МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
КАФЕДРА ОПЕРАТИВНО-РОЗШУКОВОЇ ТА ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ
КАФЕДРА КІБЕРБЕЗПЕКИ

С. В. Кухаренко
О. А. Самойленко
А. С. Мурашко

РЕЖИМ СЕКРЕТНОСТІ ТА ЗАХИСТ ІНФОРМАЦІЇ

методичні вказівки для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти ступеня бакалавра
в галузі знань – К «Безпека та оборона»
спеціальність – К9 «Правоохоронна діяльність»

Одеса
Букаєв Вадим Вікторович
2025

УДК 355.58+351.861
С17

Рекомендовано до друку навчально-методичною радою Національного університету «Одеська юридична академія» (протокол № 1 від 08.10.2025 р.).

Укладачі:

Самойленко Олена Анатоліївна (ORCID ID https://orcid.org/0000-0002-8925-4116), професор кафедри оперативно-розшукової та поліцейської діяльності Національного університету «Одеська юридична академія», доктор юридичних наук, професор;

Кухаренко Сергій Вікторович (ORCID ID: https://orcid.org/0000-0001-7100-6408), доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»; кандидат технічних наук, доцент;

Мурашко Анастасія Сергіївна (ORCID ID: https://orcid.org/0000-0002-4114-2377), асистент кафедри оперативно-розшукової та поліцейської діяльності Національного університету «Одеська юридична академія».

Рецензенти:

А. Баб'як – завідувач кафедри оперативно-розшукової діяльності навчально-наукового інституту з підготовки фахівців для підрозділів кримінальної поліції Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

О. Кобзар – т.в.о директора навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ, доктор юридичних наук, професор

В. Вербовий – завідувач кафедри тактичної підготовки навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ підполковник поліції.

Самойленко О. А.

С17 Режим секретності та захист інформації: метод. вказівки для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти ступеня бакалавра галузі знань К «Безпека та оборона», спеціальність К9 «Правоохоронна діяльність». / Електрон. дані / Самойленко О. А., Кухаренко С. В., Мурашко А. С.; Нац. ун-т «Одеська юрид. академія». Одеса : видваець Букаєв Вадим Вікторович, 2025. – 41 с. DOI: https://doi.org/10.32837/11300.30874

Методичні вказівки «Режим секретності та захист інформації» призначені в межах освітньо-професійної програми підготовки «Правоохоронна діяльність» для підготовки здобувачів вищої освіти ступеня бакалавра у Національному університеті «Одеська юридична академія» в галузі знань К «Безпека та оборона», спеціальність К9 «Правоохоронна діяльність» з метою закріплення лекційного матеріалу та підготовки до практичних занять з вказаної дисципліни. Містять вказівки та завдання до практичних занять, самостійної роботи.

Матеріали призначені для науковців, викладачів та здобувачів закладів вищої юридичної освіти.

УДК 355.58+351.861

ЗМІСТ

ЗМІСТ 3

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ 4

2.МЕТОДИЧНІ ВКАЗІВКИ 5

3. НАВЧАЛЬНИЙ КОНТЕНТ ДИСЦИПЛІНИ (мета вивчення, зміст теми-план, питання та завдання для самостійної роботи) 7

Тема 1. Загальні положення курсу «Режим секретності та захист інформації»: зміст, завдання, структура курсу; зміст та класифікація інформації з обмеженим доступом. Конфіденційна інформація як вид інформації з обмеженим доступом 7

Тема 2. Поняття, ознаки державної таємниці. Правове забезпечення охорони державної таємниці. 9

Тема 3. Віднесення інформації до державної таємниці. Режими секретності 11

Тема 4. Матеріальні носії секретної інформації. Організація режиму та ступені секретності матеріального носія державної таємниці 12

Тема 5. Компетенції державних органів та органів місцевого самоврядування у сфері охорони секретної інформації, допуску та доступу до державної таємниці. Служба безпеки України 13

Тема 6. Нормативно-правове забезпечення у сфері технічного захисту інформації. Концепція технічного захисту інформації в Україні 15

Тема 7. Основні положення щодо організації системи захисту інформації 16

Тема 8. Класифікація технічних каналів витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів 17

Тема 9. Засоби та методи захисту інформації 18

Тема 10. Створення комплексів технічного захисту інформації, комплексної системи захисту інформації. 20

5. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ТА ВМІНЬ 22

6. ТЕСТОВІ ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ ЗДОБУВАЧА **24**

7. КРИТЕРІЇ ОЦІНЮВАННЯ УСПІШНОСТІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ **37**

8. РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ **38**

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Ця навчальна дисципліна є дисципліною обов'язкової складової навчального плану циклу дисциплін, які формують професійні компетентності за спеціальністю «Правоохоронна діяльність». Здобувачі отримують теоретичні знання щодо суті режимів секретності, основ захисту інформації, заходів та засобів, спрямованих на організацію та забезпечення технічного захисту інформації та складових організації процесу захисту державної таємниці, а також навички із розмежування кримінальної, адміністративної та інших видів юридичної відповідальності у сфері охорони державної таємниці та конфіденційної інформації. Дисципліна має теоретико-методологічне та значне практичне значення. Вона спрямована на формування у здобувача здатності до системного аналітичного юридичного мислення та знання способів розв'язання задач, що виникають у практичній діяльності в сфері судової та правоохоронної діяльності.

Основна мета вивчення дисципліни: вивчення навчальної дисципліни «Режим секретності та захист інформації» є формулювання у здобувачів знань щодо поняття, характеристик та змісту таємної інформації, особливостей її захисту, виявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на організацію та забезпечення технічного захисту інформації на об'єктах інформаційної діяльності у практичній діяльності за фахом та роботи органів безпеки, судової та правоохоронної діяльності, правових основ та процедурних питань системи охорони державної таємниці.

Завдання:

- вільно орієнтуватися в спеціальних знаннях з метою розмежування кримінальної, адміністративної та інших видів юридичної відповідальності у сфері охорони державної таємниці та конфіденційної інформації;
- визначати в конкретній слідчій ситуації інформацію з обмеженим доступом та її види (конфіденційна, таємна, службова інформація);
- визначати режим секретності та обґрунтовувати віднесення інформації до категорії з обмеженим доступом, конкретний її вид (конфіденційна, таємна, службова інформація);
- знати специфіку роботи органів захисту державної таємниці, засобів і методів захисту відомостей, що становлять державну таємницю, і їх носіїв, а також заходів, що проводяться в цих цілях;
- набути теоретичні й практичні навички для діяльності висококваліфікованого фахівця правоохоронних органів у сфері обігу конфіденційної інформації;
- проводити аналіз основних загроз безпеці програм та даних, типів атак;

використовувати сучасні процедури забезпечення основних послуг безпеки інформації в інформаційно-комунікаційних ресурсах та кіберпросторі. Аудиторне навчання із можливістю застосування електронного навчання і дистанційних освітніх технологій.

Методи, які використовуються під час навчання.

1. Лекція: викладач використовує структуровану презентацію, доповнюючи теоретичний матеріал прикладами з практики правоохоронних органів; застосовує інтерактивні елементи (короткі опитування, постановка запитань до аудиторії).

2. Практичні заняття: проводяться у формі презентацій, доповідей студентів, аналізу та обговорення реальних кейсів та моделювання дій в ситуації витоку секретної інформації, визначення заходів реагування.

3. Самостійна робота: робота з аналітичними матеріалами, аналіз судових рішень за фактами порушення режимів секретності; розробка алгоритмів реагування на інциденти витоку конфіденційних даних.

В ході аудиторної роботи також можуть бути використані наступні форми контролю: тестування знань; підготовка практичних завдань у вигляді кейсів для групового обговорення. Використання групових кейсів та ділових ігор дозволяє студентам оцінювати ризики та приймати рішення реагування.

