МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Кафедра криміналістики, судових експертиз та поліграфології

КІБЕРБЕЗПЕКА
(підготовка до ЄДКІ)

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»/ F5 «Кібербезпека та захист інформації»

Одеса
2026

УДК: 007:004.056(073)

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
(*протокол № 5 від 24 червня 2026 р.*)

Укладачі:

Аркуша Лариса Ігорівна (ORCID ID https://orcid.org/0000-0002-0422-6416) – доктор юридичних наук, професор, завідувач кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»;

Чернов Олександр Віталійович (ORCID ID https://orcid.org/0009-0002-6038-9479) – доктор філософії, доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»;

Дикий Олег Вікторович (ORCID ID https://orcid.org/0000-0001-9659-9350) – кандидат юридичних наук, доцент, декан факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»;

Пишненко Ірина Юріївна (ORCID ID https://orcid.org/0009-0004-4380-7071) – асистент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія».

Рецензенти:

Соколов Артем Вікторович **–** доктор технічних наук, професор, завідувач спеціалізованою лабораторією «Кіберполігон», завідувач кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Лісніченко Дмитро Вікторович – кандидат юридичних наук, доцент, доцент кафедри кримінального процесу та криміналістики Одеського державного університету внутрішніх справ.

К381 **Кібербезпека (підготовка до ЄДКІ):** метод. вказівки для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»/ F5 «Кібербезпека та захист інформації» [Електронне видання] / укладачі: Л.І. Аркуша, О.В. Чернов, О.В. Дикий, І.Ю. Пишненко; Нац. ун-т «Одеська юрид. академія». Одеса : НУ«ОЮА», 2026. 88 с. URL: …

Методичні рекомендації призначені для здобувачів вищої освіти ступеня бакалавра, які навчаються спеціальністю 125 «Кібербезпека та захист інформації»/ F5 «Кібербезпека та захист інформації» на факультеті кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія». Матеріали спрямовані на формування системних теоретичних знань і практичних умінь у сфері забезпечення інформаційної та кібербезпеки, необхідних для виявлення та протидії кіберзагрозам, а також для захисту інформаційних ресурсів і інформаційно-комунікаційних систем.

Методичні рекомендації орієнтовані на розвиток у здобувачів здатності застосовувати сучасні технології кіберзахисту, аналізувати вразливості інформаційних систем і впроваджувати ефективні заходи захисту інформації. Посібник містить теоретичні матеріали, завдання до практичних занять і самостійної роботи, тестові завдання та питання для підсумкового контролю, що сприяють системному засвоєнню навчального матеріалу дисципліни «Кібербезпека (підготовка до ЄДКІ)» та формуванню професійних компетентностей майбутніх фахівців у сфері кібербезпеки.

УДК: 007:004.056(073)

ЗМІСТ

ВСТУП

Навчальна дисципліна «Кібербезпека (підготовка до ЄДКІ)» викладається здобувачам вищої освіти ступеня бакалавра факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія» у межах підготовки за галуззю знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації». Її зміст і спрямування визначаються необхідністю формування у майбутніх фахівців системного розуміння сучасних викликів у сфері кібербезпеки, засвоєння теоретичних основ і практичних механізмів захисту інформаційних систем, а також підготовки до складання єдиного державного кваліфікаційного іспиту, який є підсумковим етапом підтвердження професійної компетентності здобувачів вищої освіти у сфері інформаційної та кібернетичної безпеки.

В умовах стрімкої цифровізації суспільства, активного розвитку інформаційно-комунікаційних технологій, розширення глобального кіберпростору та зростання кількості кіберзагроз особливої актуальності набуває підготовка фахівців, здатних забезпечувати надійний захист інформаційних ресурсів, комп'ютерних систем і телекомунікаційних мереж. Сучасні кіберінциденти, спрямовані на державні інформаційні ресурси, критичну інфраструктуру, фінансові системи та приватний сектор, демонструють високий рівень організованості, технологічної складності та масштабності кіберзлочинності. У зв'язку з цим професійна підготовка майбутніх спеціалістів з кібербезпеки має бути орієнтована не лише на засвоєння фундаментальних теоретичних знань, але й на формування практичних компетентностей, необхідних для виявлення, аналізу та нейтралізації кіберзагроз у різних сегментах інформаційного середовища.

Концептуальною основою навчальної дисципліни є системне узагальнення ключових знань, що формуються у здобувачів протягом навчання за освітньою програмою, та їх інтеграція у комплекс компетентностей, необхідних для успішного складання єдиного державного кваліфікаційного іспиту. У межах дисципліни розглядаються фундаментальні засади інформаційної та кібернетичної безпеки, принципи побудови та функціонування захищених інформаційних систем, методи протидії кіберзагрозам, організаційні та технічні механізми захисту інформації, а також питання управління ризиками інформаційної безпеки. Особлива увага приділяється нормативно-правовому забезпеченню кібербезпеки, міжнародним стандартам та практикам захисту інформації, що визначають сучасні підходи до організації систем кіберзахисту в державному та приватному секторах.

Зміст дисципліни охоплює широкий спектр питань, пов'язаних із функціонуванням сучасних інформаційних систем і мереж, методами виявлення кіберінцидентів, аналізом вразливостей, організацією систем моніторингу безпеки, криптографічним захистом інформації, безпекою програмного забезпечення та мережевих технологій. Значна увага приділяється питанням кіберзахисту державних інформаційних ресурсів і критичної інформаційної інфраструктури, що набуває особливого значення в умовах воєнного стану та гібридних загроз у кіберпросторі. У цьому контексті підготовка майбутніх фахівців з кібербезпеки спрямована на формування здатності аналізувати складні кіберінциденти, оцінювати ризики інформаційної безпеки та розробляти ефективні заходи реагування на кіберзагрози.

Практична складова дисципліни орієнтована на систематизацію знань і відпрацювання навичок розв'язання типових тестових та ситуаційних завдань, що

відповідають структурі та змісту єдиного державного кваліфікаційного іспиту. У процесі підготовки здобувачі вищої освіти набувають умінь аналізувати комплексні завдання у сфері кібербезпеки, визначати найбільш ефективні методи захисту інформаційних систем, оцінювати потенційні загрози та застосовувати сучасні технологічні рішення для забезпечення інформаційної безпеки. Значна увага приділяється розвитку аналітичного мислення, здатності до системного аналізу кіберризиків та формування навичок прийняття обґрунтованих рішень у складних умовах інформаційного протистояння.

Таким чином, навчальна дисципліна «Кібербезпека (підготовка до ЄДКІ)» є важливою складовою професійної підготовки бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації». Вона спрямована на узагальнення та систематизацію отриманих знань, формування здатності комплексно оцінювати сучасні кіберзагрози та застосовувати ефективні механізми їх нейтралізації, а також на забезпечення належного рівня підготовки здобувачів вищої освіти до складання єдиного державного кваліфікаційного іспиту та подальшої професійної діяльності у сфері забезпечення інформаційної та кібернетичної безпеки.

Метою викладання навчальної дисципліни «Кібербезпека (підготовка до ЄДКІ)» є формування у здобувачів вищої освіти системних теоретичних знань і практичних умінь у сфері забезпечення інформаційної та кібернетичної безпеки, необхідних для ефективного функціонування сучасних інформаційно-комунікаційних систем, захисту інформаційних ресурсів від кіберзагроз та успішного складання єдиного державного кваліфікаційного іспиту за спеціальністю 125 «Кібербезпека та захист інформації». Дисципліна спрямована на узагальнення, систематизацію та поглиблення знань, здобутих протягом навчання за освітньою програмою, а також на формування здатності застосовувати ці знання для розв’язання комплексних професійних завдань у сфері кібербезпеки.

Зміст навчальної дисципліни орієнтований на інтеграцію фундаментальних теоретичних положень кібербезпеки, сучасних технологій захисту інформації та практичних підходів до протидії кіберзагрозам. У межах курсу розглядаються питання функціонування та захисту інформаційних систем і мереж, організації систем управління інформаційною безпекою, виявлення і аналізу кіберінцидентів, оцінювання вразливостей програмного забезпечення та мережевих ресурсів, застосування криптографічних методів захисту інформації, а також особливості забезпечення кіберзахисту державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури. Особлива увага приділяється сучасним міжнародним стандартам і практикам кіберзахисту, а також нормативно-правовим засадам функціонування національної системи кібербезпеки.

Навчальна дисципліна також спрямована на формування у здобувачів вищої освіти аналітичного мислення та здатності комплексно оцінювати сучасні кіберризики. Вивчення курсу передбачає розвиток умінь аналізувати складні кіберінциденти, визначати джерела потенційних загроз, оцінювати рівень захищеності інформаційних систем та розробляти ефективні заходи щодо попередження, локалізації та нейтралізації кіберзагроз. Важливим елементом дисципліни є формування здатності застосовувати сучасні методи моніторингу інформаційної безпеки, аналізу цифрових доказів та реагування на інциденти кібербезпеки.

Основними завданнями навчальної дисципліни «Кібербезпека (підготовка до ЄДКІ)» є:

- формування у здобувачів вищої освіти системного розуміння основних понять, принципів і категорій у сфері кібербезпеки, а також сучасних тенденцій розвитку інформаційних технологій та їх впливу на стан інформаційної безпеки;

- узагальнення та систематизація знань щодо архітектури інформаційних систем і мереж, механізмів їх функціонування та основних вразливостей, що можуть бути використані для здійснення кібернетичних атак;

- засвоєння сучасних підходів і методів забезпечення кібербезпеки, включаючи криптографічний захист інформації, безпеку мережевої інфраструктури, захист програмного забезпечення та організаційні механізми управління інформаційною безпекою;

- формування практичних умінь щодо виявлення, аналізу та реагування на кіберінциденти, а також оцінювання ризиків інформаційної безпеки у різних сегментах інформаційного середовища;

- набуття здатності аналізувати типові та комплексні тестові завдання, що відповідають структурі єдиного державного кваліфікаційного іспиту, та обґрунтовувати правильні рішення у сфері кіберзахисту;

- формування розуміння нормативно-правових засад забезпечення кібербезпеки на національному та міжнародному рівнях, а також принципів функціонування систем кіберзахисту держави;

- розвиток навичок системного аналізу кіберзагроз, прогнозування можливих сценаріїв кіберінцидентів і розроблення ефективних заходів протидії;

- формування здатності застосовувати отримані знання у практичній діяльності фахівця з кібербезпеки, зокрема у сфері захисту інформаційних систем, мережевих ресурсів і цифрових даних.

Опанування навчальної дисципліни передбачає відвідування лекційних і практичних занять, виконання самостійної роботи, опрацювання навчально-методичних матеріалів, а також систематичне розв’язання тестових і ситуаційних завдань, що відповідають структурі єдиного державного кваліфікаційного іспиту. Значна увага приділяється розвитку навичок практичного застосування знань у сфері кібербезпеки, зокрема під час аналізу реальних кіберінцидентів, моделювання сценаріїв кіберзагроз та оцінювання ефективності заходів кіберзахисту.

Після завершення вивчення дисципліни здобувачі вищої освіти повинні:

- розуміти основні принципи та концептуальні засади забезпечення кібербезпеки в сучасному інформаційному середовищі;

- знати нормативно-правові, організаційні та технологічні основи функціонування систем кіберзахисту;

- володіти методами виявлення, аналізу та попередження кіберзагроз;

- орієнтуватися у сучасних технологіях захисту інформації, включаючи криптографічні засоби, системи моніторингу безпеки та інструменти аналізу кіберінцидентів;

- уміти оцінювати рівень захищеності інформаційних систем і мереж та визначати потенційні вразливості;

- застосовувати знання з кібербезпеки під час розв’язання практичних і тестових завдань, що відповідають структурі єдиного державного кваліфікаційного іспиту;

- моделювати сценарії кіберзагроз і розробляти заходи щодо їх попередження та нейтралізації;

- інтегрувати отримані знання у подальшу професійну діяльність у сфері забезпечення інформаційної та кібернетичної безпеки.

Засвоєння навчальної дисципліни сприяє формуванню у майбутніх фахівців з кібербезпеки системного бачення проблем інформаційної безпеки, розвитку аналітичного та критичного мислення, здатності оперативно реагувати на сучасні кіберзагрози та

забезпечувати надійний захист інформаційних систем і ресурсів у різних сферах суспільної діяльності.

Технологія навчання з дисципліни «Кібербезпека (підготовка до ЄДКІ)» ґрунтується на поєднанні словесних, наочних та практичних методів навчання з домінуванням аналітико-практичної складової, що зумовлено прикладним характером дисципліни та її спрямованістю на систематизацію знань і формування професійних компетентностей у сфері забезпечення кібербезпеки. Освітній процес орієнтований на узагальнення теоретичних знань, здобутих у межах освітньої програми, а також на формування здатності застосовувати їх для розв'язання комплексних тестових і ситуаційних завдань, що відповідають структурі єдиного державного кваліфікаційного іспиту за спеціальністю 125 «Кібербезпека та захист інформації».

Словесні методи навчання, зокрема пояснення, консультації, аналіз типових помилок і обговорення складних теоретичних положень, забезпечують системне розуміння основних категорій, принципів і механізмів забезпечення кібербезпеки. Застосування цих методів сприяє формуванню у здобувачів вищої освіти здатності логічно аналізувати інформаційні процеси, інтерпретувати результати аналізу кіберінцидентів і аргументовано обґрунтовувати прийняті рішення щодо забезпечення інформаційної безпеки. Важливе значення має розбір типових тестових завдань, характерних для структури єдиного державного кваліфікаційного іспиту, що дозволяє сформувати у здобувачів вищої освіти системне розуміння логіки побудови контрольних завдань і підходів до їх розв'язання.

Наочні методи навчання реалізуються шляхом використання навчальних презентацій, схем функціонування інформаційних систем, моделей мережевої взаємодії, прикладів реальних кіберінцидентів, а також демонстрації принципів роботи сучасних засобів захисту інформації. Застосування візуальних матеріалів сприяє формуванню у здобувачів цілісного уявлення про архітектуру інформаційних систем, механізми виникнення кіберзагроз і технології їх виявлення та нейтралізації. Візуалізація складних інформаційних процесів і алгоритмів захисту інформації дозволяє значно підвищити ефективність засвоєння навчального матеріалу та сприяє розвитку системного мислення у сфері кібербезпеки.

