, яку введено в дію з 1 липня 1995 року. Дата оновлення: 13 грудня 2022 року N 2849-IX. Ips.Ligazakon.Net Сайт. URL: https://ips.ligazakon.net/document/z950051

7. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

8. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки: Навчальний посібник. Вінниця. ВНТУ. 2018. 316 с.

9. Бурячок В. Л. , Киричок Р. В. , Складанний П. М. Основи інформаційної та кібернетичної безпеки: Навчальний посібник. Київ 2019. р. 320 с..

10. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах: Підручник. Ужгород : ПП «АУТДОР-ШАРК»,. 2021. 184 с.

11. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: НА СБ України, 2020. 256 с.

12. Герасименко В.А., Малюк А.А. Основи захисту інформації. К.: Інкомбук, 2019. 540 с.

13. Кутова М.А Основи інформаційної безпеки в системі електронного урядування. Науковий журнал «Economic Synergy», випуск 1 (11), 2024. С. 20-30.

Допоміжна:

14. Сучасні підходи щодо адаптивного автоматизованого управління складними системами в умовах невизначеності: монографія / Кокошко В.С., Ісмайлов К.Ю., Балтовський А.О., Сіфоров О.І., Пядишев В.Г., Форос Г.В. та ін. Одеса: ОДУВС, 2019. 340 с.

15. Балтовський О.А., Белека І.А., Ісмайлов К.Ю. Методика аналізу схем цифро-аналогових перетворювачів з використанням матриць гібридного типу. Вісник Інженерної академії України Кіровоградського національного технічного університету. 2019. № 3. С. 79-85.

16. Ісмайлов К.Ю., Балтовський О.А., Сіфоров О.І. Основні підходи щодо вирішення завдання оптимального календарного планування з використанням спеціалізованих алгоритмів. Електронне наукове видання «Порівняльно- аналітичне право». 2019. №2. С. 98-101.

17. Ярмакі Х.П., Музика С.С. Класифікація конфіденційної інформації. Південноукраїнський правничий часопис. 2021. № 1. С. 94-98.

18. Bearfield G. Safety of technical systems: the next 30 years. railtechnologymagazine. Feb/March 2019. Site. URL: https://www.railtechnologymagazine.com/Comment/safety-of-technical-systems-the-next-30-years

19. El-Kady A.H., Halim S., El-Halwagi M.M., Khan F. Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety and Environmental Protection. Volume 173, May 2023, P. 384-413. Site. URL: https://www.sciencedirect.com/science/article/abs/pii/S0957582023002045

Інформаційні ресурси:

1. Офіційний сайт Верховної Ради України: www.rada.gov.ua
2. Науково-дослідний центр правової інформатики: http://ippi.org.ua
3. Електронна бібліотека http://textbooks.net.ua
4. Український юридичний портал «Радник»: http://radnuk.info
5. Український інститут науково технічної інформації, сайт: http://www.uintei.kiev.ua/viewpage.php?page_id=7
6. Навчальний сайт «Інформаційні системи та технології»: http://informatic-10.at.ua/index/informacijni_sistemi_ta_tekhnologiji/0-29/
7. Експертні системи як прикладна галузь штучного інтелекту. — URL: http://uareferat.com/Експертні_системи_як_прикладна_галузь_штучного_інтелекту
8. Експертні системи та їх використання. URL: http://uareferat.com/Експертні_систми_та_їх_використання
9. Експертні системи: інформаційні технології та моделювання. URL: https://pidruchniki.com/10811007/informatika/ekspertni_sistemi
10. Модульне середовище для навчання MOODLE. Організація баз даних та знань. URL: https://msn.khnu.km.ua/course/view.php?id=5253

ГЛОСАРІЙ

Автентифікація - електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних

автоматизовані інформаційно-пошукові системи – сукупність методів і засобів, призначених для зберігання та пошуку документів, відомостей про них чи певних фактів;

автоматизовані комп'ютерні системи (АКС) – сукупність взаємопов'язаних АЕОМ, периферійного обладнання та програмного забезпечення, призначених для автоматизації прийому, зберігання, обробки, пошуку і видачі інформації споживачам;

аналітичний документ - вторинний документ, що містить узагальнену інформацію, отриману в результаті всебічного, глибокого та критичного аналізу первинних документів, аргументовану оцінку стану і тенденцій розвитку проблеми, що розвивається;

база даних - систематизована сукупність даних, що відображає стан об’єктів та їх взаємозв’язків у визначеній предметній сфері;

банк даних - система програмно-апаратних, організаційних та технічних засобів, призначених для централізованого накопичення, обробки та використання даних;

веб-сайт - сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб’єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу

виконавці завдань, проектів, робіт з інформатизації Національної програми інформатизації (далі - виконавці) - підприємства, установи, організації незалежно від форми власності, фізичні особи - підприємці, які визначаються замовниками відповідно до законодавства у сфері публічних закупівель;

дозвіл – документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;

документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

доступність – властивість інформації бути захищеною від несанкціонованого блокування;

електронна ідентифікація – процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або уповноваженого представника юридичної особи