МЕТОДИЧНІ ВКАЗІВКИ

Підчас навчання та вироблення практичних навичок в сфері діяльності з захисту інформації. рекомендується користуватися нормативно-правовими актами та методичними документами України, зокрема враховуючи наступні позиції:

1. Кодекс України про адміністративні правопорушення (від 7 грудня 1984 р. № 8073-X) та Кримінальний кодекс України (від 5 квітня 2001 р. № 2341-III) є основними актами, що регулюють адміністративну та кримінальну відповідальність за порушення правових норм, включаючи питання захисту інформації.

2. Закони України «Про державну таємницю», «Про інформацію», «Про Національну поліцію», «Про Службу безпеки України» та «Про оперативно-розшукову діяльність» є базовими у сфері захисту державної таємниці та регламентують порядок обігу конфіденційної інформації, а також специфіку та діяльність державних органів щодо її захисту.

3. Окремі норми (Закону України «Про захист інформації в інформаційно-комунікаційних системах», Правила забезпечення захисту інформації в інформаційних та комунікаційних системах, укази Президента та постанови КМУ щодо технічного захисту інформації) встановлюють вимоги щодо організації безпечного обігу інформації та створення комплексних систем захисту.

4. Нормативні документи ТЗІ (технічного захисту інформації) – НД ТЗІ 1.1-002-99, 3.7-003-05, 3.1-001-07, 2.5-004-99 та інші, що містять методичні вказівки щодо організації технічного захисту інформації, блокування каналів витоку та класифікації заходів захисту містять стандарти захисту інформації при передачі її адресату.

5. ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» є стандартом, який встановлює основні терміни і визначення у сфері технічного захисту інформації.

6. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) надає доступ до актуальних нормативних документів та методичних рекомендацій для забезпечення технічного захисту інформації.

Таким чином, зазначена література та нормативно-правові акти можуть використовуватися як основна база для аналізу, організації роботи та розробки практичних заходів із захисту інформації в Україні.

Також для опрацювання матеріалу сфери захисту таємної інформації рекомендується звернутися до підручників та навчально-методичних посібників, підготовлених українськими авторами, серед яких особливу увагу звернути на роботи: В. С. Зачепило, З. А. Шандра, І. Р. Опірського, В. І. Школьнікова, Ю. Ю. Орлова, А. М. Супруненко, І. І. Башта, А. М. Лисеюка, К. С. Свіріна.

Аудиторне навчання має два змістовних блока роботи для студента.

Перший блок інформації навчального курсу сконцентрований на: 1) вивченні класифікації інформації, видів обмеженого доступу, правил роботи з матеріальними носіями державної таємниці; 2) формуванні схем-конспектів основних положень законодавства та нормативних актів у будь-якій зручній формі (порівняльні таблиці, схеми, алгоритми);

Другий блок інформації навчального курсу спрямований на аналіз прикладів з практики НП України/інших держав щодо охорони конфіденційної та державної таємниці; можливим є підготовка міні-рефератів та практичних завдань щодо стандартів захисту інформації та порівняльно-правовий аналіз та тестування.

Для підготовки до поточного контролю та тестування слід повторити основні положення тем, які включають: види інформації та їх правовий режим, державну таємницю, грифи секретності, матеріальні носії інформації, компетенції органів влади у сфері охорони секретної інформації, технічний захист інформації, способи та засоби захисту, стандарти.

Для підготовки до практичних занять (практичних занять, в тому числі із застсуванням кейсів та ділових ігор) рекомендовано: при аналізі практичних ситуацій звертати увагу на різні точки зору щодо правового регулювання інформації з обмеженим доступом та секретності; використовувати актуальні нормативні документи та приклади реальної практики НП України, СБУ, органів місцевого самоврядування; підготувати короткі конспекти для обговорення проблемних питань, наприклад, щодо визначення меж доступу до відкритої та конфіденційної інформації; розробляти алгоритми дій у моделях ситуацій (наприклад, інцидент витоку інформації, неправильне оформлення матеріального носія, порушення режиму доступу).

Допускаться для виконання практичних завдань використовувати порівняльний та аналітичний підходи, зокрема: порівнювати національне законодавство із міжнародними стандартами (ЄС, ООН тощо) щодо захисту інформації та державної таємниці; аналізувати кейси з практики правозастосування щодо порушень режиму секретності та технічного захисту інформації; використовувати системний підхід для оцінки ризиків та вибору

оптимальних методів захисту інформації залежно від її виду та ступеня секретності.

Всі конспекти, міні-реферати та таблиці повинні відображати структуровану інформацію, наприклад, щодо: видів та класифікації інформації; порядку допуску та доступу до інформації з обмеженим доступом; грифів секретності та порядок їх застосування; матеріальних носіїв та технічних засобів захисту; компетенції державних органів та організаційні заходи захисту інформації; нормативно-правове забезпечення та міжнародні стандарти.

Кожен конспект або таблиця має включати короткі пояснення, приклади та схеми, що спрощують запам'ятовування та систематизацію знань.

З метою поглиблення знань і формування практичних навичок рекомендується здійснювати опрацювання кожного пункту Планів самостійної роботи, які подані нижче в навчальному контенті до кожної з тем навчальної дисципліни. Це сприятиме глибшому розумінню механізмів функціонування національної системи охорони секретної інформації, а також допоможе підготуватися до практичних занять і тематичних дискусій.

НАВЧАЛЬНИЙ КОНТЕНТ ДИСЦИПЛІНИ

Тема 1. Загальні положення курсу «Режим секретності та захист інформації»: зміст, завдання, структура курсу; зміст та класифікація інформації з обмеженим доступом. Конфіденційна інформація як вид інформації з обмеженим доступом

Мета вивчення

Ознайомити здобувачів вищої освіти з теоретичними основами курсу «Режим секретності та захист інформації», сформувати у них розуміння категорій інформації, що підлягає правовому захисту, структури обмеженого доступу до інформації, а також особливостей класифікації конфіденційної інформації як окремої категорії.

Зміст теми - план

1. Загальне поняття та види інформації як об'єкта правового захисту (залежно від режиму відображення, від сфери існування, від призначення, від стадій виникнення, за стабільністю, за ступенем організованості, за порядком доступу).
2. Відкрита інформація та інформація з обмеженим доступом.
3. Поняття інформації з обмеженим доступом та її види (конфіденційна, таємна, службова інформація).
4. Конфіденційна інформація. як вид інформації з обмеженим доступом
5. Зміст та місце курсу «Режим секретності та захист інформації» в системі підготовки працівників НП України.

Контрольні запитання для перевірки досягнення результатів навчання

1. Які є основні види інформації як об'єкта правового захисту згідно з різними критеріями?
2. У чому полягає відмінність між відкритою інформацією та інформацією з обмеженим доступом?
3. Які категорії охоплює інформація з обмеженим доступом згідно з законодавством України?
4. Що таке конфіденційна інформація та в чому полягає її правовий режим?
5. Яке значення має курс «Режим секретності та захист інформації» для майбутньої професійної діяльності співробітників поліції?

Результати навчання

Після опрацювання теми здобувач вищої освіти знатиме: класифікацію інформації за різними критеріями, визначення і правову природу відкритої та обмеженої в доступі інформації, види обмеженого доступу до інформації та їхнє нормативне забезпечення, сутність, ознаки й правовий режим конфіденційної інформації, місце і значення курсу «Режим секретності та захист інформації» в системі підготовки співробітників НПУ.

І буде вміти: аналізувати види інформації з обмеженим доступом відповідно до правового регулювання, застосовувати знання щодо захисту конфіденційної інформації у професійній діяльності, визначати місце курсу у загальній структурі професійної підготовки, аргументовано пояснювати межі доступу до інформації відповідно до її класифікації.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Підготувати міні реферати на теми (може бути розглянуто в межах двох наступних тем курсу):

1) Поняття та правова природа інформації з обмеженим доступом: вітчизняна та міжнародна практика.