Провідне місце в освітньому процесі посідають практичні методи навчання, що передбачають виконання тестових і ситуаційних завдань, аналіз кіберінцидентів, моделювання типових сценаріїв кіберзагроз і розроблення алгоритмів реагування на них. Практичні заняття спрямовані на формування навичок аналізу вразливостей інформаційних систем, оцінювання ризиків інформаційної безпеки, визначення можливих шляхів несанкціонованого доступу до інформаційних ресурсів і вибору ефективних заходів кіберзахисту. У процесі навчання значна увага приділяється формуванню здатності швидко орієнтуватися у складних інформаційних ситуаціях, приймати обґрунтовані рішення щодо забезпечення безпеки інформаційних систем та застосовувати сучасні технології кіберзахисту.

Важливою складовою навчального процесу є моделювання ситуацій кіберзагроз, що передбачає аналіз умов виникнення кіберінцидентів, визначення потенційних вразливостей інформаційної інфраструктури та відпрацювання алгоритмів реагування на кібернетичні атаки. Такий підхід дозволяє максимально наблизити освітній процес до умов реальної професійної діяльності фахівців з кібербезпеки та сприяє розвитку аналітичного мислення, здатності до системного аналізу інформаційних процесів і прийняття ефективних управлінських рішень у сфері кіберзахисту. Комплексне застосування зазначених методів навчання забезпечує підвищення рівня професійної підготовленості здобувачів вищої освіти, розвиток їхніх аналітичних та практичних навичок, а також формування готовності до

успішного складання єдиного державного кваліфікаційного іспиту та подальшої професійної діяльності у сфері кібербезпеки.

Оцінювання результатів навчання з дисципліни «Кібербезпека (підготовка до ЄДКІ)» здійснюється відповідно до вимог Положення про організацію освітнього процесу в Національному університеті «Одеська юридична академія». Контроль рівня засвоєння навчального матеріалу передбачає використання поточного та підсумкового оцінювання, спрямованого на перевірку сформованості теоретичних знань, аналітичних умінь і практичних навичок у сфері забезпечення кібербезпеки. Особлива увага приділяється оцінюванню здатності здобувачів вищої освіти розв’язувати комплексні тестові завдання, що відповідають структурі та змісту єдиного державного кваліфікаційного іспиту, аналізувати ситуації кіберзагроз та обґрунтовувати ефективні рішення щодо забезпечення інформаційної безпеки.

ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№	Найменування теми	Аудиторна робота		Самостійна робота
		Лекції	Практичні заняття	
Тема 1.	Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки.	2	2	8
Тема 2.	Інформаційні технології в інформаційній та/ або кібербезпеці.	2	2	8
Тема 3.	Безпека інформаційно-комунікаційних систем.	4	2	12
Тема 4.	Комплексні системи захисту інформації.	2	2	8
Тема 5.	Управління інформаційною та/або кібербезпекою.	2	2	8
Тема 6.	Криптографічний захист інформації.	2	2	8
Тема 7.	Технічний захист інформації.	2	2	8
ВСЬОГО:		**16**	**14**	**60**

ТЕМА 1. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ.

Національне законодавство України у сфері інформаційної та кібербезпеки: система, структура та основні напрями правового регулювання.

Державна система забезпечення кібербезпеки в Україні: повноваження суб'єктів, механізми координації та нормативне забезпечення.

Міжнародно-правові стандарти та зобов'язання у сфері кібербезпеки: європейський і глобальний вимір.

Міжнародні та галузеві стандарти управління інформаційною безпекою: ISO/IEC, NIST, best practices і їх імплементація в діяльність організацій.

Стрімкий розвиток інформаційних технологій, глобальна цифровізація суспільства, широке впровадження мережевих сервісів, хмарних технологій та автоматизованих систем управління суттєво підвищили роль інформації як стратегічного ресурсу сучасної держави. У таких умовах питання забезпечення інформаційної та кібернетичної безпеки набувають особливої актуальності, оскільки інформаційна інфраструктура є важливою складовою функціонування державних інституцій, економічних систем, фінансових установ, енергетичних мереж, транспортних систем та інших сфер суспільного життя. Водночас зростання залежності від цифрових технологій супроводжується підвищенням рівня кіберзагроз, що проявляється у поширенні кіберзлочинності, кібершпигунства, кібератак на об'єкти критичної інфраструктури, а також у використанні інформаційних технологій як інструменту гібридного впливу на державу та суспільство.

У зв'язку з цим формування ефективної системи правового регулювання у сфері інформаційної та кібернетичної безпеки є одним із ключових завдань сучасної державної політики. Законодавча та нормативно-правова база у цій сфері визначає основні принципи функціонування системи кібербезпеки, встановлює правила діяльності суб'єктів інформаційних відносин, визначає механізми захисту інформаційних ресурсів і регламентує порядок реагування на кіберзагрози.

Інформаційна безпека розглядається як складова національної безпеки держави і охоплює комплекс правових, організаційних, технічних та технологічних заходів, спрямованих на забезпечення захисту інформації, інформаційних ресурсів, інформаційно-комунікаційних систем та мереж від несанкціонованого доступу, витоку, знищення, модифікації або блокування інформації. Забезпечення належного рівня інформаційної безпеки передбачає створення ефективної системи правового регулювання, що визначає права, обов'язки та відповідальність усіх суб'єктів інформаційних відносин[1].

Основу національної системи правового регулювання у сфері інформаційної безпеки становлять положення Конституції України. Основний Закон держави гарантує кожному право на інформацію, право на захист персональних даних, недоторканність приватного життя, а також визначає принципи свободи інформаційної діяльності. Водночас Конституція України передбачає можливість обмеження доступу до інформації у випадках, коли це необхідно для захисту національної безпеки, територіальної цілісності або громадського порядку.

На основі конституційних положень сформовано систему спеціалізованого законодавства, що регламентує різні аспекти інформаційної безпеки та кіберзахисту. Одним

1 Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

із ключових нормативно-правових актів у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України». Цей закон визначає правові та організаційні основи функціонування національної системи кібербезпеки, встановлює принципи державної політики у сфері кіберзахисту, а також визначає коло суб'єктів, відповідальних за забезпечення кібербезпеки держави.

Національна система кібербезпеки України включає низку державних органів, які виконують спеціалізовані функції у сфері захисту кіберпростору. До таких органів належать Рада національної безпеки і оборони України, яка координує діяльність органів виконавчої влади у сфері національної безпеки; Кабінет Міністрів України, що забезпечує реалізацію державної політики у сфері кібербезпеки; Служба безпеки України, яка здійснює контррозвідувальну діяльність у кіберпросторі; Державна служба спеціального зв'язку та захисту інформації України, що відповідає за технічний та криптографічний захист інформації; Національна поліція України, яка здійснює боротьбу з кіберзлочинністю; Міністерство оборони України, що забезпечує кіберзахист у сфері оборони; а також інші державні органи, діяльність яких пов'язана із захистом інформаційної інфраструктури.

Законодавче регулювання інформаційної безпеки в Україні також здійснюється через низку спеціалізованих законів. Зокрема, Закон України «Про інформацію» визначає правові основи інформаційних відносин, встановлює принципи доступу до інформації, її поширення та використання. Закон України «Про захист інформації в інформаційно-комунікаційних системах» регламентує порядок організації системи технічного та криптографічного захисту інформації у державних і приватних інформаційних системах.

Важливе значення для забезпечення інформаційної безпеки має Закон України «Про державну таємницю», який визначає порядок віднесення інформації до державної таємниці, правила її обробки, зберігання та передачі. Закон України «Про захист персональних даних» встановлює правові засади обробки персональних даних та визначає права суб'єктів персональних даних.

У структурі правового регулювання кібербезпеки важливу роль відіграють також підзаконні нормативно-правові акти, серед яких укази Президента України, постанови Кабінету Міністрів України, нормативні акти центральних органів виконавчої влади. Значну роль у цій сфері відіграють нормативні документи Державної служби спеціального зв'язку та захисту інформації України, які регламентують порядок створення та функціонування систем технічного і криптографічного захисту інформації, а також встановлюють вимоги до комплексних систем захисту інформації.

Особливе місце у системі кібербезпеки займає питання захисту критичної інформаційної інфраструктури. Під об'єктами критичної інформаційної інфраструктури розуміються інформаційні системи та мережі, порушення функціонування яких може призвести до значних негативних наслідків для національної безпеки, економіки або життєдіяльності населення. До таких об'єктів належать системи енергетики, банківської сфери, транспортної інфраструктури, телекомунікаційних мереж, системи управління водопостачанням та інші важливі об'єкти[2].

Захист таких об'єктів передбачає впровадження спеціальних організаційних і технічних заходів, регулярне проведення аудитів інформаційної безпеки, створення центрів реагування на кіберінциденти та запровадження систем моніторингу кіберзагроз.

З огляду на глобальний характер кіберпростору забезпечення кібербезпеки не може здійснюватися виключно на національному рівні. Ефективна протидія кіберзлочинності та кіберзагрозам потребує міжнародного співробітництва, обміну інформацією між державами та гармонізації правових стандартів у сфері кібербезпеки.

Одним із ключових міжнародних документів у сфері кібербезпеки є Конвенція Ради Європи про кіберзлочинність, відома як Будапештська конвенція. Цей міжнародний договір визначає правові механізми криміналізації кіберзлочинів, встановлює процедури

2 Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

міжнародного співробітництва у сфері розслідування кіберзлочинності та регламентує порядок обміну інформацією між правоохоронними органами різних держав.

Важливу роль у формуванні міжнародної політики у сфері кібербезпеки відіграють міжнародні організації, зокрема Організація Об'єднаних Націй, Європейський Союз, НАТО, Рада Європи та інші міжнародні структури. У межах цих організацій розробляються міжнародні стратегії кібербезпеки, рекомендації щодо захисту інформаційної інфраструктури, а також стандарти безпеки інформаційних систем.

Одним із найбільш поширених міжнародних стандартів у сфері інформаційної безпеки є серія стандартів ISO/IEC 27000, що визначає вимоги до систем управління інформаційною безпекою. Зокрема стандарт ISO/IEC 27001 встановлює вимоги до створення, впровадження та підтримки систем управління інформаційною безпекою в організаціях. Він передбачає системний підхід до управління ризиками інформаційної безпеки, включаючи ідентифікацію загроз, оцінювання вразливостей та впровадження відповідних заходів контролю.

Крім стандартів ISO, важливе значення мають стандарти Національного інституту стандартів і технологій США, зокрема NIST Cybersecurity Framework. Цей документ визначає методологію управління ризиками кібербезпеки та містить рекомендації щодо захисту інформаційних систем.

У практиці забезпечення кібербезпеки також широко застосовуються галузеві стандарти, зокрема стандарт PCI DSS, що регламентує вимоги до захисту платіжних систем, а також рекомендації Європейського агентства з кібербезпеки.

Важливим напрямом розвитку сучасної системи кібербезпеки є впровадження ризик-орієнтованого підходу до управління інформаційною безпекою. Такий підхід передбачає систематичний аналіз загроз і вразливостей, оцінювання потенційних ризиків для інформаційних систем та розроблення ефективних заходів їх мінімізації.

Отже, законодавча та нормативно-правова база у сфері інформаційної та кібернетичної безпеки має комплексний характер і включає національне законодавство, підзаконні нормативні акти, міжнародні договори, а також стандарти і рекомендації міжнародних організацій. Її ефективне функціонування є важливою умовою забезпечення стабільності інформаційного простору, захисту державних інформаційних ресурсів, критичної інфраструктури та прав громадян у цифровому середовищі.

Практичне заняття 1.
Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Поняття інформаційної та кібернетичної безпеки в системі національної безпеки держави та їх правове регулювання.

2. Основні принципи державної політики України у сфері інформаційної та кібербезпеки.

3. Нормативно-правова база України у сфері захисту інформації та кіберзахисту інформаційно-комунікаційних систем.

4. Суб'єкти національної системи кібербезпеки України та їх повноваження.

5. Правові засади забезпечення захисту інформації в інформаційно-комунікаційних системах.

6. Роль міжнародного співробітництва у сфері протидії кіберзлочинності та забезпечення кібербезпеки.

7. Міжнародні стандарти управління інформаційною безпекою та їх значення для формування національної системи кіберзахисту.

8. Значення міжнародних організацій та стандартів у формуванні сучасної системи кібербезпеки

II. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Законодавчі основи формування системи кібербезпеки України.

2. Система державного управління у сфері інформаційної та кібербезпеки в Україні.

3. Правові засади захисту інформації в інформаційно-комунікаційних системах.

4. Особливості правового регулювання захисту критичної інформаційної інфраструктури.

5. Міжнародно-правові механізми протидії кіберзлочинності.

6. Стандарти ISO/IEC у сфері управління інформаційною безпекою та їх практичне застосування.

7. Роль міжнародних організацій у формуванні глобальної системи кібербезпеки.

8. Ризик-орієнтований підхід до управління інформаційною безпекою відповідно до міжнародних стандартів.

III. Розв’язати тестові завдання:

1. Який закон визначає правові та організаційні засади функціонування національної системи кібербезпеки України?

А) Закон України «Про інформацію»

Б) Закон України «Про основні засади забезпечення кібербезпеки України»

В) Закон України «Про захист прав споживачів»

Г) Закон України «Про національну поліцію»

2. Інформаційна безпека є складовою:

А) економічної безпеки

Б) національної безпеки

В) екологічної безпеки

Г) соціальної політики

3. Який закон регламентує захист інформації в інформаційно-комунікаційних системах?

А) Закон України «Про захист інформації в інформаційно-комунікаційних системах»

Б) Закон України «Про інформацію»

В) Закон України «Про доступ до публічної інформації»

Г) Закон України «Про державну службу»

4. Який орган в Україні забезпечує технічний і криптографічний захист інформації?