електронні дані – будь-яка інформація в електронній формі

електронні інформаційні ресурси – систематизовані відомості і дані, створені, оброблені та збережені в електронній формі за допомогою технічних засобів та/або програмних продуктів

захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, технологічних та виробничих процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій;

інформаційна система - сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів;

інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави;

інформаційна інфраструктура – сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування;

інформаційна мережа – мережа, призначена для обробки, зберігання та передачі даних;

інформаційна продукція - матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин;

інформаційна система – автоматизована система, комп'ютерна мережа або система зв'язку;

інформаційне забезпечення - це: 1) комплекс організаційних, правових, технічних і технологічних заходів, засобів та методів, котрі забезпечують в процесі управління і функціонування системи інформаційні зв'язки та елементів (суб'єктів і об'єктів) шляхом оптимальної організації інформаційних масивів баз даних і знань; 2) діяльність, що організується в рамках управління, спрямована на проектування, функціонування та вдосконалення інформаційних систем, що забезпечують ефективне виконання задач управління; 3)органічна єдність роботи щодо визначення змісту, обсягів, якості інформації, необхідної для здійснення управління, а також заходів щодо раціональної організації процесів для здійснення управління, а також заходів щодо раціональної організації процесів збирання, систематизації, накопичення та обробки цієї інформації шляхом;

інформаційний ресурс – систематизована інформація або знання, що мають цінність у певній предметній області і можуть бути використані людиною в своїй діяльності для досягнення певної мети;

інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

кібербезпека - безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

комп'ютерна інформація – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному вигляді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися при допомозі ЕОМ (комп'ютерів);

конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;

локалізація програмних продуктів - приведення програмних продуктів у відповідність із законами та іншими нормативно-правовими актами, стандартами, нормами і правилами, передбаченими законодавством;

моделювання – це метод дослідження різних явищ і процесів, вироблення варіантів управлінських рішень;

модернізація (модифікація, розвиток) засобу інформатизації - процес продовження створення засобу інформатизації, спрямований на вдосконалення, розвиток такого засобу, зокрема, але не виключно, технічне переоснащення, покращення характеристик, розширення функціональних можливостей;

моніторинг – комплекс наукових, технічних, технологічних, організаційних та інших засобів, які забезпечують систематичний контроль (стеження) за станом та тенденціями розвитку природних, техногенних та суспільних процесів;

обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

програмний продукт – програмне забезпечення, результат комп’ютерного програмування у вигляді операційної системи, системної, прикладної, розважальної та/або навчальної комп’ютерної програми (їх компонентів), а також у вигляді інтернет-сайтів та/або онлайн-сервісів та доступу до них,

примірники (копії, екземпляри) комп'ютерних програм, їх частин, компонентів у матеріальній та/або електронній формі, у тому числі у формі коду (кодів) та/або посилань для завантаження комп'ютерної програми та/або їх частин, компонентів у формі коду (кодів) для активації комп'ютерної програми чи в іншій формі, криптографічні засоби захисту інформації;

режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації;

система активної протидії агресії у кіберпросторі – сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

система інформаційного забезпечення - це сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання таких вимог: наявності нормативно-правової бази; організаційно-кадрового забезпечення інформаційних підрозділів; організації підготовки та перепідготовки кадрів; наявності відповідних технічних, програмних та телекомунікаційних технологій; матеріально-технічного та фінансового забезпечення;

система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

Додатки

ЗАКОН УКРАЇНИ

Про захист інформації в інформаційно-телекомунікаційних системах

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: володільці інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом:

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України Л.КУЧМА м. Київ, 5 липня 1994 року N 80/94-ВР

ЗАТВЕРДЖЕНО
Указом Президента України від 27 вересня 1999 року N 1229/99

ПОЛОЖЕННЯ
про технічний захист інформації в Україні

1. Це Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій (далі - органи, щодо яких здійснюється ТЗІ).

2. Ужиті в цьому Положенні терміни мають таке значення:

конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;

цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

доступність – властивість інформації бути захищеною від несанкціонованого блокування;

технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку;

дозвіл - документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;

комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

3. Правову основу технічного захисту інформації в Україні становлять Конституція України (254к/96-ВР), закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, з питань технічного захисту інформації, а також це Положення.

4. Державна політика технічного захисту інформації формується згідно із законодавством і реалізується Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку України) у взаємодії з органами, щодо яких здійснюється ТЗІ.

5. Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їх керівників.

6. Організаційно-технічні принципи, порядок здійснення заходів з технічного захисту інформації, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації

визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Нормативно-правові акти з технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

7. Розроблення, видання нормативно-правових актів з питань технічного захисту інформації, а також роботи, пов'язані з розробленням і виконанням загальнодержавних програм розвитку системи технічного захисту інформації, здійснюються за рахунок коштів державного бюджету та інших джерел фінансування, не заборонених законодавством.

8. Суб'єктами системи технічного захисту інформації є:

Держспецзв'язку України;

органи, щодо яких здійснюється ТЗІ;

науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;

військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

11. Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

здійснення контролю за станом технічного захисту інформації.