2) Класифікація конфіденційної інформації та особливості її захисту в Національній поліції України.

3) Таємна та службова інформація: правові підстави та режим використання.

4) Відкрита інформація vs інформація з обмеженим доступом: проблеми визначення меж доступу.

5) Особливості обігу службової інформації у правоохоронних органах.

6) Юридична відповідальність за порушення режиму секретності: огляд практики.

7) Організація інформаційної безпеки в державних органах: роль посадових осіб.

8) Доступ до публічної інформації: баланс між відкритістю і національною безпекою.

9) Психологічний аспект роботи з інформацією, що має обмежений доступ: формування відповідальності у працівника.

10) Міжнародні стандарти захисту конфіденційної інформації: порівняльно-правовий аналіз.

11) Цифрова безпека та захист інформації з обмеженим доступом в умовах кіберзагроз.

12) Роль спеціальних навчальних курсів у формуванні культури секретності в поліції.

13) Правове регулювання обігу персональних даних у межах режиму конфіденційності.

14) Інформація з обмеженим доступом у судовому процесі: межі розголошення.

15) Етичні стандарти поводження з конфіденційною інформацією в публічній службі.

Тема 2. Поняття, ознаки державної таємниці. Правове забезпечення охорони державної таємниці

Мета вивчення

Ознайомити здобувачів вищої освіти з поняттям, змістом і ознаками державної таємниці, сформувати у них системне розуміння механізмів правового регулювання охорони державної таємниці в Україні, з урахуванням її місця серед інформації з обмеженим доступом та особливостей класифікації і захисту.

Зміст теми – план

1. Організаційно-правові основи охорони державної таємниці.
2. Ознаки державної таємниці як особливого виду інформації з обмеженим доступом. Відомості, які не можуть відноситися до державної таємниці.
3. Перелік відомостей, що становлять державну таємницю (сфери, до яких може належати).
4. Допуск та доступ громадян до відомостей, що становлять державну таємницю: суб'єкти, відповідальні за охорону державної таємниці, система допуску до державної таємниці: форми, порядок, обмеження.
5. Відповідальність за порушення законодавства у сфері охорони державної таємниці.
6. Взаємозв'язок державної таємниці з іншими видами інформації з обмеженим доступом (конфіденційною, службовою).

Контрольні запитання для перевірки досягнення результатів навчання

1. Що таке державна таємниця і яка її правова природа?

2. Які ознаки притаманні інформації, що належить до державної таємниці?

3. Хто визначає перелік відомостей, що становлять державну таємницю?

4. Які категорії осіб мають право доступу до державної таємниці і на яких умовах?

5. У чому полягає правове забезпечення охорони державної таємниці?

6. Які існують правові наслідки порушення режиму збереження державної таємниці?

7. Чим відрізняється державна таємниця від інших видів інформації з обмеженим доступом?

Результати навчання

Після опрацювання теми здобувач вищої освіти:

Знатиме: поняття, ознаки та структуру державної таємниці; правову базу охорони державної таємниці; механізми класифікації відомостей та форми допуску до секретної інформації; відмінності між видами інформації з обмеженим доступом. **Умітиме**: аналізувати правові акти щодо охорони державної таємниці; визначати сферу належності інформації до державної таємниці; застосовувати знання в умовах професійної діяльності; пояснювати порядок допуску до державної таємниці та юридичні наслідки його порушення.

План самостійної роботи

1. Опрацювання лекційного матеріалу та нормативно-правових актів (Закон України «Про державну таємницю» та ін.).
2. Підготовка до практичного заняття: аналіз правових ситуацій, пов’язаних з держтаємницею.
3. Підготовка міні-рефератів на теми:

1) Правове регулювання захисту державної таємниці: національні особливості.

2) Суб’єкти та обов’язки щодо збереження державної таємниці.

3) Доступ до державної таємниці: процедура та юридичні обмеження.

4) Порушення режиму державної таємниці: кримінально-правові наслідки.

5) Порівняння держтаємниці та конфіденційної інформації: межі і перетин.

6) Забезпечення державної таємниці в умовах воєнного стану: виклики та ризики.

Тема 3. Віднесення інформації до державної таємниці. Тежими секретності

Мета вивчення

Ознайомити здобувачів вищої освіти з процедурою віднесення інформації до державної таємниці, критеріями та підставами класифікації інформації, а також з видами грифів секретності, що встановлюються відповідно до ступеня можливої шкоди національній безпеці у разі розголошення.

Зміст теми – план

1. Загальні підстави та критерії віднесення інформації до державної таємниці.
2. Порядок формування і затвердження Зводу відомостей, що становлять державну таємницю.
3. Повноваження суб'єктів, які приймають рішення щодо віднесення інформації до державної таємниці.
4. Грифи секретності: поняття, види, правове значення.
5. Зміст і застосування грифів секретності: «Цілком таємно», «Таємно», «Для службового користування» (ДСК).
6. Обмеження доступу до інформації за грифом секретності.
7. Контроль за дотриманням правил засекречування та відповідальність за їх порушення.

Контрольні запитання для перевірки досягнення результатів навчання

1. Які критерії визначають можливість віднесення інформації до державної таємниці?
2. Що таке Звід відомостей, що становлять державну таємницю, і як він формується?
3. Хто має право класифікувати інформацію як таку, що містить державну таємницю?
4. У чому полягає сутність грифів секретності та як вони застосовуються?
5. Які є види грифів секретності та яку інформацію вони охоплюють?
6. Яка відповідальність настає за порушення процедури віднесення інформації до державної таємниці?

Результати навчання

Після опрацювання теми здобувач вищої освіти:

Знатиме: критерії та порядок віднесення інформації до державної таємниці; функції та структуру Зводу відомостей, що становлять державну таємницю; класифікацію грифів секретності, їх значення та строки дії; повноваження суб'єктів, уповноважених на засекречування інформації.

Умітиме: визначати відповідність інформації критеріям державної таємниці; застосовувати знання про гриф секретності у практичній діяльності; орієнтуватися в нормативно-правовій базі, що регламентує процедуру

засекречування; аналізувати юридичні наслідки порушення режиму секретності.

План самостійної роботи

1. Опрацювання лекційного матеріалу, Закону України «Про державну таємницю» та нормативних актів.
2. Вивчення структури та змісту чинного Зводу відомостей, що становлять державну таємницю.
3. Підготовка до практичного заняття: розгляд кейсів щодо неправомірного застосування грифів секретності.
4. Підготовка міні-рефератів на теми:

1) Порядок віднесення інформації до державної таємниці в Україні та міжнародна практика.
2) Строки дії грифів секретності та процедура їх продовження/зняття.
3) Типові порушення під час класифікації інформації як такої, що становить державну таємницю.
4) Порівняльний аналіз грифів секретності в Україні та країнах НАТО.
5) Відповідальність за безпідставне засекречування інформації: аналіз правозастосовної практики.

Тема 4. Матеріальні носії секретної інформації. Організація режиму та ступені секретності матеріального носія державної таємниці

Мета вивчення

Сформувати у здобувачів вищої освіти знання про поняття матеріального носія секретної інформації, особливості поводження з ним, організацію режиму секретності, а також критерії визначення ступеня секретності матеріального носія залежно від рівня важливості інформації, яку він містить.

Зміст теми – план

1. Поняття та види матеріальних носіїв секретної інформації. Ідентифікація матеріального носія державної таємниці.
2. Гриф секретності на матеріальному носії: порядок нанесення та оформлення.
3. Організація режиму секретності щодо матеріальних носіїв.
4. Зберігання, передача, транспортування та знищення матеріальних носіїв державної таємниці.
5. Відповідальність за порушення правил поводження з матеріальними носіями, що містять державну таємницю.