А) Національна поліція України

Б) Служба безпеки України

В) Державна служба спеціального зв’язку та захисту інформації України

Г) Міністерство оборони України

5. Який міжнародний стандарт визначає вимоги до системи управління інформаційною безпекою?

А) ISO 9001

Б) ISO 27001

В) ISO 14001

Г) ISO 31000

6. Яка міжнародна конвенція є ключовим документом у сфері боротьби з кіберзлочинністю?

А) Женевська конвенція

Б) Будапештська конвенція про кіберзлочинність

В) Гаазька конвенція

Г) Віденська конвенція

7. Який стандарт застосовується для забезпечення безпеки платіжних карткових систем?

А) ISO 27001

Б) PCI DSS

В) ISO 31000

Г) COBIT

8. Основною метою системи управління інформаційною безпекою є:

А) зменшення кількості інформаційних систем

Б) управління ризиками інформаційної безпеки

В) обмеження доступу до інформації

Г) створення нових інформаційних ресурсів

9. Кіберзлочини в Україні розслідує спеціалізований підрозділ:

А) Служби безпеки України

Б) Державної служби спеціального зв’язку

В) Кіберполіції Національної поліції України

Г) Міністерства цифрової трансформації

10. До критичної інформаційної інфраструктури належать:

А) лише державні вебсайти

Б) інформаційні системи, порушення функціонування яких може призвести до значних негативних наслідків для держави або суспільства

В) усі приватні інформаційні системи

Г) лише телекомунікаційні мережі

11. Підприємство енергетичного сектору впроваджує систему управління інформаційною безпекою відповідно до міжнародних стандартів. Який стандарт найбільш безпосередньо визначає вимоги до такої системи?

А) ISO 9001

Б) ISO/IEC 27001

В) ISO 22000
Г) ISO 14001

12. Під час аудиту інформаційної безпеки виявлено, що організація не здійснює системного аналізу загроз та вразливостей інформаційної системи. Який підхід до управління безпекою порушено?
А) адміністративний
Б) ризик-орієнтований
В) функціональний
Г) процесний

13. Міжнародна компанія працює з платіжними картками клієнтів і повинна забезпечити захист відповідної інформації. Який стандарт є обов'язковим для таких систем?
А) ISO 27001
Б) PCI DSS
В) NIST CSF
Г) COBIT

14. У державній установі здійснюється обробка інформації з обмеженим доступом. Який нормативно-правовий акт регламентує порядок віднесення інформації до державної таємниці?
А) Закон України «Про інформацію»
Б) Закон України «Про державну таємницю»
В) Закон України «Про захист персональних даних»
Г) Закон України «Про телекомунікації»

15. У ході міжнародного розслідування кіберзлочину виникла необхідність обміну електронними доказами між державами. Який міжнародний документ регламентує таке співробітництво?
А) Будапештська конвенція про кіберзлочинність
Б) Женевська конвенція
В) Паризька угода
Г) Римський статут

16. Організація впроваджує модель управління кіберризиками, що передбачає ідентифікацію загроз, оцінювання вразливостей і вибір заходів контролю. Який міжнародний підхід реалізується?
А) NIST Cybersecurity Framework
Б) ITIL
В) Six Sigma
Г) Agile

17. Внаслідок кібератаки було порушено роботу систем управління енергетичною мережею. До якої категорії об'єктів належить така система?
А) об'єктів державної власності
Б) об'єктів критичної інформаційної інфраструктури

В) інформаційних ресурсів загального користування
Г) приватних інформаційних систем

18. Державний орган планує створити систему моніторингу кіберінцидентів та реагування на них. Який підрозділ у національній системі кібербезпеки України відіграє ключову роль у координації технічного реагування на кіберзагрози?
А) CERT-UA
Б) Державна аудиторська служба
В) Антимонопольний комітет
Г) Національний банк України

19. Організація застосовує міжнародний стандарт, що передбачає безперервний цикл управління безпекою, який включає планування, впровадження, перевірку та вдосконалення заходів захисту інформації. Яку модель використано?
А) PDCA
Б) SWOT
В) PEST
Г) SMART

20. Державний орган розробляє систему кіберзахисту, що відповідає міжнародним практикам управління ризиками інформаційної безпеки. Яка головна мета такого підходу?
А) повна ізоляція інформаційної системи
Б) мінімізація кіберризиків до прийнятного рівня
В) заборона використання мережі Інтернет
Г) зменшення кількості користувачів інформаційної системи

Методичні рекомендації

Опрацювання теми, присвяченої законодавчій та нормативно-правовій базі, державним і міжнародним вимогам, практикам та стандартам у сфері інформаційної та кібербезпеки, є важливим етапом формування професійної компетентності здобувачів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». Розуміння правових засад функціонування системи кібербезпеки дозволяє майбутнім фахівцям орієнтуватися у нормативному регулюванні діяльності у сфері захисту інформації, усвідомлювати роль державних інституцій у забезпеченні кіберзахисту та застосовувати міжнародні стандарти й практики управління інформаційною безпекою.

Під час вивчення цієї теми здобувачам вищої освіти доцільно приділити особливу увагу системі національного законодавства у сфері інформаційної та кібербезпеки. Передусім необхідно проаналізувати основні положення Конституції України, які визначають право громадян на інформацію, захист персональних даних та недоторканність приватного життя. Важливим елементом опрацювання теми є вивчення базових законодавчих актів, що регулюють сферу інформаційних відносин і кіберзахисту, зокрема законів України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про державну таємницю», а також інших нормативно-правових актів, що визначають механізми забезпечення інформаційної безпеки.

Значну увагу необхідно приділити аналізу функцій і повноважень суб'єктів національної системи кібербезпеки України. Здобувачі повинні чітко розуміти роль і компетенцію таких органів, як Рада національної безпеки і оборони України, Кабінет Міністрів України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України та інших органів, які беруть участь у формуванні та реалізації державної політики у сфері кібербезпеки. Особливу увагу слід приділити питанням захисту критичної інформаційної інфраструктури та організації реагування на кіберінциденти.

Під час самостійної роботи здобувачам доцільно проаналізувати міжнародні нормативні акти та документи, що регулюють співробітництво у сфері кібербезпеки. Особливе значення має вивчення положень Конвенції Ради Європи про кіберзлочинність, відомої як Будапештська конвенція, яка визначає міжнародні механізми боротьби з кіберзлочинністю та співробітництва між державами у сфері розслідування кіберінцидентів. Необхідно також ознайомитися з діяльністю міжнародних організацій, таких як Організація Об'єднаних Націй, Європейський Союз, НАТО та інші інституції, які формують міжнародну політику у сфері кібербезпеки.

Окремим напрямом вивчення теми є опрацювання міжнародних стандартів і практик управління інформаційною безпекою. Здобувачам слід звернути увагу на стандарти серії ISO/IEC 27000, зокрема стандарт ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою, а також інші міжнародні документи, що регламентують управління кіберризиками, зокрема NIST Cybersecurity Framework. Важливим є розуміння ризик-орієнтованого підходу до забезпечення інформаційної безпеки, який передбачає системний аналіз загроз, оцінювання вразливостей інформаційних систем та впровадження відповідних заходів захисту.

У процесі підготовки до практичних занять здобувачам рекомендується опрацювати відповідні законодавчі акти, міжнародні документи та стандарти, звернувши увагу на їх структуру, основні принципи та механізми реалізації. Доцільно також проаналізувати практичні приклади застосування міжнародних стандартів у сфері інформаційної безпеки, що дозволить сформувати цілісне уявлення про сучасні підходи до організації систем кіберзахисту.

Ефективним методом засвоєння матеріалу є порівняльний аналіз національних і міжнародних підходів до забезпечення кібербезпеки. Такий підхід дозволяє виявити спільні принципи та відмінності у правовому регулюванні інформаційної безпеки, а також оцінити перспективи розвитку національного законодавства у цій сфері.

Під час підготовки до підсумкового контролю здобувачам рекомендується систематизувати отримані знання, звертаючи увагу на ключові поняття, принципи функціонування системи кібербезпеки, структуру національної системи кіберзахисту, міжнародні стандарти управління інформаційною безпекою та механізми міжнародного співробітництва у сфері протидії кіберзлочинності.

Опрацювання цієї теми сприяє формуванню у здобувачів системного розуміння правових і організаційних засад забезпечення інформаційної та кібернетичної безпеки, розвитку аналітичного мислення та здатності застосовувати міжнародні стандарти і національне законодавство у практичній діяльності фахівця з кібербезпеки. Такі знання є необхідними для подальшої професійної діяльності у сфері захисту інформаційних систем, управління інформаційними ризиками та протидії сучасним кіберзагрозам, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-Київ, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 1
Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки.

1. Що розуміється під інформаційною та кібернетичною безпекою і яке їх місце у системі національної безпеки держави?

2. Які конституційні норми України гарантують право на інформацію та захист інформаційної безпеки?

3. Які основні положення та принципи визначає Закон України «Про основні засади забезпечення кібербезпеки України»?

4. Які органи державної влади входять до національної системи кібербезпеки України та які їх основні повноваження?

5. Які нормативно-правові акти регулюють захист інформації в інформаційно-комунікаційних системах?

6. Які правові механізми забезпечують захист персональних даних та інформації з обмеженим доступом?

7. Що належить до об’єктів критичної інформаційної інфраструктури та які особливості їх захисту?

8. Яке значення має міжнародне співробітництво у сфері кібербезпеки та які основні положення Будапештської конвенції про кіберзлочинність?

9. Які міжнародні стандарти управління інформаційною безпекою використовуються у сучасній практиці кіберзахисту?

10. У чому полягає ризик-орієнтований підхід до забезпечення інформаційної безпеки та як він реалізується у міжнародних стандартах?

ТЕМА 2. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ.

Інформаційні системи, мережі та цифрова інфраструктура як об'єкти забезпечення інформаційної та кібербезпеки.

Технології захисту інформації та кіберзахисту в сучасних інформаційно-комунікаційних системах.

Інформаційні технології моніторингу, виявлення та реагування на кіберінциденти.

Перспективні цифрові технології та їх вплив на стан інформаційної й кібербезпеки.

Розвиток інформаційних технологій у сучасному світі істотно трансформував усі сфери суспільного життя, включаючи економічні процеси, державне управління, банківську систему, систему національної безпеки, транспорт, медицину, освіту та інші сфери діяльності. Цифровізація суспільства сприяла створенню нових інформаційних ресурсів, електронних сервісів та глобальних інформаційно-комунікаційних мереж, які забезпечують швидкий обмін інформацією та ефективне функціонування сучасних інформаційних систем. У таких умовах інформаційні технології стали ключовим інструментом формування інформаційного суспільства, в якому інформація виступає стратегічним ресурсом розвитку держави та суспільства.

Разом із розширенням використання інформаційних технологій значно зростає і рівень загроз, пов'язаних із функціонуванням інформаційних систем. Кіберзлочинність, несанкціонований доступ до інформаційних ресурсів, шкідливе програмне забезпечення, інформаційні атаки та інші загрози становлять серйозну небезпеку для стабільності інформаційної інфраструктури. У зв'язку з цим важливого значення набуває забезпечення інформаційної та кібернетичної безпеки, що передбачає застосування сучасних технологічних рішень для захисту інформації, інформаційних систем і комп'ютерних мереж.

Інформаційні технології в інформаційній та кібербезпеці являють собою сукупність технічних, програмних і організаційних засобів, що забезпечують захист інформації від різноманітних загроз. До таких загроз належать несанкціонований доступ до інформації, її знищення, блокування, модифікація або копіювання, а також інші форми протиправного втручання у функціонування інформаційних систем[3]. Основною метою використання інформаційних технологій у сфері кібербезпеки є забезпечення трьох базових принципів інформаційної безпеки: конфіденційності, цілісності та доступності інформації.

Конфіденційність інформації означає, що доступ до інформаційних ресурсів мають лише уповноважені користувачі. Для реалізації цього принципу використовуються різноманітні технології управління доступом до інформації. До таких технологій належать системи автентифікації користувачів, які дозволяють перевіряти їхню особу під час входу до інформаційної системи, системи авторизації, що визначають рівень доступу користувача до певних інформаційних ресурсів, а також системи управління ідентифікацією користувачів.

Однією з найбільш поширених сучасних технологій захисту інформації є багатофакторна автентифікація. Вона передбачає використання декількох незалежних факторів перевірки особи користувача, таких як пароль, одноразовий код, біометричні дані або спеціальний апаратний токен. Застосування багатофакторної автентифікації значно підвищує рівень захисту інформаційних систем, оскільки навіть у разі компрометації одного з факторів доступ до інформації залишається захищеним.

---

3 Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

Важливим компонентом інформаційної безпеки є забезпечення цілісності інформації. Цілісність означає, що інформація повинна залишатися незмінною під час її зберігання, обробки та передачі, якщо такі зміни не були санкціоновані уповноваженими користувачами. Для забезпечення цілісності інформації застосовуються спеціальні програмні та криптографічні засоби, які дозволяють контролювати зміни у даних та виявляти спроби несанкціонованого втручання.

До таких технологій належать криптографічні хеш-функції, які дозволяють створювати унікальні цифрові відбитки даних, а також цифрові підписи, що забезпечують підтвердження автентичності інформації та її автора. Крім того, широко використовуються системи контролю цілісності файлів, які дозволяють автоматично перевіряти, чи не було змінено важливі файли операційної системи або програмного забезпечення.

Третім ключовим принципом інформаційної безпеки є доступність інформації. Доступність означає, що інформаційні ресурси повинні бути доступними для користувачів у той момент, коли вони потребують доступу до них. Для забезпечення доступності використовуються різноманітні технології, зокрема системи резервного копіювання даних, відмовостійкі серверні системи, системи балансування навантаження та системи захисту від атак типу відмова в обслуговуванні.

Особливо важливу роль відіграють технології резервного копіювання інформації. Регулярне створення резервних копій дозволяє відновити інформацію у разі її втрати внаслідок технічних збоїв, кібернетичних атак або інших надзвичайних ситуацій. Сучасні системи резервного копіювання використовують як локальні сховища даних, так і хмарні сервіси, що забезпечують додатковий рівень захисту інформаційних ресурсів.