12. Органи, щодо яких здійснюється ТЗІ, відповідно до покладених на них завдань:

створюють або визначають підрозділи, на які покладається забезпечення технічного захисту інформації та контроль за його станом, узгоджують основні завдання та функції цих підрозділів;

видають за погодженням з Адміністрацією Держспецзв'язку України та впроваджують нормативно-правові акти з питань технічного захисту інформації;

погоджують з Адміністрацією Держспецзв'язку України проведення підприємствами, установами, організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-технічної бази системи технічного захисту інформації, які здійснюються за рахунок коштів державного бюджету;

створюють або визначають за погодженням з Адміністрацією Держспецзв'язку України підприємства, установи та організації, що забезпечують технічний захист інформації;

забезпечують підготовку, перепідготовку та підвищення кваліфікації кадрів з технічного захисту інформації;

надають Адміністрації Держспецзв'язку України за його запитами відомості про стан технічного захисту інформації.

13. Основними завданнями інших суб'єктів системи технічного захисту інформації є:

дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;

створення та виробництво засобів забезпечення технічного захисту інформації;

розроблення, впровадження, супроводження комплексів технічного захисту інформації;

підвищення кваліфікації фахівців з технічного захисту інформації.

14. Суб'єкти системи технічного захисту інформації мають право співробітничати з підприємствами, установами, організаціями іноземних держав, які здійснюють аналогічну діяльність, на основі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, та інших актів законодавства України.

15. Матеріально-технічна база системи технічного захисту інформації складається з технічних засобів загального призначення та спеціальних технічних засобів.

Технічні засоби загального призначення повинні мати документ, що засвідчує їх відповідність вимогам нормативно-правових актів з технічного захисту інформації, одержаний у порядку, що встановлюється Адміністрацією Держспецзв'язку України і Державним комітетом України з питань технічного регулювання та споживчої політики.

16. Техніко-економічне обгрунтування, проектування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення інформаційних систем, зразків озброєнь, військової та спеціальної техніки, критичних і небезпечних технологій виконуються за завданнями, до яких включаються вимоги з технічного захисту інформації, якщо під час виконання передбачених завданням робіт та у процесі функціонування зазначених об'єктів, систем, зразків і технологій циркулюватиме інформація, охорона якої забезпечується державою.

Під час віднесення замовником таких робіт до особливо важливих та створення інформаційних систем державних органів завдання та результати приймання їх етапів погоджуються з Адміністрацією Держспецзв'язку України. Фінансування створення цих систем здійснюється після такого погодження.

Витрати на заходи з технічного захисту інформації включаються до кошторисної вартості робіт.

17. Під час розроблення і впровадження заходів з технічного захисту інформації використовуються засоби, дозволені Адміністрацією Держспецзв'язку України для застосування та включені до відповідних переліків.

18. Контроль у сфері технічного захисту інформації полягає в перевірці виконання вимог цього Положення, інших нормативно-правових актів з питань технічного захисту інформації та в оцінюванні захищеності інформації на об'єкті, де вона циркулюватиме або циркулює.

Оцінювання захищеності інформації здійснюється шляхом атестації або експертизи комплексів технічного захисту інформації та інспекційних

перевірок. За результатами атестації або експертизи комплексів технічного захисту інформації визначається можливість введення в експлуатацію об'єкта, де циркулюватиме інформація, охорона якої забезпечується державою.

19. Порядок експертизи та інспекційних перевірок захищеності інформації визначається відповідними нормативно-правовими актами.

20. Розроблення, впровадження, атестація та експлуатація комплексів технічного захисту інформації для власних потреб здійснюються відповідними підрозділами органів, щодо яких здійснюється ТЗІ, або військовими частинами, підприємствами, установами, організаціями, на які в установленому порядку покладено забезпечення технічного захисту інформації, за наявності у них відповідного дозволу.

До виконання цих робіт можуть бути залучені суб'єкти підприємницької діяльності, що мають відповідні ліцензії.

Результати атестації на державних об'єктах, віднесених замовником до особливо важливих, погоджуються з Адміністрацією Держспецзв'язку України.

21. Роботи з технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, здійснюються за рахунок коштів, що виділяються на їх утримання, прибутку та інших джерел, не заборонених законодавством.

Керівники зазначених органів створюють належні умови для контролю за забезпеченням технічного захисту інформації.

22. У разі порушення вимог щодо забезпечення технічного захисту інформації посадові особи та громадяни несуть відповідальність згідно із законодавством України.

Глава Адміністрації Президента України М.БІЛОБЛОЦЬКИЙ

Науково-методичне видання

О.А. БАЛТОВСЬКИЙ
В.Г. ПЯДИШЕВ
А.В. ФОРОС

Навчально-методичні рекомендації
до вивчення навчальної дисципліни

«БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ»

Розроблено для підготовки фахівців
освітнього ступеня «магістр»
освітньо-професійної програми «Кримінальний аналіз»
спеціальність 124 «Системний аналіз»

Підписано до друку 30.09.2024. .Формат 60х84/16 Папір офсетний.
Гарн. «Times New Roman». Друк цифровий. Ум. друк .арк. 2,11.
Надруковано з готового оригінал-макета.
Наклад 30 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.