Контрольні запитання для перевірки досягнення результатів навчання

1. Що таке матеріальний носій секретної інформації та які його основні види?
2. Як ідентифікуються матеріальні носії, що містять державну таємницю?

3. Як оформляється гриф секретності на матеріальному носії?

4. Які вимоги пред'являються до обліку, зберігання і транспортування матеріальних носіїв?

5. У чому полягають особливості режиму секретності щодо матеріальних носіїв?

6. Які ступені секретності застосовуються до матеріальних носіїв і як вони визначаються?

7. Яка відповідальність настає за неналежне поводження з матеріальними носіями державної таємниці?

Результати навчання

Після опрацювання теми здобувач вищої освіти:

Знатиме: поняття та види матеріальних носіїв секретної інформації; правила нанесення грифів секретності; організаційно-правові засади поводження з такими носіями; класифікацію ступенів секретності матеріального носія; вимоги до обліку, зберігання, передачі та знищення носіїв.

Умітиме: застосовувати норми законодавства щодо організації режиму секретності матеріальних носіїв; оформляти матеріальні носії відповідно до встановленого ступеня секретності; визначати порушення режиму та оцінювати юридичні наслідки; виявляти прогалини або помилки в поводженні з секретними матеріальними носіями.

План самостійної роботи

1. Опрацювання нормативно-правових актів щодо режиму секретності матеріальних носіїв інформації.

2. Вивчення інструкцій з обліку, зберігання та знищення матеріальних носіїв, що містять державну таємницю.

3. Підготовка до практичного заняття: аналіз ситуацій неправомірного поводження з матеріальними носіями секретної інформації.

4. Підготовка міні-рефератів на теми: Практика знищення матеріальних носіїв, що містять державну таємницю; Відповідальність за втрату або розголошення інформації, що зберігається на матеріальному носії.

Тема 5. Компетенції державних органів та органів місцевого самоврядування у сфері охорони секретної інформації, допуску та доступу до державної таємниці. Служба безпеки України

Мета вивчення

Надати здобувачам вищої освіти комплексне уявлення про роль Служби безпеки України як спеціально уповноваженого органу у сфері захисту інормації.

Зміст теми – план

1. Компетенція органів державної влади у сфері охорони державної таємниці.

2. Роль Служби безпеки України в системі забезпечення охорони державної таємниці.

3 Контроль за дотриманням режиму доступу та відповідальність за його порушення.

Контрольні запитання для перевірки досягнення результатів навчання

1. Які органи є суб'єктами системи охорони державної таємниці в Україні?

2. У чому полягає компетенція органів місцевого самоврядування у сфері охорони секретної інформації?

3. Які функції виконує Служба безпеки України щодо захисту державної таємниці?

4. Які види допуску до державної таємниці існують і в чому їхні відмінності?

5. У чому полягає процедура перевірки осіб перед наданням їм допуску до держтаємниці?

6. Як здійснюється облік осіб, які отримали допуск до секретної інформації?

7. За яких умов може бути припинено або скасовано допуск до державної таємниці?

8. Яка відповідальність настає за порушення правил допуску або доступу до держтаємниці?

Результати навчання

Після опрацювання теми здобувач вищої освіти:

Знатиме: структуру системи охорони державної таємниці; компетенції органів влади у цій сфері; порядок і умови отримання допуску до державної таємниці; функції та повноваження СБУ як головного органу в галузі захисту секретної інформації.

Умітиме: розрізняти рівні допуску до держтаємниці; застосовувати знання для аналізу повноважень різних органів у сфері секретності; визначати правові підстави для отримання чи скасування доступу; оцінювати дії посадових осіб щодо дотримання режиму доступу.

План самостійної роботи

1. Опрацювання Закону України «Про державну таємницю» щодо компетенції органів державної влади та СБУ.

2. Ознайомлення з нормативно-правовими актами, що регламентують допуск до держтаємниці.

3. Аналіз практики роботи органів місцевого самоврядування у сфері захисту секретної інформації.

4. Підготовка міні-рефератів на теми: Роль СБУ у забезпеченні режиму секретності в Україні. Порівняльна характеристика допуску до державної таємниці в Україні та країнах ЄС. Повноваження органів місцевого самоврядування в контексті збереження держтаємниці.

Тема 6. Нормативно-правове забезпечення у сфері технічного захисту інформації. Концепція технічного захисту інформації в Україні

Мета вивчення

Сформувати у студентів цілісне розуміння нормативно-правової бази та концептуальних засад технічного захисту інформації в Україні, ознайомити з основними законами, підзаконними актами, державними стандартами та концепціями, що регламентують діяльність у сфері технічного захисту інформації (ТЗІ), а також навчити застосовувати їх на практиці для забезпечення комплексної безпеки інформації.

Зміст теми – план

1. Нормативно-правове забезпечення безпеки інформації.
2. Державна політика у сфері технічного захисту інформації.

Контрольні запитання для перевірки досягнення результатів навчання

1. Які є потенційні загрози національній безпеці України в інформаційній сфері?
2. Яка основна мета Закону України «Про інформацію»?
3. Надайте визначення інформації.
4. Які правові основи інформаційної діяльності закладено у Закон України «Про інформацію»?
5. Які основні види інформації визначаються у Законі України «Про інформацію»?
6. Як поділяється інформація за режимом доступу до неї?
7. Як здійснюється контроль за режимом доступу до інформації?
8. Яка інформація відноситься до конфіденційної?
9. Яка інформація відноситься до таємної інформації?
10. Чим та як визначається інформація, що складає державну таємницю?
11. Чим визначається ступень таємності інформації?
12. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
13. Що визначає та має забезпечити «Концепція технічного захисту інформації в Україні»?
14. Надайте визначення ТЗІ.
15. Що складає правову основу забезпечення ТЗІ в Україні?
16. Які основні напрями державної політики у сфері ТЗІ?

17. Надайте визначення системи ТЗІ.
18. Що становить правову основу забезпечення ТЗІ в Україні?
19. Які принципи державної політики у сфері ТЗІ?
20. Перелічите основні функції організаційних структур системи ТЗІ.
21. Чим визначається державна політика у сфері ТЗІ?
22. З чого складається нормативно-правова база у сфері ТЗІ?

Результати навчання

Після вивчення даної теми студенти повинні знати: основні нормативно-правові акти України у сфері (ТЗІ); роль та компетенцію органів державного управління (Держспецзв'язок, СБУ, НБУ тощо) у сфері ТЗІ; принципи та положення Концепції технічного захисту інформації в Україні.

Вміти: аналізувати правові акти, що регламентують захист інформації; визначати вимоги до систем технічного захисту інформації згідно з нормативно-правовою базою; зіставляти положення Концепції ТЗІ з практичними завданнями забезпечення безпеки інформаційних систем.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на тестові питання до теми.

Тема 7. Основні положення щодо організації системи захисту інформації

Мета вивчення

Сформувати у студентів теоретичні знання та практичні навички з організації комплексної системи захисту інформації, що забезпечує конфіденційність, цілісність та доступність даних в інформаційних системах і на об'єктах інформаційної діяльності.

Зміст теми – план

1. Принципи побудови системи захисту інформації.
2. Етапи організації системи захисту інформації Об'єкти захисту інформації.
3. Складові системи захисту інформації.

Контрольні запитання для перевірки досягнення результатів навчання

1. Як розглядають канал зв'язку з точки зору захисту інформації?
2. Назвіть об'єкти захисту інформації.
3. Дайте визначення основних технічних засобів та систем.
4. Дайте визначення допоміжних технічних засобів та систем.