Суттєве значення у системі інформаційної безпеки мають технології моніторингу інформаційних систем. До таких технологій належать системи управління інформаційною безпекою, системи моніторингу подій інформаційної безпеки, системи виявлення вторгнень та системи запобігання вторгненням. Ці технології дозволяють аналізувати події, що відбуваються у комп'ютерних мережах, виявляти підозрілу активність та оперативно реагувати на можливі кіберзагрози.

Системи виявлення вторгнень призначені для аналізу мережевого трафіку та виявлення ознак несанкціонованого доступу або інших кібернетичних атак. Системи запобігання вторгненням виконують більш активну роль, оскільки вони не лише виявляють загрози, але й автоматично блокують підозрілу активність у мережі.

Особливе місце у системі інформаційної безпеки займають криптографічні технології. Криптографія використовується для забезпечення конфіденційності інформації шляхом її шифрування, що робить інформацію недоступною для сторонніх осіб без відповідного ключа дешифрування. Криптографічні технології широко застосовуються у банківській сфері, електронній комерції, електронному документообігу, захисті електронної пошти та інших сферах діяльності[4].

З розвитком сучасних цифрових технологій з'являються нові типи інформаційних систем, такі як хмарні обчислення, мобільні платформи та системи інтернету речей. Хмарні технології дозволяють організаціям зберігати великі обсяги інформації у віддалених дата-центрах та отримувати доступ до них через мережу Інтернет. Однак використання хмарних технологій також створює нові ризики для інформаційної безпеки, пов'язані з можливістю несанкціонованого доступу до даних або порушенням конфіденційності інформації.

Системи інтернету речей також створюють нові виклики для забезпечення кібербезпеки. Такі системи об'єднують велику кількість пристроїв, які обмінюються інформацією через мережу Інтернет. У разі недостатнього рівня захисту такі пристрої можуть стати об'єктом кібернетичних атак або бути використані для здійснення масових мережевих атак.

---

4 Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

Важливим напрямом розвитку інформаційних технологій у сфері кібербезпеки є використання технологій штучного інтелекту та машинного навчання. Ці технології дозволяють автоматизувати процеси аналізу великих обсягів інформації, виявляти аномалії у функціонуванні інформаційних систем та прогнозувати можливі кіберзагрози. Використання алгоритмів машинного навчання дозволяє створювати інтелектуальні системи кіберзахисту, здатні адаптуватися до нових типів кібернетичних атак.

Крім того, значну роль у забезпеченні інформаційної безпеки відіграють технології цифрової криміналістики. Цифрова криміналістика включає методи збору, аналізу та збереження цифрових доказів, які можуть використовуватися у процесі розслідування кіберзлочинів. Використання спеціалізованих програмних засобів дозволяє відновлювати видалені файли, аналізувати мережеву активність, встановлювати джерела кібернетичних атак та виявляти осіб, причетних до протиправної діяльності.

У сучасних умовах забезпечення інформаційної безпеки передбачає створення комплексних систем захисту інформації, які поєднують організаційні, технічні та програмні заходи. Такі системи повинні забезпечувати багаторівневий захист інформаційної інфраструктури, включаючи захист мережевих комунікацій, серверів, баз даних, програмного забезпечення та користувацьких пристроїв.

Отже, інформаційні технології відіграють ключову роль у забезпеченні інформаційної та кібернетичної безпеки сучасного суспільства. Використання сучасних технологічних рішень дозволяє створювати ефективні механізми захисту інформаційних систем, протидіяти кіберзагрозам та забезпечувати стабільне функціонування інформаційної інфраструктури держави. Ефективне застосування інформаційних технологій у сфері кібербезпеки є важливою умовою розвитку інформаційного суспільства та забезпечення національної безпеки.

Практичне заняття 2
Інформаційні технології в інформаційній та/або кібербезпеці.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Поняття та класифікація інформаційних технологій у сфері інформаційної та кібербезпеки.
2. Принципи конфіденційності, цілісності та доступності інформації у сучасних інформаційних системах.
3. Технології управління ідентифікацією та доступом користувачів в інформаційних системах.
4. Технології моніторингу та аналізу подій інформаційної безпеки.
5. Системи виявлення та запобігання вторгненням у комп’ютерних мережах.
6. Технології резервного копіювання та відновлення інформаційних ресурсів.
7. Інформаційні технології забезпечення безпеки мережевої інфраструктури.
8. Технологічні засоби захисту інформації в умовах розвитку хмарних сервісів та інтернету речей.

ІІ. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Інформаційні технології як складова системи забезпечення інформаційної безпеки.
2. Технології криптографічного захисту інформації у сучасних інформаційних системах.

3. Використання технологій багатофакторної автентифікації у системах кіберзахисту.

4. Системи управління інформаційною безпекою та їх роль у захисті інформаційних ресурсів.

5. Використання технологій штучного інтелекту у сфері кібербезпеки.

6. Технології цифрової криміналістики у розслідуванні кіберзлочинів.

7. Забезпечення кібербезпеки хмарних інформаційних систем.

8. Технології захисту інформаційних систем від мережевих атак.

ІІІ. Розв'язати тестові завдання:

1. Який принцип інформаційної безпеки передбачає обмеження доступу до інформації лише для уповноважених осіб?

А) Доступність

Б) Цілісність

В) Конфіденційність

Г) Стабільність

2. Яка технологія використовується для підтвердження особи користувача під час входу до інформаційної системи?

А) Аутентифікація

Б) Архівація

В) Віртуалізація

Г) Реплікація

3. Який метод забезпечує перевірку незмінності даних?

А) Хешування

Б) Архівування

В) Балансування

Г) Дефрагментація

4. Яка технологія передбачає використання кількох способів перевірки особи користувача?

А) Мережевий моніторинг

Б) Багатофакторна автентифікація

В) Реплікація даних

Г) Віртуалізація

5. Яка система призначена для виявлення несанкціонованого доступу до мережі?

А) IDS

Б) DNS

В) DHCP

Г) FTP

6. Яка система не лише виявляє, але й блокує мережеві атаки?

А) IPS

Б) VPN

В) DNS

Г) SMTP

7. Яка технологія використовується для створення резервних копій даних?
А) Backup
Б) Encryption
В) Authentication
Г) Routing

8. Який метод захисту інформації полягає у перетворенні даних у зашифрований вигляд?
А) Шифрування
Б) Архівування
В) Кодування
Г) Реплікація

9. Який тип атак спрямований на перевантаження сервера великою кількістю запитів?
А) SQL Injection
Б) DDoS
В) Phishing
Г) Spoofing

10. Яка технологія дозволяє безпечно передавати дані через публічні мережі?
А) VPN
Б) FTP
В) HTTP
Г) SMTP

11. Організація впровадила систему, що аналізує мережевий трафік та виявляє підозрілу активність без автоматичного блокування атак. Який тип системи використовується?
А) IDS
Б) IPS
В) Firewall
Г) VPN

12. Під час перевірки безпеки інформаційної системи встановлено, що користувачі мають доступ лише до тих ресурсів, які необхідні для виконання їхніх службових обов’язків. Який принцип реалізовано?
А) принцип мінімальних привілеїв
Б) принцип резервування
В) принцип масштабованості
Г) принцип сумісності

13. Компанія використовує систему аналізу журналів подій безпеки з різних серверів та мережевих пристроїв для централізованого виявлення кіберінцидентів. Який тип технології використовується?

А) SIEM
Б) VPN
В) RAID
Г) NAT

14. Під час передачі інформації між сервером і клієнтом використовується криптографічний протокол, що забезпечує шифрування мережевого з’єднання. Який це протокол?
А) HTTPS
Б) FTP
В) Telnet
Г) SNMP

15. У системі безпеки використовується алгоритм, що аналізує мережеву активність і визначає відхилення від нормальної поведінки системи. Яка технологія застосовується?
А) машинне навчання
Б) віртуалізація
В) дефрагментація
Г) компресія

16. Під час кібератаки зловмисник намагається отримати доступ до бази даних через вебформу, вводячи спеціально сформовані запити. Який тип атаки здійснюється?
А) SQL Injection
Б) Phishing
В) DDoS
Г) Spoofing

17. Організація використовує технологію, що дозволяє створювати ізольовані віртуальні середовища на одному фізичному сервері. Яка це технологія?
А) Віртуалізація
Б) Реплікація
В) Архівація
Г) Шифрування

18. Під час аудиту безпеки встановлено, що інформаційна система здатна автоматично відновлювати дані після збою за допомогою резервних копій. Яку властивість інформаційної безпеки це забезпечує?
А) доступність
Б) конфіденційність
В) цілісність
Г) автентичність

19. У великій організації застосовується система, що дозволяє централізовано керувати правами доступу користувачів до інформаційних ресурсів. Яка технологія використовується?
А) IAM (Identity and Access Management)

Б) DNS
В) SMTP
Г) FTP

20. Під час аналізу кіберінциденту спеціалісти використовують програмні інструменти для відновлення видалених файлів і дослідження цифрових доказів. До якої галузі належить така діяльність?
А) цифрова криміналістика
Б) мережеве адміністрування
В) програмування
Г) системне тестування

Методичні рекомендації

Опрацювання теми, присвяченої інформаційним технологіям у сфері інформаційної та кібербезпеки, має важливе значення для формування професійної компетентності здобувачів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». Сучасні інформаційні технології є основою функціонування інформаційних систем, комп'ютерних мереж та цифрових сервісів, тому їх ефективне використання безпосередньо пов'язане із забезпеченням належного рівня захисту інформаційних ресурсів. Вивчення цієї теми спрямоване на формування у здобувачів системного розуміння технологічних засобів забезпечення інформаційної безпеки, принципів їх функціонування та можливостей практичного застосування для протидії сучасним кіберзагрозам.

Під час вивчення теми здобувачам необхідно зосередити увагу на основних принципах інформаційної безпеки, зокрема на забезпеченні конфіденційності, цілісності та доступності інформації. Важливо усвідомити, що сучасні інформаційні технології є ключовим інструментом реалізації цих принципів. Здобувачі повинні розуміти, які технологічні рішення застосовуються для обмеження доступу до інформації, запобігання її несанкціонованій зміні або знищенню, а також забезпечення безперервного функціонування інформаційних систем.

Особливу увагу слід приділити технологіям управління доступом до інформаційних ресурсів. У процесі опрацювання теми здобувачам рекомендується проаналізувати механізми автентифікації та авторизації користувачів, принципи функціонування систем управління ідентифікацією та доступом, а також можливості використання багатофакторної автентифікації для підвищення рівня захисту інформаційних систем. Необхідно також звернути увагу на роль криптографічних технологій у забезпеченні конфіденційності інформації та захисті даних під час їх передачі через комп'ютерні мережі.

Під час підготовки до практичних занять здобувачам доцільно ознайомитися з основними технологіями мережевої безпеки, зокрема з принципами функціонування міжмережевих екранів, систем виявлення вторгнень та систем запобігання вторгненням. Важливо розуміти їх призначення, принципи роботи та роль у забезпеченні захисту інформаційних систем від мережевих атак. Доцільно також приділити увагу технологіям моніторингу подій інформаційної безпеки, що дозволяють виявляти підозрілу активність у комп'ютерних мережах та оперативно реагувати на кіберінциденти.

Значну роль у сучасній системі кібербезпеки відіграють технології резервного копіювання та відновлення інформації. У процесі вивчення теми здобувачам необхідно

усвідомити значення таких технологій для забезпечення безперервності функціонування інформаційних систем, а також розглянути основні підходи до організації резервного зберігання даних. Особливу увагу слід приділити питанням захисту інформації у хмарних середовищах, оскільки використання хмарних технологій є однією з ключових тенденцій розвитку сучасних інформаційних систем.

Важливим напрямом вивчення теми є ознайомлення з новітніми інформаційними технологіями, що використовуються у сфері кібербезпеки. До таких технологій належать системи аналізу великих обсягів даних, технології штучного інтелекту та машинного навчання, які дозволяють автоматизувати процеси виявлення кіберзагроз та аналізу мережевої активності. Здобувачам необхідно зрозуміти можливості використання таких технологій для підвищення ефективності систем кіберзахисту та прогнозування потенційних кіберінцидентів.

У процесі самостійної роботи рекомендується опрацювати навчальну та наукову літературу, присвячену сучасним інформаційним технологіям у сфері кібербезпеки, а також проаналізувати приклади практичного застосування таких технологій у різних галузях діяльності. Доцільно також розглянути сучасні тенденції розвитку інформаційних технологій, зокрема розвиток хмарних обчислень, інтернету речей, технологій штучного інтелекту та інших інноваційних напрямів, що впливають на формування сучасної системи кібербезпеки.

Під час підготовки до підсумкового контролю здобувачам рекомендується систематизувати отримані знання, звертаючи увагу на основні технології забезпечення інформаційної безпеки, їх функціональне призначення, принципи роботи та сфери застосування. Особливу увагу слід приділити взаємозв’язку між різними технологічними засобами захисту інформації та їх ролі у створенні комплексної системи кіберзахисту.

Таким чином, опрацювання теми сприяє формуванню у здобувачів системного розуміння ролі інформаційних технологій у забезпеченні інформаційної та кібернетичної безпеки, розвитку навичок аналізу сучасних кіберзагроз та здатності застосовувати сучасні технологічні рішення для захисту інформаційних систем. Отримані знання є важливою складовою професійної підготовки фахівців у сфері кібербезпеки та необхідні для подальшої практичної діяльності у галузі захисту інформаційних ресурсів і цифрових систем, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. . Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист

інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В.В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 2
Інформаційні технології в інформаційній та/або кібербезпеці.

1. Що розуміється під інформаційними технологіями у сфері інформаційної та кібербезпеки?

2. Які основні принципи інформаційної безпеки забезпечуються за допомогою сучасних інформаційних технологій?

3. Які технології використовуються для управління ідентифікацією та доступом користувачів в інформаційних системах?

4. Яку роль відіграють криптографічні технології у забезпеченні конфіденційності інформації?

5. Які інформаційні технології застосовуються для забезпечення цілісності даних в інформаційних системах?

6. Які технології використовуються для забезпечення доступності інформаційних ресурсів і запобігання їх блокуванню?

7. Яке призначення систем моніторингу подій інформаційної безпеки та аналізу кіберінцидентів?

8. Які функції виконують системи виявлення та запобігання вторгненням у комп’ютерних мережах?

9. Які особливості забезпечення кібербезпеки при використанні хмарних інформаційних технологій?

10. Які можливості використання технологій штучного інтелекту та машинного навчання у сфері кібербезпеки?

ТЕМА 3. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ.

Загальні засади забезпечення безпеки інформаційно-комунікаційних систем.
Загрози, вразливості та ризики безпеці інформаційно-комунікаційних систем.
Технології та засоби захисту інформаційно-комунікаційних систем.
Організація моніторингу, реагування на інциденти та підтримання стійкості інформаційно-комунікаційних систем.

У сучасному інформаційному суспільстві інформаційно-комунікаційні системи відіграють ключову роль у забезпеченні функціонування держави, економіки та соціальної інфраструктури. Вони забезпечують обробку, зберігання, передачу та використання інформації у різних сферах діяльності, включаючи державне управління, банківську систему, транспорт, енергетику, телекомунікації, медицину, освіту та інші галузі. Розвиток цифрових технологій сприяв створенню складних інформаційних інфраструктур, що об'єднують численні комп'ютерні системи, сервери, мережеве обладнання, програмне забезпечення та канали зв'язку. Водночас широке використання інформаційно-комунікаційних систем супроводжується зростанням кількості кіберзагроз, що потребує впровадження ефективних механізмів захисту інформаційних ресурсів і мережевих інфраструктур.

Інформаційно-комунікаційна система являє собою сукупність технічних, програмних, телекомунікаційних та організаційних компонентів, які забезпечують створення, обробку, зберігання та передачу інформації між користувачами або інформаційними системами. До складу таких систем входять комп'ютери, сервери, мережеві комутатори, маршрутизатори, канали зв'язку, бази даних, операційні системи, прикладне програмне забезпечення, а також різноманітні інформаційні сервіси. Ефективне функціонування таких систем залежить від їх надійності, доступності та захищеності від внутрішніх і зовнішніх загроз.

Безпека інформаційно-комунікаційних систем передбачає комплекс організаційних, технічних та програмних заходів, спрямованих на забезпечення захисту інформаційних ресурсів, програмного забезпечення та мережевої інфраструктури від несанкціонованого доступу, знищення, модифікації, блокування або розголошення інформації. Основною метою забезпечення безпеки інформаційно-комунікаційних систем є підтримання стабільного функціонування інформаційної інфраструктури та запобігання негативним наслідкам кібернетичних атак, технічних збоїв або людського фактору.

Основою забезпечення безпеки інформаційно-комунікаційних систем є реалізація трьох фундаментальних принципів інформаційної безпеки, відомих як модель CIA, яка включає конфіденційність, цілісність та доступність інформації. Ці принципи є базовими орієнтирами для створення ефективних систем захисту інформації.

Конфіденційність інформації передбачає, що доступ до інформаційних ресурсів мають лише ті користувачі, які мають відповідні повноваження. Реалізація цього принципу здійснюється за допомогою різноманітних технологій контролю доступу до інформації. До таких технологій належать системи автентифікації користувачів, які дозволяють перевіряти їхню особу під час входу до інформаційної системи, системи авторизації, які визначають рівень доступу користувача до конкретних інформаційних ресурсів, а також системи управління ідентифікацією користувачів[5]. Для підвищення рівня захисту інформаційних

5 Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

систем широко застосовується багатофакторна автентифікація, що передбачає використання декількох незалежних методів перевірки особи користувача.

Важливим інструментом забезпечення конфіденційності інформації є криптографічні методи захисту. Криптографія дозволяє перетворювати інформацію у зашифрований вигляд, який є недоступним для сторонніх осіб без відповідного ключа дешифрування. Сучасні криптографічні алгоритми використовуються для захисту електронної пошти, передачі даних через мережу Інтернет, електронного документообігу, банківських операцій та інших інформаційних сервісів.

Другим важливим принципом безпеки інформаційно-комунікаційних систем є забезпечення цілісності інформації. Цілісність означає, що інформація повинна залишатися незмінною під час її обробки, передачі та зберігання, якщо такі зміни не були санкціоновані відповідними користувачами. Для забезпечення цілісності інформації застосовуються спеціальні програмні та криптографічні засоби, які дозволяють контролювати зміни у даних і виявляти спроби несанкціонованого втручання.

Одним із таких засобів є криптографічні хеш-функції, які дозволяють створювати унікальні цифрові відбитки даних. У разі зміни інформації навіть незначна модифікація даних призводить до зміни хеш-значення, що дозволяє виявити спроби несанкціонованого втручання. Крім того, широко використовуються цифрові підписи, які забезпечують підтвердження авторства інформації та гарантують її достовірність.

Третім базовим принципом безпеки інформаційно-комунікаційних систем є забезпечення доступності інформаційних ресурсів. Доступність означає, що інформаційні системи повинні бути доступними для користувачів у будь-який необхідний момент часу. Для забезпечення доступності використовуються різні технології резервування та відновлення інформації, відмовостійкі серверні системи, системи балансування навантаження та інші технологічні рішення.

Особливе значення має використання технологій резервного копіювання даних. Регулярне створення резервних копій дозволяє відновити інформацію у разі її втрати або пошкодження внаслідок технічних збоїв, кібернетичних атак або інших надзвичайних ситуацій. Сучасні системи резервного копіювання можуть використовувати локальні сховища даних, віддалені сервери або хмарні сервіси.

Забезпечення безпеки інформаційно-комунікаційних систем передбачає застосування комплексного підходу, що включає організаційні, технічні та програмні заходи захисту. Організаційні заходи включають розроблення політики інформаційної безпеки, встановлення правил доступу до інформаційних ресурсів, підготовку персоналу та контроль за дотриманням вимог безпеки. Важливою складовою таких заходів є проведення регулярних аудитів інформаційної безпеки та оцінювання ризиків.

Технічні заходи захисту включають використання спеціалізованого обладнання та програмного забезпечення, що забезпечують захист інформаційних систем від кібернетичних атак. До таких засобів належать міжмережеві екрани, системи виявлення вторгнень, системи запобігання вторгненням, системи шифрування даних та інші технології кіберзахисту.

Міжмережеві екрани виконують функцію контролю мережевого трафіку між різними сегментами комп’ютерних мереж. Вони дозволяють фільтрувати мережеві пакети відповідно до заданих правил безпеки та блокувати несанкціоновані спроби доступу до інформаційних систем. Системи виявлення вторгнень аналізують мережевий трафік та виявляють підозрілу активність, яка може свідчити про здійснення кібернетичної атаки.

Системи запобігання вторгненням виконують більш активну функцію, оскільки вони можуть автоматично блокувати підозрілі мережеві з’єднання або інші дії, що можуть становити загрозу для інформаційної системи. Використання таких систем дозволяє значно підвищити рівень захисту мережевої інфраструктури.

У сучасних умовах важливу роль у забезпеченні безпеки інформаційно-комунікаційних систем відіграють системи моніторингу подій інформаційної безпеки. Такі системи дозволяють збирати та аналізувати інформацію про події, що відбуваються у

комп'ютерних мережах, і виявляти потенційні кіберзагрози. Використання таких систем дозволяє своєчасно реагувати на кіберінциденти та мінімізувати їх наслідки[6].

З розвитком сучасних інформаційних технологій виникають нові виклики для забезпечення безпеки інформаційно-комунікаційних систем. Зокрема, використання хмарних технологій, мобільних пристроїв та систем інтернету речей створює нові потенційні вразливості, які можуть бути використані для здійснення кібернетичних атак. У зв'язку з цим важливим завданням є розроблення нових технологій кіберзахисту, що дозволяють забезпечити безпеку сучасної інформаційної інфраструктури.

Особливого значення набуває створення комплексних систем захисту інформації, які поєднують різні технологічні рішення для забезпечення багаторівневого захисту інформаційних ресурсів. Такий підхід передбачає використання різних механізмів захисту на різних рівнях інформаційної системи, включаючи мережевий рівень, рівень операційних систем, рівень прикладного програмного забезпечення та рівень користувацьких пристроїв.

Отже, безпека інформаційно-комунікаційних систем є важливою складовою сучасної системи інформаційної та кібернетичної безпеки. Ефективне забезпечення захисту таких систем потребує комплексного підходу, що включає використання сучасних технологічних засобів захисту інформації, впровадження ефективної політики інформаційної безпеки та постійне вдосконалення механізмів протидії сучасним кіберзагрозам. Надійний захист інформаційно-комунікаційних систем є необхідною умовою стабільного функціонування інформаційної інфраструктури держави, розвитку цифрової економіки та забезпечення національної безпеки.

Практичне заняття 3
Безпека інформаційно-комунікаційних систем.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Поняття та структура інформаційно-комунікаційних систем у сучасному цифровому середовищі.
2. Принципи забезпечення конфіденційності, цілісності та доступності інформації в інформаційно-комунікаційних системах.
3. Організаційні заходи забезпечення безпеки інформаційно-комунікаційних систем.
4. Технічні засоби захисту мережевої інфраструктури інформаційно-комунікаційних систем.
5. Системи контролю доступу та управління правами користувачів у інформаційних системах.
6. Технології резервного копіювання та відновлення інформації як складова безпеки інформаційно-комунікаційних систем.
7. Механізми моніторингу та реагування на інциденти інформаційної безпеки.
8. Багаторівневий підхід до забезпечення захисту інформаційно-комунікаційних систем.

ІІ. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Сучасні загрози безпеці інформаційно-комунікаційних систем та їх класифікація.

---

6 Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Використання міжмережевих екранів у забезпеченні безпеки комп’ютерних мереж.

3. Системи виявлення та запобігання мережевим вторгненням у комп’ютерних мережах.

4. Криптографічні методи захисту інформації в інформаційно-комунікаційних системах.

5. Захист інформаційно-комунікаційних систем у хмарних середовищах.

6. Технології забезпечення безпеки мобільних інформаційних систем.

7. Роль систем моніторингу подій інформаційної безпеки у захисті мережевої інфраструктури.

8. Використання комплексних систем захисту інформації в сучасних інформаційно-комунікаційних системах.

ІІІ. Розв’язати тестові завдання:

1. Інформаційно-комунікаційна система – це:

А) лише комп’ютерна мережа

Б) сукупність технічних, програмних та організаційних засобів для обробки, зберігання і передачі інформації

В) лише програмне забезпечення

Г) база даних

2. Який принцип інформаційної безпеки передбачає захист інформації від несанкціонованого доступу?

А) Доступність

Б) Конфіденційність

В) Масштабованість

Г) Надійність

3. Який принцип інформаційної безпеки означає збереження незмінності інформації?

А) Конфіденційність

Б) Цілісність

В) Доступність

Г) Масштабованість

4. Який принцип інформаційної безпеки забезпечує можливість отримання інформації уповноваженим користувачем у потрібний час?

А) Доступність

Б) Конфіденційність

В) Цілісність

Г) Автентичність

5. Який мережевий пристрій призначений для фільтрації мережевого трафіку відповідно до правил безпеки?

А) Комутатор

Б) Маршрутизатор

В) Міжмережевий екран (Firewall)

Г) Модем

6. Яка система призначена для виявлення підозрілої активності у мережі?
А) IDS
Б) VPN
В) FTP
Г) DHCP

7. Який тип системи автоматично блокує мережеві атаки?
А) IDS
Б) IPS
В) DNS
Г) SMTP

8. Який механізм забезпечує перевірку особи користувача?
А) Аутентифікація
Б) Архівація
В) Балансування
Г) Реплікація

9. Яка технологія використовується для створення резервних копій інформації?
А) Backup
Б) Routing
В) Switching
Г) Encoding

10. Яка технологія використовується для захисту даних під час передачі через мережу?
А) Шифрування
Б) Архівування
В) Реплікація
Г) Сканування

11. Під час аудиту безпеки виявлено, що сервер автоматично відновлює роботу після відмови одного з вузлів системи. Яку властивість інформаційної системи це забезпечує?
А) конфіденційність
Б) доступність
В) масштабованість
Г) сумісність

12. У мережі організації встановлено пристрій, що аналізує пакети даних і блокує підозрілі з’єднання відповідно до встановлених політик безпеки. Який тип технології використовується?
А) Firewall
Б) DNS
В) FTP
Г) SMTP

13. Під час атаки на інформаційну систему зловмисник намагається перевантажити сервер великою кількістю запитів. Який тип атаки здійснюється?

А) SQL Injection

Б) DDoS

В) Phishing

Г) Spoofing

14. Під час аналізу кіберінциденту встановлено, що зловмисник отримав доступ до системи через використання вразливості програмного забезпечення. Який етап забезпечення безпеки був недостатньо реалізований?

А) управління вразливостями

Б) резервне копіювання

В) балансування навантаження

Г) маршрутизація

15. У системі безпеки використовується принцип, за яким користувач отримує лише ті права доступу, які необхідні для виконання його службових обов’язків. Який принцип реалізується?

А) принцип мінімальних привілеїв

Б) принцип масштабованості

В) принцип резервування

Г) принцип сумісності

16. Організація використовує централізовану систему збору та аналізу журналів подій безпеки з різних серверів і мережевих пристроїв. Яку технологію застосовано?

А) SIEM

Б) RAID

В) DNS

Г) FTP

17. У системі безпеки використовується технологія, що дозволяє створювати захищене з’єднання через публічну мережу Інтернет. Яку технологію застосовано?

А) VPN

Б) SMTP

В) SNMP

Г) FTP

18. Під час передавання інформації використовується механізм перевірки, який дозволяє встановити, що дані не були змінені. Яка технологія використовується?

А) хешування

Б) компресія

В) маршрутизація

Г) кешування

19. У системі захисту застосовується багаторівнева архітектура безпеки, що передбачає використання кількох незалежних механізмів захисту. Який принцип реалізується?