5. Дайте визначення терміну «захист інформації».
6. Які властивості характеризують інформацію як об’єкт захисту?
7. Дайте визначення технічного захисту інформації?
8. Що, являє собою система технічного захисту інформації?
9. Де здійснюється технічний захист інформації?
10. Що є об’єктами технічного захисту інформації?
11. Дайте визначення об’єкту інформаційної діяльності.
12. Що є суб’єктами системи ТЗІ?
13. На які напрямки умовно можна розділити технічний захист інформації?
14. Що необхідно здійснити для побудови систем (комплексів) захисту інформації?

Результати навчання

Після вивчення теми студент повинен розуміти принципи побудови системи захисту інформації та їх практичну реалізацію.

Вміти визначати загрози та оцінювати ризики для інформаційних ресурсів, а також знати основні етапи створення та підтримки системи захисту інформації. Бути здатним застосовувати нормативно-правові акти та стандарти у сфері інформаційної безпеки.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Ознайомитись з Законом України «Про захист інформації в інформаційно-комунікаційних системах»
4. Відповісти на тестові питання до теми.

Тема 8. Класифікація технічних каналів витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів

Мета вивчення

Ознайомитися з основними видами технічних каналів витоку інформації. Зрозуміти фізичну природу та принципи їх утворення. Вивчити методи та засоби несанкціонованого зняття інформації. Сформувати навички аналізу ризиків витоку даних та вибору відповідних заходів захисту.

Зміст теми – план

1. Класифікація технічних каналів витоку інформації.
1.1. Акустичні канали.
1.2. Вібраційні канали.
1.3. Електромагнітні канали.
1.4. Оптичні канали.

2. Способи несанкціонованого зняття інформації з технічних каналів.
2.1. Пасивні методи.
2.2. Активні методи.

Контрольні запитання для перевірки досягнення результатів навчання

1. Що таке технічний канал витоку інформації?
2. Які основні види каналів витоку інформації ви знаєте?
3. У чому різниця між акустичним та вібраційним каналами витоку?
4. Як класифікують методи зняття інформації з технічних каналів?
5. Які основні заходи застосовують для запобігання витоку інформації?

Результати навчання

Після вивчення теми студенти повинні вміти:

1. Класифікувати технічні канали витоку інформації за фізичною природою та способом утворення.
2. Пояснювати принципи роботи основних методів несанкціонованого знімання інформації.
3. Оцінювати ризики витоку інформації через технічні канали на прикладі реальних ситуацій.
4. Пропонувати заходи захисту від конкретних типів технічних каналів витоку.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Завдання для виконання:

1. Дослідити типи технічних каналів витоку інформації та навести приклади для кожного типу.
2. Скласти таблицю, де зазначити:

– канал витоку;
– можливий спосіб несанкціонованого зняття інформації;
– можливі заходи захисту.

3. Пояснити різницю між пасивними та активними методами зняття інформації.
4. Описати приклади комбінованих каналів витоку та методів протидії.

Тема 9. Засоби та методи захисту інформації

Мета вивчення

Метою вивчення теми є формування у студентів знань та практичних навичок щодо сучасних засобів і методів забезпечення конфіденційності, цілісності та доступності інформації. Студенти повинні зрозуміти принципи

побудови систем захисту, ознайомитися з інструментами протидії загрозам, навчитися обирати та застосовувати відповідні методи залежно від характеру інформації, що захищається, та можливих ризиків.

Зміст теми – план

1. Поняття інформаційної безпеки та її складові.
2. Класифікація загроз та уразливостей.
3. Методи захисту.
4. Засоби захисту.

Контрольні запитання для перевірки досягнення результатів навчання

1. Назвіть основні методи захисту інформації.
2. У чому різниця між програмними та апаратними засобами?
3. Які основні загрози інформаційним системам ви знаєте?
4. Чим відрізняються методи організаційного та технічного захисту інформації?
5. Що таке криптографічні методи захисту?
6. Які існують методи автентифікації користувачів?
7. Які засоби контролю доступу застосовуються в інформаційних системах?
8. Як класифікують засоби технічного захисту інформації (апаратні, програмні, організаційні)?

Результати навчання

Після вивчення даної теми студенти повинні Знати та розуміти: класифікацію загроз інформаційній безпеці та вразливостей систем; основні засоби захисту інформації: організаційні, технічні, криптографічні, програмні та апаратні; методи захисту інформації від несанкціонованого доступу, витоку, модифікації та знищення. Уміти: обирати оптимальні методи та засоби захисту залежно від типу інформації та рівня загроз; застосовувати програмні та апаратні засоби для забезпечення конфіденційності, цілісності та доступності даних; оцінювати ефективність використаних засобів та методів захисту.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Ознайомитися з основними принципами захисту інформації.
4. Дослідити класифікацію засобів захисту інформації (організаційні, технічні, програмні, криптографічні).
5. Вивчити методи захисту інформації.
6. Проаналізувати реальні інциденти витоку інформації (причини виникнення).

7. Порівняти апаратні та програмні засоби захисту інформаці (переваги та недоліки кожного підходу).

Тема 10. Створення комплексів технічного захисту інформації, комплексної системи захисту інформації

Мета вивчення

Ознайомитися з принципами проєктування, побудови та інтеграції комплексів технічного захисту інформації (ТЗІ) та комплексних систем захисту інформації. Навчитися аналізувати загрози, оцінювати ризики, підбирати відповідні технічні засоби захисту та організаційні заходи для забезпечення конфіденційності, цілісності та доступності інформації в різних об'єктах інформаційної діяльності.

Зміст теми – план

1. Основні цілі створення комплексів ТЗІ.
2. Основні компоненти комплексів ТЗІ.
3. Етапи створення комплексної системи захисту інформації.
4. Методи оцінки ефективності комплексів ТЗІ

Контрольні запитання для перевірки досягнення результатів навчання

1. Що таке комплекс технічного захисту інформації (КТЗІ)?
2. Які основні компоненти комплексної системи захисту інформації (КСЗІ)?
3. Чим відрізняється технічний захист інформації від організаційного та програмного?
4. Що таке контрольована зона у КСЗІ?
5. Назвіть основні державні та міжнародні стандарти, що регламентують створення КТЗІ.
6. Які нормативні документи регламентують класифікацію інформації та її захист у комплексних системах?
7. Які етапи проектування комплексної системи захисту інформації?
8. Опишіть процес вибору технічних засобів захисту для конкретного об'єкта інформаційної діяльності.
9. Як оцінюється ефективність комплексного захисту інформації?
10. Які методи захисту інформації за допомогою технічних засобів ви знаєте?
11. Як організовується моніторинг та контроль за станом КСЗІ?
12. Які потенційні загрози можуть виникати при невірному проектуванні КТЗІ?
13. Як забезпечити баланс між ефективністю захисту та вартістю впровадження КСЗІ?
14. Які є головні принципи та етапи захисту від загроз?

15. Які є види захисту інформації?
16. Які нормативні акти України передбачають створення КСЗІ?
17. Для захисту від яких видів загроз створюється КСЗІ?
18. Які засоби захисту використовуються у складі КСЗІ?
19. Хто є відповідальним за захист інформації в організації?

Результати навчання

Після опанування теми студент має вміти: пояснювати принципи побудови комплексних систем технічного захисту інформації (ТЗІ); розрізняти види комплексів ТЗІ за рівнем захисту, об'єктами та технологіями; описувати основні компоненти та функції комплексів ТЗІ (апаратні, програмні, мережеві та організаційні засоби); аналізувати нормативно-правові та технічні вимоги до побудови систем захисту інформації; визначати критичні інформаційні ресурси та рівні їхнього захисту; оцінювати відповідність існуючих технічних засобів захисту інформації вимогам безпеки об'єкта. Формувати комплексні технічні рішення для забезпечення конфіденційності, цілісності та доступності інформації. Використовувати сучасні програмні та апаратні засоби для побудови надійних систем захисту інформації.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на тестові питання до теми.