А) Defense in Depth
Б) Least Privilege
В) Zero Trust
Г) Failover

20. Під час кібератаки зловмисник намагається отримати конфіденційні дані користувачів шляхом створення підробленого вебсайту, який імітує офіційний ресурс. Який тип атаки здійснюється?

А) Phishing
Б) DDoS
В) SQL Injection
Г) Brute Force

Методичні рекомендації

Опрацювання теми, присвяченої безпеці інформаційно-комунікаційних систем, є важливим етапом формування професійних компетентностей здобувачів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». У сучасному цифровому середовищі інформаційно-комунікаційні системи є основою функціонування державних установ, підприємств, банківських установ, транспортної інфраструктури та інших сфер діяльності. У зв’язку з цим забезпечення їх безпеки є одним із ключових завдань у сфері інформаційної та кібернетичної безпеки. Вивчення цієї теми спрямоване на формування у здобувачів системного розуміння принципів побудови захищених інформаційно-комунікаційних систем, а також механізмів протидії сучасним кіберзагрозам.

Під час опрацювання теми здобувачам необхідно звернути особливу увагу на поняття та структуру інформаційно-комунікаційних систем. Доцільно проаналізувати основні компоненти таких систем, зокрема апаратне забезпечення, програмне забезпечення, телекомунікаційні мережі, бази даних та інформаційні сервіси. Важливо усвідомити, що кожен із цих компонентів може бути об’єктом кібернетичних атак або інших загроз, що потребує застосування відповідних засобів захисту.

У процесі вивчення теми здобувачам рекомендується детально розглянути базові принципи інформаційної безпеки, зокрема конфіденційність, цілісність та доступність інформації. Необхідно зрозуміти, яким чином ці принципи реалізуються у сучасних інформаційно-комунікаційних системах та які технологічні рішення застосовуються для їх забезпечення. Особливу увагу слід приділити технологіям контролю доступу, криптографічного захисту інформації, а також механізмам контролю цілісності даних.

Важливим аспектом вивчення теми є ознайомлення з технічними засобами забезпечення безпеки інформаційно-комунікаційних систем. До таких засобів належать міжмережеві екрани, системи виявлення вторгнень, системи запобігання вторгненням, системи моніторингу подій інформаційної безпеки та інші технологічні рішення, що дозволяють захищати інформаційні системи від мережевих атак. Здобувачам необхідно розуміти принципи функціонування цих систем, їх призначення та роль у забезпеченні комплексного захисту інформаційної інфраструктури.

Під час підготовки до практичних занять здобувачам рекомендується проаналізувати сучасні методи захисту інформаційно-комунікаційних систем, зокрема використання криптографічних алгоритмів для захисту інформації під час її передачі через мережу, застосування технологій резервного копіювання та відновлення даних, а також використання систем моніторингу для виявлення потенційних кіберзагроз. Доцільно також розглянути практичні приклади реалізації багаторівневого захисту інформаційних систем.

Значну увагу необхідно приділити питанням організаційного забезпечення безпеки інформаційно-комунікаційних систем. До таких заходів належать розроблення політики інформаційної безпеки, регламентація доступу до інформаційних ресурсів, навчання персоналу правилам безпечної роботи з інформаційними системами, а також проведення регулярних аудитів інформаційної безпеки. Важливо усвідомити, що ефективний захист інформаційних систем неможливий без поєднання технічних і організаційних заходів.

Під час самостійної роботи здобувачам рекомендується опрацювати навчальну та наукову літературу, що стосується сучасних технологій забезпечення безпеки інформаційно-комунікаційних систем. Доцільно також ознайомитися з практичними прикладами реалізації систем кіберзахисту у державних і корпоративних інформаційних інфраструктурах. Аналіз таких прикладів дозволяє краще зрозуміти особливості застосування сучасних технологій кібербезпеки у реальних умовах.

Під час підготовки до підсумкового контролю здобувачам рекомендується систематизувати отримані знання щодо основних принципів і методів забезпечення безпеки інформаційно-комунікаційних систем, звертаючи увагу на їх взаємозв’язок та комплексний характер. Особливу увагу слід приділити розумінню ролі різних технологічних засобів захисту інформації у створенні ефективної системи кіберзахисту.

Таким чином, вивчення теми сприяє формуванню у здобувачів цілісного уявлення про сучасні підходи до забезпечення безпеки інформаційно-комунікаційних систем, розвитку аналітичного мислення та здатності застосовувати сучасні технологічні рішення для захисту інформаційної інфраструктури. Отримані знання є важливою складовою професійної підготовки фахівців у сфері кібербезпеки та необхідні для подальшої практичної діяльності у галузі захисту інформаційних систем, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. . Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я. Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист

інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 3
Безпека інформаційно-комунікаційних систем.

1. Що розуміється під інформаційно-комунікаційними системами та які основні компоненти входять до їх структури?

2. Які основні принципи забезпечення безпеки інформаційно-комунікаційних систем?

3. Які основні загрози можуть виникати під час функціонування інформаційно-комунікаційних систем?

4. Які технології використовуються для забезпечення конфіденційності інформації в інформаційно-комунікаційних системах?

5. Які механізми застосовуються для забезпечення цілісності даних у комп’ютерних мережах та інформаційних системах?

6. Які технологічні рішення використовуються для забезпечення доступності інформаційних ресурсів?

7. Яку роль відіграють міжмережеві екрани у забезпеченні безпеки комп’ютерних мереж?

8. Які функції виконують системи виявлення та запобігання мережевим вторгненням?

9. Яке значення мають технології резервного копіювання та відновлення даних для забезпечення безпеки інформаційних систем?

10. Які організаційні заходи необхідні для ефективного забезпечення безпеки інформаційно-комунікаційних систем?

ТЕМА 4. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ.

Поняття, структура та принципи побудови комплексних систем захисту інформації.

Організаційно-правові та нормативні засади створення комплексних систем захисту інформації.

Технічні, програмні та криптографічні засоби у складі комплексних систем захисту інформації.

Оцінювання ефективності, аудит і супровід комплексних систем захисту інформації.

У сучасному інформаційному суспільстві інформаційні ресурси набувають стратегічного значення для функціонування держави, економіки та соціальної інфраструктури. Інформація використовується у процесах державного управління, фінансово-економічної діяльності, наукових досліджень, управління виробничими процесами, функціонування банківської системи, енергетичного сектору, транспортної інфраструктури та інших галузей. Широке використання інформаційно-комунікаційних технологій сприяє підвищенню ефективності діяльності організацій, але водночас створює нові ризики, пов'язані з можливістю несанкціонованого доступу до інформації, її викрадення, модифікації або знищення. У зв'язку з цим особливого значення набуває забезпечення належного рівня захисту інформації, що обробляється в інформаційних системах.

Одним із найбільш ефективних підходів до забезпечення інформаційної безпеки є створення комплексних систем захисту інформації. Такі системи являють собою сукупність взаємопов'язаних організаційних, технічних, програмних та криптографічних заходів і засобів, спрямованих на забезпечення безпеки інформації в інформаційно-комунікаційних системах відповідно до встановлених вимог. Комплексна система захисту інформації формується на основі системного підходу до забезпечення безпеки, що передбачає врахування усіх можливих загроз, оцінювання ризиків та впровадження відповідних механізмів захисту.

Основною метою створення комплексних систем захисту інформації є забезпечення трьох ключових властивостей інформації: конфіденційності, цілісності та доступності. Конфіденційність передбачає обмеження доступу до інформації лише для уповноважених користувачів[7]. Цілісність означає збереження незмінності інформації та запобігання її несанкціонованій модифікації. Доступність забезпечує можливість отримання інформації уповноваженими користувачами у потрібний момент часу.

Комплексний характер систем захисту інформації зумовлений тим, що сучасні інформаційні системи є багаторівневими структурами, які включають апаратні засоби, програмне забезпечення, мережеву інфраструктуру та людський фактор. Кожен із цих елементів може бути потенційним джерелом загроз інформаційній безпеці. Наприклад, технічні пристрої можуть бути об'єктом фізичного втручання або технічних збоїв, програмне забезпечення може містити вразливості, мережеві комунікації можуть бути перехоплені зловмисниками, а користувачі можуть порушувати правила інформаційної безпеки через необережність або недостатній рівень підготовки.

7 Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

У зв'язку з цим створення комплексної системи захисту інформації передбачає проведення всебічного аналізу інформаційної системи, визначення її архітектури, ідентифікацію можливих загроз та оцінювання рівня ризиків. На основі такого аналізу формуються вимоги до системи захисту інформації, визначається політика інформаційної безпеки та розробляється структура комплексної системи захисту.

Однією з важливих складових комплексної системи захисту інформації є організаційні заходи. Вони включають розроблення нормативних документів, що регламентують порядок роботи з інформацією, визначення правил доступу до інформаційних ресурсів, розподіл прав і обов'язків користувачів, а також встановлення відповідальності за порушення вимог інформаційної безпеки. До організаційних заходів також належать підготовка та навчання персоналу, проведення регулярних інструктажів щодо правил безпечної роботи з інформаційними системами, а також здійснення внутрішнього контролю за дотриманням встановлених правил.

Не менш важливу роль відіграють технічні засоби захисту інформації. До таких засобів належать різноманітні пристрої та системи, що забезпечують фізичний і мережевий захист інформаційних ресурсів. Серед них можна виділити міжмережеві екрани, системи виявлення вторгнень, системи запобігання вторгненням, системи контролю доступу до приміщень, засоби захисту каналів зв'язку та інші технічні рішення. Використання таких засобів дозволяє обмежити несанкціонований доступ до інформаційних систем та забезпечити захист мережевої інфраструктури від кібернетичних атак.

Програмні засоби захисту інформації включають спеціалізоване програмне забезпечення, призначене для забезпечення безпеки операційних систем, баз даних, мережевих сервісів та прикладних програм. До таких засобів належать антивірусні програми, системи моніторингу подій інформаційної безпеки, системи контролю доступу до інформаційних ресурсів, засоби шифрування даних та інші програмні інструменти кіберзахисту. Програмні засоби захисту дозволяють автоматизувати процеси виявлення загроз та реагування на кіберінциденти.

Особливе значення у комплексних системах захисту інформації мають криптографічні методи захисту. Криптографія забезпечує конфіденційність інформації шляхом її шифрування, що унеможливлює доступ до даних сторонніх осіб. Крім того, криптографічні технології використовуються для забезпечення цілісності інформації за допомогою хеш-функцій, а також для підтвердження автентичності інформації за допомогою цифрових підписів. Такі технології широко застосовуються у системах електронного документообігу, банківських системах, системах електронної комерції та інших інформаційних сервісах.

Важливим елементом комплексної системи захисту інформації є системи контролю доступу до інформаційних ресурсів. Такі системи дозволяють визначати права користувачів щодо доступу до інформації відповідно до їх службових повноважень. Застосування систем контролю доступу дозволяє обмежити можливості несанкціонованого використання інформаційних ресурсів та зменшити ризик витоку конфіденційної інформації[8].

Значну роль у забезпеченні безпеки інформаційних систем відіграють технології резервного копіювання та відновлення даних. Резервне копіювання передбачає створення копій інформаційних ресурсів, які зберігаються у безпечному місці та можуть бути використані для відновлення інформації у разі її втрати або пошкодження. Використання таких технологій дозволяє забезпечити безперервність функціонування інформаційних систем навіть у разі виникнення технічних збоїв або кібернетичних атак.

З розвитком інформаційних технологій комплексні системи захисту інформації постійно вдосконалюються та доповнюються новими технологічними рішеннями. Сучасні системи кіберзахисту включають системи моніторингу подій інформаційної безпеки,

8 Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

системи аналізу мережевого трафіку, засоби управління інформаційними ризиками та інші інструменти, що дозволяють своєчасно виявляти потенційні загрози та реагувати на них.

Особливо перспективним напрямом розвитку комплексних систем захисту інформації є використання технологій штучного інтелекту та машинного навчання. Такі технології дозволяють автоматизувати процеси аналізу великих обсягів даних, виявляти аномалії у функціонуванні інформаційних систем та прогнозувати можливі кіберзагрози. Використання таких технологій значно підвищує ефективність систем кіберзахисту.

Комплексні системи захисту інформації широко застосовуються у державних органах, банківських установах, телекомунікаційних компаніях, підприємствах критичної інфраструктури та інших організаціях, діяльність яких пов'язана з обробкою значних обсягів інформації. Впровадження таких систем дозволяє забезпечити багаторівневий захист інформаційних ресурсів та значно знизити ризик виникнення кіберінцидентів.

Отже, комплексні системи захисту інформації є важливою складовою сучасної системи інформаційної та кібернетичної безпеки. Вони забезпечують багаторівневий захист інформаційних ресурсів шляхом поєднання організаційних, технічних, програмних та криптографічних засобів захисту. Ефективне впровадження комплексних систем захисту інформації є необхідною умовою стабільного функціонування інформаційної інфраструктури держави, розвитку цифрової економіки та протидії сучасним кіберзагрозам.

Практичне заняття 4
Комплексні системи захисту інформації.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Поняття та призначення комплексних систем захисту інформації в інформаційно-комунікаційних системах.
2. Основні принципи побудови комплексних систем захисту інформації.
3. Архітектура та структурні компоненти комплексної системи захисту інформації.
4. Організаційні заходи як складова комплексного забезпечення інформаційної безпеки.
5. Технічні засоби захисту інформації у структурі комплексної системи захисту.
6. Програмні механізми забезпечення безпеки інформаційних ресурсів.
7. Криптографічні методи захисту інформації в комплексних системах безпеки.
8. Багаторівневий підхід до забезпечення захисту інформаційних ресурсів.

ІІ. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Нормативно-правове регулювання створення комплексних систем захисту інформації в Україні.
2. Етапи створення та впровадження комплексної системи захисту інформації в інформаційних системах.
3. Методи оцінювання ризиків під час побудови комплексної системи захисту інформації.
4. Використання криптографічних технологій у комплексних системах захисту інформації.
5. Системи моніторингу та реагування на інциденти інформаційної безпеки.