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ ЗДОБУВАЧА

1. Ознаки державної таємниці як особливого виду інформації з обмеженим доступом. Відомості, які не можуть відноситися до державної таємниці.
2. Перелік відомостей, що становлять державну таємницю (сфери, до яких може належати).
3. Допуск та доступ громадян до відомостей, що становлять державну таємницю: суб'єкти, відповідальні за охорону державної таємниці, система допуску до державної таємниці: форми, порядок, обмеження.
4. Відповідальність за порушення законодавства у сфері охорони державної таємниці.
5. Взаємозв'язок державної таємниці з іншими видами інформації з обмеженим доступом (конфіденційною, службовою).
6. Загальне поняття та види інформації як об'єкта правового захисту (залежно від режиму відображення, від сфери існування, від призначення, від стадій виникнення, за стабільністю, за ступенем організованості, за порядком доступу).
7. Відкрита інформація та інформація з обмеженим доступом.
8. Поняття інформації з обмеженим доступом та її види (конфіденційна, таємна, службова інформація).
9. Конфіденційна інформація. як вид інформації з обмеженим доступом
10. Зміст та місце курсу «Режим секретності та захист інформації» в системі підготовки працівників НП України.
11. Які критерії визначають можливість віднесення інформації до державної таємниці?
12. Що таке Звід відомостей, що становлять державну таємницю, і як він формується?
13. Хто має право класифікувати інформацію як таку, що містить державну таємницю?
14. У чому полягає сутність грифів секретності та як вони застосовуються?
15. Які є види грифів секретності та яку інформацію вони охоплюють?
16. Як встановлюється строк засекречування і коли гриф секретності може бути знятий?
17. Яка відповідальність настає за порушення процедури віднесення інформації до державної таємниці
18. Що таке матеріальний носій секретної інформації та які його основні види
19. Як ідентифікуються матеріальні носії, що містять державну таємницю
20. Як оформляється гриф секретності на матеріальному носії?

21. Які вимоги пред'являються до обліку, зберігання і транспортування матеріальних носіїв?
22. У чому полягають особливості режиму секретності щодо матеріальних носіїв?
23. Які ступені секретності застосовуються до матеріальних носіїв і як вони визначаються?
24. Яка відповідальність настає за неналежне поводження з матеріальними носіями державної таємниці?
25. Компетенція органів державної влади у сфері охорони державної таємниці.
26. Роль Служби безпеки України в системі забезпечення охорони державної таємниці.
27. Контроль за дотриманням режиму доступу та відповідальність за його порушення.
28. Нормативно-правове забезпечення безпеки інформації.
29. Державна політика у сфері технічного захисту інформації.
30. Принципи побудови системи захисту інформації.
31. Етапи організації системи захисту інформації.
32. Об'єкти захисту інформації.
33. Складові системи захисту інформації.
34. Класифікація технічних каналів витоку інформації.
35. Акустичні канали. Вібраційні канали.
36. Електромагнітні канали.
37. Оптичні канали.
38. Способи несанкціонованого зняття інформації з технічних каналів.
39. Пасивні методи.
40. Активні методи.
41. Поняття інформаційної безпеки та її складові.
42. Класифікація загроз та уразливостей.
43. Методи захисту.
44. Засоби захисту.
45. Основні цілі створення комплексів ТЗІ.
46. Основні компоненти комплексів ТЗІ.
47. Етапи створення комплексної системи захисту інформації.
48. Методи оцінки ефективності комплексів ТЗІ.
49. етапи проектування комплексної системи захисту.
50. моніторинг та контроль за станом КСЗІ.

ТЕСТОВІ ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ ЗДОБУВАЧА

(денна та заочна форма навчання)

1. Правила розмежування доступу це:

а) звернення одного об'єкта комп'ютерної системи до іншого з метою отримання певного типу доступу

б) частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів

в) доступ до інформації, що не порушує правила розмежування доступу

г) дозвіл або заборона здійснення певного типу доступу

2. Безпека інформації це:

а) сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації

б) сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації

в) стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації

г) діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз

3. Доступність це:

а) властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки

б) властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний

в) властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії

г) властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом

4. Пароль це:

а) секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до комп'ютерної системи або до інформації

б) процедура присвоєння ідентифікатора об'єкту комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором; впізнання

в) вид паролю, що звичайно складається тільки із цифр, і який, як правило, має бути пред'явлений нарівні з носимим ідентифікатором

г) процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності

5. Автентифікація це:

а) інформація, що використовується для автентифікації

б) послуга, що забезпечує збирання і аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих комплексів засобів захисту

в) процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності

г) послуга, що забезпечує конфіденційність інформації відповідно до принципів довірчого керування доступом

6. Які види інформації підлягають захисту в інформаційних, комунікаційних та інформаційно-комунікаційних системах:

а) відкрита інформація, яка є власністю держави і належить до "статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами; конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу; інформація, що становить державну або іншу передбачену законом таємницю

б) інформація, яка циркулює, обробляється, накопичується і зберігається в органах державної виконавчої влади

в) відкрита інформація, яка є власністю держави, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами; конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу; інформація, що становить державну або іншу передбачену законом таємницю

г) конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про

фізичну особу; інформація, що становить державну або іншу передбачену законом таємницю

7. Ким визначається 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?

а) власником інформації

б) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації

в) законодавством

г) власником системи

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

а) Кабінет Міністрів України

б) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації

в) законодавство

г) Національний банк України

9. Цілісність це властивість інформації, яка характеризує…

а) захищеність інформації від несанкціонованого ознайомлення з нею

б) захищеність інформації від несанкціонованого блокування

в) захищеність інформації нормам та вимогам захищеності інформації

г) захищеність інформації від несанкціонованого спотворення (зміни) або знищення

10. До основних видів інформаційної діяльності відносять:

а) збирання, охорона та захист, зберігання, одержання

б) створення, збирання, одержання, видалення

в) зберігання, використання, поширення, блокування

г) захист, знищення, поширення, створення

11. Прослуховування через акустичні, електричні, оптичні, радіо канали можна розглядати як загрозу :

а) доступності

б) через технічні канали

в) цілісності

г) конфіденційності

12. Технічний захист інформації (ТЗІ) – це

а) сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією

б) діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави

в) діяльність, спрямована на забезпечення організаційно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом

г) діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації

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

а) законодавство

б) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації

в) власники інформації

г) власник системи

14. Чим визначається порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації?

а) власником системи

б) власником інформації

в) законодавством

г) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації

15. Яке поняття визначає будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків.

а) ризик

б) загроза

в) вразливість

г) атака

16. Інформація з обмеженим доступом за своїм правовим режимом поділяється на

а) конфіденційну, таємну.

б) конфіденційну, комерційну, таємну.

в) комерційну, таємну.

г) комерційну, конфіденційну, банківську, таємну.

17. Яка мета Закону України «Про захист інформації в інформаційно-комунікаційних системах»?

а) забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації;

б) встановлення загальних правових основ одержання, використання, поширення та зберігання інформації, закріплення права особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначення статусу учасників інформаційних відносин, регулювання доступу до інформації та забезпечення її охорони, захист особи та суспільства від неправдивої інформації;

в) регулювання відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

г) встановлення основ регулювання правових відносин щодо захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

18. Згідно з Законом України Про захист інформації в інформаційно-комунікаційних системах під захистом інформації в системі розуміють…

а) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

б) діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

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

г) сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

19. Що не є суб'єктом відносин, пов'язаних із захистом інформації в системах?

а) інформація;

б) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

в) власники системи;

г) користувачі.

20. Ким визначається 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?

а) власником інформації;

б) законодавством;

в) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

г) власником системи.

21. Ким визначається порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації?

а) володільцем інформації

б) законодавством

в) спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації

г) володільцем системи.

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

а) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації;

б) законодавство;

в) користувач;

г) власник системи.

23. Відповідальність за забезпечення захисту інформації в системі покладається на…

а) власника інформації;

б) користувача;

в) спеціально уповноважений орган;

г) власника системи.

24. Згідно постанови про Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах відкрита інформація під час обробки в системі повинна зберігати:

а) надійність;

б) цілісність;

в) правильність;

г) конфіденційність.

25. Конфіденційність це властивість інформації, яка характеризує…

а) захищеність інформації від несанкціонованого спотворення (зміни) або знищення;

б) захищеність інформації нормам та вимогам захищеності інформації;

в) захищеність інформації від несанкціонованого ознайомлення з нею;

г) захищеність інформації від несанкціонованого блокування.

26. Згідно з Законом України «Про інформацію» під захистом інформації розуміють

а) перетворення інформації з використанням спеціальних даних з метою приховування змісту інформації, підтвердження її справжності, цілісності;

б) сукупність методів та засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру;

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

г) діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

27. До інформації з обмеженим доступом не можуть бути віднесені такі відомості

а) про критичну технологічну інформацію;

б) про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою;

в) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

г) про місце розташування військових об’єктів.

28. До основних видів інформаційної діяльності відносять:

а) створення, збирання, одержання, видалення;

б) зберігання, використання, поширення, блокування;

3. збирання, охорона та захист, зберігання, одержання;

г) захист, знищення, поширення, створення.

29. Доступність це властивість інформації, яка характеризує…

а) захищеність інформації від несанкціонованого блокування;

б) захищеність інформації нормам та вимогам захищеності інформації;

в) захищеність інформації від несанкціонованого спотворення (зміни) або знищення;

г) захищеність інформації від несанкціонованого ознайомлення з нею.

30. Концепція технічного захисту інформації в Україні визначає основи державної політики у сфері захисту інформації

а) науково-технічними заходами;

б) інженерно-технічними заходами;

в) інженерними заходами;

г) всі перелічені відповіді вірні.

31. ТЗІ – це діяльність, спрямована на…

а) забезпечення науково-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації;

б) забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави;

в) забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з необмеженим доступом;

г) всі перелічені відповіді вірні.

32. Правову основу забезпечення ТЗІ в Україні становлять:

а) Конституція України, Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин;

б) Концепція національної безпеки України та інші нормативно-правові акти, міжнародні договори України, Конституція України, Закони України «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах»;

в) Конституція України, Концепція національної безпеки України, Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах»;

г) Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про науково-технічну інформацію», Конституція України, Концепція національної безпеки України, інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

33. Цілісність це властивість інформації, яка характеризує…

а) захищеність інформації від несанкціонованого ознайомлення з нею;

б) захищеність інформації від несанкціонованого спотворення (зміни) або знищення;

в) захищеність інформації від несанкціонованого блокування;

г) захищеність інформації нормам та вимогам захищеності інформації.

34. Фішингові сайти та ресурси можна розглядати як загрозу :

а) доступності

б) автентичності

в) конфіденційності

г) цілісності.

35. Оберіть помилкове твердження :

а) вразливість є умовою чи множиною умов, які можуть допустити вплив загрози на активи;

б) вразливість може зникнути чи втратити актуальність, якщо відбудуться зміни в активах;

в) всі вразливості чутливі до загроз;

г) вразливість послаблює систему і може призводити до небажаних наслідків.

36. Оберіть помилкове твердження :

а) ризик – імовірність того, що дана загроза, впливаючи через вразливість організації, заподіє втрати чи пошкодження активів;

б) ризики можна лише частково зменшити за допомогою засобів захисту;

в) будь-яка зміна стану активів, загроз, вразливостей і засобів захисту може вплинути на ризики;

г) за допомогою засобів захисту можна повністю усунути будь-які ризики.

37. Які види документів використовуються на етапі розробки політики безпеки інформації?

а) план захисту інформації

б) інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС

в) інструкція адміністратора безпеки в ІТС

г) робочий проект КСЗІ

38. Які види документів використовуються на етапі розробки проекту КСЗІ?

а) робочий проект КСЗІ

б) технічне завдання на створення КСЗІ

в) план захисту інформації

г) модель порушника

39. Який вид документа використовується на етапі супроводження КСЗІ?

а) інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС

б) правила управління паролями в ІТС

в) інструкція адміністратора безпеки в ІТС

г) план захисту

40. За якими результатами не приймається рішення про необхідність ствренння КСЗІ?

а) визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї

б) оцінки моделі загроз

в) аналізу нормативно-правових актів

г) забезпечення цілісності інформації відповідно до вимог нормативно-правових актів

41. До якого класу АС відноситься одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу?

а) АС класу 2

б) АС класу 3

в) АС класу 1

г) АС класу 4

42. До якого класу АС відноситься локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу?

а) АС класу 1

б) АС класу 3

в) АС класу 2

г) АС класу 4

43. До якого класу АС відноситься розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу?

а) АС класу 3

б) АС класу 1

в) АС класу 2

г) АС класу 4

44. Який документ визначає повноваження та відповідальність працівників СЗІ?

а) посадові інструкції

б) функціональні обов’язки

в) інструкція про порядок проведення контролю режиму обробки та захисту інформації в ІТС

г) положення про СЗІ

45. Які з наведених функцій не відносяться до СЗІ?

а) визначення переліків відомостей, які підлягають захисту в процесі обробки

б) розробка та коригування архітектури АС, вибір та налаштування апаратно-програмних засобів на об'єктах електронно-обчислювальної техніки

в) участь у розробці нормативних документів, чинних у межах організації і АС

г) розробка та коригування моделі загроз і моделі захисту інформації в АС

46. Як називається категоріювання ІТС, що здійснюєтья у разі її створення?

а) первинне

б) планове

в) експертне

г) обов'язкове

47. Протягом якого терміну акт категоріювання є чинним?

а) 3 роки

б) до зміни ознаки, за якою була встановлена категорія, але не більше 4 роки

в) 5 років

г) 2 роки

48. При якому обстеженні передбачається аналіз і опис класу і структури ІТС, виду каналів зв'язку та апаратно-програмних засобів захисту?

а) обстеження інформаційного середовища

б) обстеження обчислювальної системи

в) обстеження фізичного середовища

г) обстеження мережевого середовища

49. При якому обстеженні передбачається аналіз інформації та її класифікація?

а) обстеження інформаційного середовища

б) обстеження фізичного середовища

в) обстеження обчислювальної системи (середовища функціонування ІКС)

г) обстеження середовища користувачів

50. На якому етапі створення КСЗІ складається модель загроз інформації?

а) розробка політики безпеки інформації

б) формування вимог до КСЗІ

в) розробка технічного завдання на створення КСЗІ

г) введення КСЗІ в дію

51. На якому етапі створення КСЗІ проводиться навчання користувачів?