6. Забезпечення безпеки інформаційних ресурсів у державних інформаційних системах.

7. Використання сучасних технологій кіберзахисту у комплексних системах безпеки.

8. Перспективи розвитку комплексних систем захисту інформації в умовах цифрової трансформації.

ІІІ. Розв’язати тестові завдання:

1. Комплексна система захисту інформації – це:

А) система резервного копіювання даних

Б) сукупність організаційних, технічних, програмних і криптографічних заходів та засобів захисту інформації

В) лише антивірусне програмне забезпечення

Г) комп’ютерна мережа

2. Основною метою створення комплексної системи захисту інформації є:

А) збільшення швидкості обробки інформації

Б) забезпечення конфіденційності, цілісності та доступності інформації

В) зменшення вартості програмного забезпечення

Г) підвищення продуктивності комп’ютерів

3. Який принцип інформаційної безпеки передбачає обмеження доступу до інформації для сторонніх осіб?

А) доступність

Б) конфіденційність

В) масштабованість

Г) сумісність

4. Який принцип інформаційної безпеки означає збереження незмінності інформації?

А) конфіденційність

Б) цілісність

В) доступність

Г) надійність

5. Який принцип забезпечує можливість доступу до інформації уповноваженим користувачам у необхідний момент часу?

А) доступність

Б) конфіденційність

В) цілісність

Г) криптографічність

6. Який компонент комплексної системи захисту інформації включає правила роботи з інформаційними ресурсами та політику безпеки?

А) криптографічний

Б) організаційний

В) апаратний

Г) мережевий

7. Який засіб захисту використовується для шифрування інформації?

А) криптографічні алгоритми

Б) антивірусні програми

В) маршрутизатори

Г) комутатори

8. Який засіб захисту призначений для виявлення шкідливого програмного забезпечення?

А) антивірус

Б) міжмережевий екран

В) маршрутизатор

Г) комутатор

9. Яка технологія використовується для створення копій даних з метою їх відновлення?

А) резервне копіювання

Б) кешування

В) маршрутизація

Г) балансування

10. Який документ визначає правила та вимоги щодо забезпечення безпеки інформації в організації?

А) політика інформаційної безпеки

Б) технічний паспорт

В) ліцензія

Г) сертифікат

11. Під час створення системи захисту інформації організація проводить аналіз можливих загроз та оцінює їх ймовірність і можливі наслідки. Який процес здійснюється?

А) оцінювання ризиків

Б) резервне копіювання

В) маршрутизація

Г) масштабування

12. У комплексній системі захисту інформації використовується багаторівневий захист, коли кілька різних механізмів безпеки застосовуються одночасно. Який принцип реалізується?

А) принцип багаторівневого захисту

Б) принцип централізації

В) принцип сумісності

Г) принцип оптимізації

13. У системі безпеки використовується цифровий підпис для підтвердження авторства електронного документа. Яку властивість інформації забезпечує ця технологія?

А) цілісність та автентичність
Б) доступність
В) масштабованість
Г) резервування

14. Під час аудиту інформаційної безпеки виявлено, що користувачі мають доступ до більшої кількості ресурсів, ніж це необхідно для виконання їх службових обов'язків. Який принцип порушено?
А) принцип мінімальних привілеїв
Б) принцип резервування
В) принцип масштабованості
Г) принцип централізації

15. У системі кіберзахисту використовується програмне забезпечення, яке збирає та аналізує події безпеки з різних джерел. Яку технологію застосовано?
А) SIEM
Б) DNS
В) FTP
Г) DHCP

16. У системі захисту застосовується метод шифрування інформації під час її передавання через мережу. Яка властивість інформації забезпечується передусім?
А) конфіденційність
Б) доступність
В) масштабованість
Г) резервування

17. Організація впровадила систему резервного копіювання даних із регулярним збереженням копій на віддалених серверах. Яку властивість інформації це забезпечує?
А) доступність
Б) масштабованість
В) сумісність
Г) оптимізацію

18. Під час проєктування системи захисту інформації враховується людський фактор, зокрема помилки користувачів або недотримання правил безпеки. До якого типу заходів належить підготовка персоналу?
А) організаційних
Б) криптографічних
В) технічних
Г) програмних

19. У системі захисту використовуються міжмережеві екрани, антивірусні програми та системи виявлення вторгнень. Який підхід до забезпечення безпеки реалізується?
А) комплексний підхід
Б) централізований підхід

В) локальний підхід
Г) спрощений підхід

20. Під час кібератаки зловмисник намагається змінити інформацію в базі даних без відома власника системи. Яка властивість інформації порушується?
А) цілісність
Б) доступність
В) масштабованість
Г) резервування

Методичні рекомендації

Вивчення теми, присвяченої комплексним системам захисту інформації, є важливою складовою підготовки здобувачів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». У сучасних умовах цифровізації суспільства та стрімкого розвитку інформаційно-комунікаційних технологій інформаційні ресурси стають одним із ключових елементів функціонування держави, економіки та соціальної сфери. У зв'язку з цим забезпечення їх належного захисту набуває особливого значення, а створення комплексних систем захисту інформації є одним із найбільш ефективних підходів до організації інформаційної безпеки.

Під час опрацювання теми здобувачам рекомендується насамперед зосередити увагу на сутності та призначенні комплексних систем захисту інформації. Необхідно усвідомити, що такі системи являють собою сукупність взаємопов'язаних організаційних, технічних, програмних та криптографічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в інформаційно-комунікаційних системах. Важливо зрозуміти, що ефективний захист інформації можливий лише за умови поєднання різних методів і засобів захисту, які функціонують як єдина система.

Під час вивчення теми особливу увагу слід приділити принципам побудови комплексних систем захисту інформації. До таких принципів належать системність, багаторівневість захисту, безперервність контролю за станом інформаційної безпеки, мінімізація привілеїв користувачів, а також відповідність вимогам нормативно-правових актів у сфері інформаційної безпеки. Здобувачам необхідно розуміти, що реалізація цих принципів дозволяє створити ефективну систему захисту інформаційних ресурсів.

Важливим аспектом вивчення теми є ознайомлення зі структурою комплексної системи захисту інформації. Здобувачам рекомендується детально проаналізувати основні складові таких систем, зокрема організаційні заходи, технічні засоби захисту, програмні механізми безпеки та криптографічні методи захисту інформації. Доцільно також розглянути роль кожної з цих складових у забезпеченні комплексного захисту інформаційних ресурсів.

Особливу увагу слід приділити організаційним заходам забезпечення інформаційної безпеки. До них належать розроблення політики інформаційної безпеки, визначення правил доступу до інформаційних ресурсів, регламентація роботи з інформаційними системами, а також підготовка персоналу до безпечної роботи з інформаційними технологіями. Здобувачам важливо усвідомити, що людський фактор є одним із найбільш поширених джерел виникнення кіберзагроз, тому навчання персоналу та контроль за дотриманням правил інформаційної безпеки є необхідною складовою ефективної системи захисту.

У процесі вивчення теми необхідно також ознайомитися з технічними та програмними засобами захисту інформації, що застосовуються у комплексних системах

захисту. До таких засобів належать міжмережеві екрани, системи виявлення вторгнень, системи запобігання вторгненням, антивірусне програмне забезпечення, системи моніторингу подій інформаційної безпеки та інші інструменти кіберзахисту. Розуміння принципів функціонування цих засобів дозволяє здобувачам оцінювати їх ефективність та визначати можливості їх застосування у різних інформаційних системах.

Значну увагу під час опрацювання теми необхідно приділити криптографічним методам захисту інформації. Здобувачам рекомендується вивчити основні принципи використання криптографічних алгоритмів, методи шифрування інформації, механізми забезпечення цілісності даних та використання цифрових підписів. Доцільно також розглянути практичні приклади застосування криптографічних технологій у сучасних інформаційних системах.

Під час підготовки до практичних занять здобувачам рекомендується розглянути приклади впровадження комплексних систем захисту інформації у державних та корпоративних інформаційних системах. Аналіз таких прикладів дозволяє зрозуміти особливості побудови систем кіберзахисту у реальних умовах та оцінити ефективність різних технологічних рішень.

Під час самостійної роботи доцільно опрацювати навчальні та наукові джерела, що стосуються сучасних підходів до створення комплексних систем захисту інформації, а також ознайомитися з нормативно-правовими документами, які регулюють питання забезпечення інформаційної безпеки. Здобувачам рекомендується систематизувати отримані знання, приділяючи увагу взаємозв’язку між різними складовими комплексної системи захисту інформації.

Під час підготовки до підсумкового контролю необхідно узагальнити знання щодо принципів побудови комплексних систем захисту інформації, їх структурних компонентів та основних технологій кіберзахисту. Особливу увагу слід приділити розумінню ролі комплексного підходу до забезпечення інформаційної безпеки та здатності застосовувати отримані знання для аналізу та оцінювання стану захисту інформаційних систем.

Таким чином, опрацювання теми сприяє формуванню у здобувачів системного бачення сучасних підходів до забезпечення інформаційної безпеки, розвитку навичок аналізу кіберзагроз та здатності застосовувати комплексні методи захисту інформації. Отримані знання є важливою складовою професійної підготовки фахівців у сфері кібербезпеки та необхідні для подальшої практичної діяльності, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. . Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В.В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 4
Комплексні системи захисту інформації.

1. Що розуміється під комплексною системою захисту інформації та яке її основне призначення?

2. Які основні принципи покладено в основу побудови комплексних систем захисту інформації?

3. Які складові елементи входять до структури комплексної системи захисту інформації?

4. Яку роль відіграють організаційні заходи у забезпеченні захисту інформаційних ресурсів?

5. Які технічні засоби використовуються у комплексних системах захисту інформації?

6. Які програмні механізми застосовуються для забезпечення безпеки інформаційних систем?

7. Яке значення мають криптографічні методи у комплексних системах захисту інформації?

8. Які етапи передбачає створення та впровадження комплексної системи захисту інформації?

9. Яке значення має аналіз ризиків під час проєктування комплексної системи захисту інформації?

10. Яким чином забезпечується багаторівневий захист інформації в інформаційно-комунікаційних системах?

ТЕМА 5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА/АБО КІБЕРБЕЗПЕКОЮ.

Теоретико-організаційні засади управління інформаційною та кібербезпекою.

Система управління ризиками в галузі інформаційної та кібербезпеки.

Політики, процедури та організаційні механізми забезпечення інформаційної та кібербезпеки.

Моніторинг, аудит і вдосконалення системи управління інформаційною та кібербезпекою.

У сучасних умовах цифровізації суспільства інформаційні ресурси та інформаційно-комунікаційні системи стали невід'ємною складовою функціонування держави, економіки, науки та соціальної сфери. Практично всі сфери діяльності сучасної людини пов'язані з використанням комп'ютерних систем, телекомунікаційних мереж, хмарних сервісів та інших цифрових технологій. Інформація виступає важливим стратегічним ресурсом, що забезпечує ефективність управлінських процесів, конкурентоспроможність організацій та стабільність державних інституцій. Водночас широке використання інформаційних технологій створює нові ризики, пов'язані з можливістю виникнення кібернетичних атак, витоку конфіденційних даних, порушення цілісності інформації або блокування доступу до інформаційних ресурсів.

У зв'язку з цим особливої актуальності набуває питання ефективного управління інформаційною та кібербезпекою. Управління інформаційною безпекою являє собою комплекс організаційних, адміністративних, технічних і правових заходів, спрямованих на забезпечення захисту інформації та інформаційних систем від внутрішніх і зовнішніх загроз. Таке управління передбачає систематичне планування, організацію, контроль та вдосконалення процесів забезпечення безпеки інформаційних ресурсів.

Основною метою управління інформаційною та кібербезпекою є створення ефективної системи забезпечення інформаційної безпеки, яка дозволяє організації своєчасно виявляти потенційні загрози, оцінювати рівень ризиків, впроваджувати заходи захисту та реагувати на кіберінциденти. Ефективне управління інформаційною безпекою передбачає інтеграцію заходів захисту інформації у загальну систему управління організацією та врахування вимог інформаційної безпеки на всіх етапах функціонування інформаційних систем[9].

Одним із ключових елементів управління інформаційною безпекою є формування політики інформаційної безпеки організації. Політика інформаційної безпеки є основним нормативним документом, що визначає загальні принципи, правила та процедури забезпечення захисту інформаційних ресурсів. У цьому документі визначаються основні

9 Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

вимоги щодо роботи з інформацією, правила доступу до інформаційних ресурсів, порядок використання інформаційних систем, а також відповідальність користувачів за порушення встановлених вимог безпеки.

Політика інформаційної безпеки повинна враховувати особливості діяльності організації, характер інформаційних ресурсів, що використовуються, а також можливі загрози інформаційній безпеці. Крім того, вона повинна регулярно переглядатися та оновлюватися з урахуванням змін у технологічному середовищі та появи нових кіберзагроз.

Важливою складовою управління інформаційною безпекою є процес управління ризиками. Управління ризиками передбачає систематичний аналіз можливих загроз інформаційній безпеці, оцінювання їх ймовірності та потенційних наслідків, а також визначення заходів щодо зменшення або усунення ризиків. Такий підхід дозволяє організаціям визначати найбільш критичні інформаційні ресурси та спрямовувати зусилля на їх захист.

Процес управління ризиками зазвичай включає кілька етапів. Першим етапом є ідентифікація загроз інформаційній безпеці, що можуть виникати у процесі функціонування інформаційних систем. До таких загроз належать кібернетичні атаки, технічні збої, помилки користувачів, несанкціонований доступ до інформації та інші небезпечні фактори. Наступним етапом є оцінювання ризиків, що передбачає визначення ймовірності виникнення загроз та можливих наслідків для інформаційних ресурсів. Після цього визначаються заходи щодо мінімізації ризиків, включаючи впровадження технічних засобів захисту, організаційних процедур та інших механізмів безпеки.