а) розробка політики безпеки інформації

б) введення КСЗІ в дію

в) супроводження КСЗІ

г) розробка технічного завдання на створення КСЗІ

52. Положення про СЗІ затверджується:
а) керівником СЗІ
б) керівником РСО
в) начальником управління Держспецзв'язку
г) керівником організації

53. На якому етапі створення КСЗІ приймається положення про службу захисту інформації?
а) розробка політики безпеки інформації
б) формування загальних вимог до КСЗІ
в) розробка технічного завдання на створення КСЗІ
г) розробка проекту КСЗІ

54. Який документ створюється за результатами категоріювання ІТС?
а) звіт категоріювання
б) положення про категоріювання
в) акт категоріювання
г) відомість категоріювання

55. При якому обстеженні передбачається аналіз функціонального та кількісного складу користувачів, їх повноважень та рівня можливостей?
а) обстеження середовища користувачів
б) обстеження зовнішнього середовища
в) обстеження фізичного середовища
г) обстеження інформаційного середовища

56. Яке поняття визначає нездатність системи протистояти реалізації певної загрози або сукупності загроз?
а) відмова
б) вразливість
в) ризик
г) атака

57. Яке поняття визначає втрату здатності КС або її компонента виконувати певну функцію?
а) вразливість
б) загроза
в) атака
г) відмова

58. Об'єктами захисту інформації в інформаційно-комунікаційній системі є:

а) математичні методи побудови програмного забезпечення, що використовується в системі

б) інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації

в) технічні рішення, що використовуються для створення апаратури, яка утворює систему

г) апаратні рішення, використані при побудові системи

59. При обстеженні фізичного середовища здійснюється аналіз\:

а) інформації, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення)

б) взаємного розміщення засобів обробки інформації ІТС на об’єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів

в) ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз

г) структурної схеми і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо)

КРИТЕРІЇ ОЦІНЮВАННЯ УСПІШНОСТІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Національна шкала

Оцінка виставляється за національною чотирибальною шкалою: «відмінно», «добре», «задовільно», «незадовільно». При оцінці за основу слід брати повноту і правильність виконання завдань.

1. Оцінка «5» (відмінно) ставиться в тому разі, коли відповідь здобувача вищої освіти правильна, повна, послідовна, логічна; здобувач вищої освіти впевнено володіє фактичним матеріалом з усього курсу, вміє застосовувати його щодо конкретно поставлених завдань.

2. Оцінка «4» (добре) ставиться в тому разі, коли відповідь правильна, послідовна, логічна, але здобувач вищої освіти допускає у викладі окремі незначні пропуски фактичного матеріалу, вміє застосовувати його щодо конкретно поставлених завдань.

3. Оцінка «3» (задовільно) ставиться в тому разі, коли здобувач вищої освіти володіє більшою частиною фактичного матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, невірно формулює основні теоретичні положення та причинно-наслідкові зв'язки.

4. Оцінка «2» (незадовільно) ставиться в тому разі, коли здо-бувач вищої освіти виявляє незнання більшої частини фактичного матеріалу або здобувач вищої освіти відмовляється відповідати на поставлені питання.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно з можливістю	не зараховано з можливістю
0 – 34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ

Нормативно-правові акти:

1. Конституція України : Закон України від 28 черв. 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Кодекс України про адміністративні правопорушення: від 7 груд. 1984 р. №8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
3. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
4. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text
5. Про державну таємницю: Закон України від 21 січ. 1994 р. № 3855-XII URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
6. Про інформацію: Закон України від 02.10.1992 № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ СБУкраїни від 14 січня 2021 р. за № 52/35674. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text
8. Про Національну Поліцію: Закон України 2 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text
9. Про Службу безпеки України: Закон України від 25 бер. 1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text
10. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text
11. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994. Поточна редакція від 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
12. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова КМУ від 29.03.2006 № 373. Поточна редакція від 03.06.2022. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
13. Указ президента України «Про Положення про технічний захист інформації в Україні». URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text
14. Постанова Кабінету Міністрів України від 8 жовтня 1997 р. № 1126 «Про затвердження Концепції технічного захисту інформації в Україні». URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text
15. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу». URL: https://tzi.com.ua/downloads/1.1-002-99.pdf
16. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі». URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf
17. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні

роботи. [Чинний від 2007.12.12]. Київ, 2007. 12с. URL: https://tzi.com.ua/downloads/3.1-001-07.pdf

18.НД ТЗІ 2.5-004-99 Класифікація технічних каналів витоку інформації та основні заходи з їх блокування. [Чинний від 1999.04.28]. Київ, 1999. 60с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

19.НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 1999.04.28]. Київ, 1999. 21с. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf

20.Державна службу спеціального зв'язку та захисту інформації України - URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi.

21.ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. [Чинний від 1997.04.11]. Київ, 1997. 16с. URL: https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-3396.2-97.pdf

Основні джерела:

1. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності : навч. посіб. / Лаптєв О.А., Савченко В.А., Шуклін Г.В. К.: Державний університет телекомунікацій, 2020 126 с.

2. Здобуття доказової інформації в мережі Інтернет. В.К. Школьніков, Ю.Ю. Орлов та ін. К.: НАВС, 2019. 58 с.

3. Методи та засоби технічного захисту інформації. Опорний конспект лекцій : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: В. М. Луценко, Д. О. Прогонов. – Київ : КПІ ім. Ігоря Сікорського, 2021. 289 с.

4. Охорона державної таємниці та захист інформації: навч. посіб. В. С. Зачепило, З. А. Шандра, І. Р. Опірський та ін. ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». Львів : Вид-во Львівської політехніки, 2019. 168 с.

5. Організація охорони державної таємниці в Україні : навчальний посібник А. М. Супруненко, І. І. Башта, А. М. Лисеюк, К. С. Свіріна ; Університет державної фіскальної служби України. Ірпінь. УДФСУ, 2020. 370 с.

6. Самойленко О.А. Основи методики розслідування злочинів, вчиненихуу кіберпросторі: монографія / О. А. Самойленко ; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

Чердинцев Ю.Г. Адміністративно-правове регулювання режиму державної таємниці в Україні : дис. ... канд. юрид. наук. Одеса, 2020. 239 с.

Допоміжні джерела:

1. Zadereyko O., Trofymenko O., Prokop Y., Loginova N., Dyka A., Kukharenko S. Research of potential data leaks in information and communication systems. Radioelectronic and Computer Systems. 2022. No 4. P.64-84. URL: http://nti.khai.edu/ojs/index.php/reks/article/view/reks.2022.4.05

2. Домарєв В.В., Кухаренко С.В., Тімков В.Ф. Підхід щодо створення автоматизованих систем з комплексним захистом інформації // Сучасна спеціальна техніка, наук.-пр. журн. / Держ. н.-д. ін-т МВС України, Київ. 2021. № 1(64), С. 37-44.

3. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Аналіз витоків даних в інформаційних системах // Сучасна спеціальна техніка, наук.-пр. журн. / Держ. н.-д. ін-т МВС України, Київ. 2021. № 3(66), С. 16-30.

4. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов и др. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2019. 216 с.

5. Кухаренко С.В., Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І. Аналіз витоків даних в інформаційних системах // Сучасна спеціальна техніка, наук.-пр. журн. / Держ. н.-д. ін-т МВС України, Київ. 2021. № 3(66), С. 16-30.

6. Кухаренко С.В. Комплексна оцінка рівня захищеності автоматизованої системи. Сучасна спеціальна техніка, наук.-пр. журн. / Держ. н.-д. ін-т МВС України, Київ. 2021. № 2(65), С. 28-34.

7. Олійник В. І. Кримінально-правове, кримінологічне та кримінально-виконавче забезпечення охорони державної таємниці в Україні : дис. ... д-ра юрид. наук : 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» (081 – Право) / В. І. Олійник ; ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом». Київ, 2023. 473 с. URL : https://maup.com.ua/assets/files/dis/olijnik/olijnik-disertaciya.pdf

8. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці : монографія / О. Г. Корченко, О. Є. Архипов, Ю. О. Дрейс. Київ : Нац. акад. Служби безпеки України, 2014. 332 с. URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/5221/1/drey_ocin_2014_monog.pdf

9.

Навчальне видання

САМОЙЛЕНКО Олена Анатоліївна
КУХАРЕНКО Сергій Вікторович
МУРАШКО Анастасія Сергіївна

РЕЖИМ СЕКРЕТНОСТІ ТА ЗАХИСТ ІНФОРМАЦІЇ

методичні вказівки для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти ступеня бакалавра
в галузі знань – К «Безпека та оборона»
спеціальність – К9 «Правоохоронна діяльність»