Одним із важливих напрямів управління інформаційною безпекою є управління доступом до інформаційних ресурсів. Системи управління доступом дозволяють визначати права користувачів щодо використання інформаційних ресурсів відповідно до їх службових обов’язків. При цьому широко застосовується принцип мінімальних привілеїв, відповідно до якого кожен користувач отримує лише той рівень доступу, який необхідний для виконання його функціональних обов’язків.

Для забезпечення контролю доступу використовуються різні механізми автентифікації та авторизації користувачів. Сучасні системи кібербезпеки часто застосовують багатофакторну автентифікацію, яка передбачає використання кількох незалежних методів підтвердження особи користувача. Це дозволяє значно підвищити рівень захисту інформаційних систем.

Не менш важливим елементом управління інформаційною безпекою є моніторинг стану інформаційних систем. Моніторинг передбачає постійне спостереження за функціонуванням інформаційної інфраструктури з метою своєчасного виявлення підозрілої активності або ознак кібернетичних атак. Для цього використовуються спеціалізовані системи моніторингу подій інформаційної безпеки, які дозволяють автоматично збирати та аналізувати інформацію про події, що відбуваються у комп’ютерних мережах.

Важливим напрямом управління кібербезпекою є управління інцидентами інформаційної безпеки. Інцидентом інформаційної безпеки вважається будь-яка подія, що може призвести до порушення конфіденційності, цілісності або доступності інформації. До таких інцидентів належать несанкціонований доступ до інформації, витік даних, пошкодження інформаційних ресурсів або збої у функціонуванні інформаційних систем.

Процес управління інцидентами включає кілька основних етапів: виявлення інциденту, аналіз причин його виникнення, локалізацію загрози, усунення наслідків та відновлення нормального функціонування інформаційних систем. Ефективна система реагування на інциденти дозволяє мінімізувати негативні наслідки кібернетичних атак та запобігти повторному виникненню подібних ситуацій.

Значну роль у системі управління інформаційною безпекою відіграє проведення аудитів інформаційної безпеки. Аудит інформаційної безпеки являє собою процес оцінювання стану захищеності інформаційних систем та перевірки відповідності існуючих механізмів захисту встановленим вимогам безпеки. Проведення аудиту дозволяє виявляти

вразливості інформаційних систем та визначати напрями вдосконалення механізмів захисту інформації[10].

Важливим елементом системи управління інформаційною безпекою є підготовка персоналу. Людський фактор є одним із найбільш поширених джерел виникнення кіберзагроз, тому навчання працівників правилам безпечної роботи з інформаційними системами є важливою складовою забезпечення інформаційної безпеки. Проведення навчальних заходів, тренінгів та інструктажів дозволяє підвищити рівень обізнаності працівників щодо сучасних кіберзагроз та методів їх запобігання.

У сучасних умовах управління інформаційною безпекою здійснюється на основі міжнародних стандартів та кращих світових практик. Одним із найбільш відомих стандартів у цій сфері є стандарт ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою. Використання таких стандартів дозволяє організаціям впроваджувати ефективні механізми управління інформаційною безпекою та забезпечувати відповідність міжнародним вимогам.

Значну роль у сучасних системах управління кібербезпекою відіграє автоматизація процесів забезпечення інформаційної безпеки. Сучасні інформаційні технології дозволяють автоматизувати процеси моніторингу мережевої активності, аналізу подій інформаційної безпеки, управління доступом до інформаційних ресурсів та реагування на кіберінциденти. Використання таких технологій дозволяє значно підвищити ефективність систем кіберзахисту.

Особливо перспективним напрямом розвитку управління інформаційною безпекою є використання технологій штучного інтелекту та машинного навчання. Такі технології дозволяють аналізувати великі обсяги даних, виявляти аномалії у функціонуванні інформаційних систем та прогнозувати можливі кіберзагрози. Використання таких технологій дозволяє значно підвищити рівень захищеності інформаційних систем.

Отже, управління інформаційною та кібербезпекою є складним і багатокомпонентним процесом, що передбачає поєднання організаційних, технічних, правових та управлінських заходів. Ефективна система управління інформаційною безпекою дозволяє забезпечити надійний захист інформаційних ресурсів, своєчасно реагувати на кіберзагрози та підтримувати стабільне функціонування інформаційної інфраструктури. В умовах стрімкого розвитку інформаційних технологій та зростання кількості кібернетичних атак ефективне управління інформаційною безпекою стає одним із ключових чинників забезпечення національної безпеки, економічної стабільності та сталого розвитку суспільства.

Практичне заняття 5
Управління інформаційною та/або кібербезпекою.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Сутність та основні завдання управління інформаційною та кібербезпекою.

2. Політика інформаційної безпеки як основа системи управління безпекою організації.

3. Процеси управління ризиками у сфері інформаційної та кібербезпеки.

4. Організаційна структура управління інформаційною безпекою в установах та організаціях.

---

10 Державно-правовий експеримент в галузі інформатизації: монографія / Я. Ю. Дорогий, І. О. Бердиченко, О.О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Управління доступом до інформаційних ресурсів та реалізація принципу мінімальних привілеїв.

6. Моніторинг стану інформаційної безпеки та аналіз подій безпеки в інформаційних системах.

7. Управління інцидентами інформаційної безпеки та реагування на кіберзагрози.

8. Аудит інформаційної безпеки як інструмент оцінювання ефективності системи кіберзахисту.

ІІ. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Міжнародні стандарти управління інформаційною безпекою та їх застосування в організаціях.

2. Система управління інформаційною безпекою відповідно до стандарту ISO/IEC 27001.

3. Методи оцінювання ризиків у системах управління кібербезпекою.

4. Роль людського фактору у забезпеченні інформаційної безпеки організацій.

5. Використання систем моніторингу подій інформаційної безпеки у процесі управління кіберзахистом.

6. Автоматизація процесів управління інформаційною безпекою в сучасних організаціях.

7. Управління кіберінцидентами у корпоративних інформаційних системах.

8. Перспективи розвитку систем управління кібербезпекою в умовах цифрової трансформації.

ІІІ. Розв’язати тестові завдання:

1. Управління інформаційною безпекою – це:

А) процес обробки інформації

Б) сукупність організаційних, технічних та адміністративних заходів щодо захисту інформації

В) лише використання антивірусного програмного забезпечення

Г) лише контроль доступу до комп’ютерів

2. Основною метою управління інформаційною безпекою є:

А) підвищення швидкості роботи комп’ютерних систем

Б) забезпечення захисту інформаційних ресурсів від загроз

В) зменшення витрат на інформаційні технології

Г) збільшення кількості користувачів системи

3. Документ, який визначає правила та вимоги щодо забезпечення захисту інформації в організації, називається:

А) технічний паспорт

Б) політика інформаційної безпеки

В) ліцензійна угода

Г) регламент мережі

4. Який принцип передбачає надання користувачу лише тих прав доступу, які необхідні для виконання його службових обов’язків?

А) принцип резервування
Б) принцип мінімальних привілеїв
В) принцип масштабованості
Г) принцип сумісності

5. Процес визначення можливих загроз інформаційній безпеці та оцінювання їх впливу називається:
А) маршрутизацією
Б) управлінням ризиками
В) резервним копіюванням
Г) шифруванням

6. Подія, яка може призвести до порушення конфіденційності, цілісності або доступності інформації, називається:
А) інформаційним інцидентом
Б) резервною копією
В) протоколом передачі даних
Г) мережею

7. Процес перевірки відповідності системи вимогам інформаційної безпеки називається:
А) аудит інформаційної безпеки
Б) шифрування
В) маршрутизація
Г) балансування

8. Який фактор часто є причиною виникнення кіберінцидентів у системах інформаційної безпеки?
А) людський фактор
Б) кліматичні умови
В) технічний прогрес
Г) модернізація обладнання

9. Яка система дозволяє збирати та аналізувати події інформаційної безпеки з різних джерел?
А) SIEM
Б) FTP
В) DNS
Г) DHCP

10. Який стандарт визначає вимоги до систем управління інформаційною безпекою?
А) ISO/IEC 27001
Б) IEEE 802.11
В) TCP/IP
Г) HTTP

11. Організація впроваджує систему управління інформаційною безпекою відповідно до міжнародних стандартів. Який стандарт найчастіше використовується для цього?

А) ISO/IEC 27001

Б) IEEE 802.3

В) HTML5

Г) SQL

12. У компанії впроваджено процедури регулярного аналізу загроз, оцінювання ризиків та розроблення заходів щодо їх мінімізації. Який процес реалізується?

А) управління ризиками

Б) маршрутизація

В) балансування навантаження

Г) архівування

13. Під час перевірки інформаційної системи було виявлено низку вразливостей та невідповідність встановленим вимогам безпеки. Який процес здійснювався?

А) аудит інформаційної безпеки

Б) шифрування

В) резервне копіювання

Г) маршрутизація

14. У системі кібербезпеки використовується принцип, згідно з яким доступ до інформаційних ресурсів надається лише після перевірки особи користувача. Який процес реалізується?

А) автентифікація

Б) компресія

В) маршрутизація

Г) балансування

15. У системі управління інформаційною безпекою використовується механізм постійного спостереження за станом мережі та виявлення підозрілої активності. Який процес здійснюється?

А) моніторинг безпеки

Б) архівування

В) маршрутизація

Г) резервування

16. Під час інциденту інформаційної безпеки спеціалісти здійснюють аналіз причин атаки, локалізують загрозу та відновлюють роботу системи. Який процес реалізується?

А) управління інцидентами

Б) балансування

В) резервування

Г) масштабування

17. У системі безпеки використовується принцип, що передбачає застосування кількох незалежних механізмів захисту одночасно. Який підхід реалізується?

А) багаторівневий захист
Б) централізація
В) стандартизація
Г) оптимізація

18. Під час аналізу ризиків визначено, що ймовірність виникнення певної кіберзагрози є високою, а її наслідки можуть бути критичними. Яке рішення повинно бути прийняте?
А) впровадження додаткових заходів захисту
Б) ігнорування загрози
В) видалення інформаційної системи
Г) відключення мережі

19. У системі управління інформаційною безпекою регулярно проводяться навчання працівників щодо правил безпечної роботи з інформаційними системами. Яка мета таких заходів?
А) зменшення ризиків, пов’язаних із людським фактором
Б) збільшення продуктивності комп’ютерів
В) зменшення витрат на обладнання
Г) модернізація програмного забезпечення

20. Під час кіберінциденту зловмисник отримав доступ до конфіденційних даних через обліковий запис працівника, який використовував простий пароль. Який елемент системи управління безпекою був реалізований недостатньо ефективно?
А) управління доступом та політика паролів
Б) резервне копіювання
В) маршрутизація
Г) балансування навантаження

Методичні рекомендації

Опрацювання теми, присвяченої управлінню інформаційною та кібербезпекою, має важливе значення для формування у здобувачів вищої освіти системного розуміння організації процесів забезпечення захисту інформаційних ресурсів та інформаційно-комунікаційних систем. У сучасних умовах цифровізації суспільства інформаційні технології активно використовуються у державному управлінні, фінансовому секторі, промисловості, наукових дослідженнях та інших сферах діяльності. Водночас зростання кількості кіберзагроз вимагає впровадження ефективних механізмів управління інформаційною безпекою, які дозволяють своєчасно виявляти потенційні загрози, оцінювати ризики та впроваджувати заходи щодо їх нейтралізації.

Під час вивчення теми здобувачам необхідно звернути увагу на сутність та основні принципи управління інформаційною та кібербезпекою. Важливо усвідомити, що управління у цій сфері передбачає системну діяльність, спрямовану на планування, організацію, координацію та контроль процесів забезпечення захисту інформаційних ресурсів. Доцільно також розглянути роль управління інформаційною безпекою у загальній системі управління організацією та його значення для забезпечення стабільного функціонування інформаційної інфраструктури.

Особливу увагу слід приділити вивченню політики інформаційної безпеки як основного документа, що визначає принципи та правила роботи з інформаційними ресурсами. Здобувачам рекомендується проаналізувати структуру політики інформаційної безпеки, її основні елементи та роль у забезпеченні захисту інформації. Важливо розуміти, що політика інформаційної безпеки повинна враховувати особливості діяльності організації, характер інформаційних ресурсів та рівень можливих загроз.

У процесі опрацювання теми необхідно приділити значну увагу управлінню ризиками у сфері інформаційної безпеки. Здобувачам рекомендується розглянути основні етапи цього процесу, зокрема ідентифікацію загроз, оцінювання ризиків, визначення пріоритетних напрямів захисту та впровадження заходів щодо мінімізації ризиків. Доцільно також ознайомитися з основними методами оцінювання ризиків та їх застосуванням у процесі забезпечення кібербезпеки.

Важливим аспектом вивчення теми є управління доступом до інформаційних ресурсів. Здобувачам необхідно проаналізувати основні механізми контролю доступу, зокрема автентифікацію, авторизацію та облік дій користувачів. Особливу увагу слід приділити принципу мінімальних привілеїв, який передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їх службових обов’язків.

Під час підготовки до практичних занять здобувачам рекомендується розглянути сучасні методи моніторингу стану інформаційної безпеки та аналізу подій безпеки. Доцільно також ознайомитися з функціонуванням систем моніторингу подій інформаційної безпеки, які дозволяють своєчасно виявляти підозрілу активність у комп’ютерних мережах та реагувати на можливі кіберзагрози.

Значну увагу необхідно приділити процесу управління інцидентами інформаційної безпеки. Здобувачам рекомендується розглянути основні етапи реагування на інциденти, включаючи їх виявлення, аналіз, локалізацію загрози, усунення наслідків та відновлення функціонування інформаційних систем. Аналіз практичних прикладів кіберінцидентів дозволяє краще зрозуміти особливості реагування на сучасні кіберзагрози.

Важливим напрямом вивчення теми є аудит інформаційної безпеки. Здобувачам необхідно розглянути мету та основні етапи проведення аудиту інформаційної безпеки, а також його роль у виявленні вразливостей інформаційних систем та підвищенні рівня їх захищеності.

Під час самостійної роботи здобувачам рекомендується опрацювати навчальну та наукову літературу, що стосується сучасних підходів до управління інформаційною безпекою, а також ознайомитися з міжнародними стандартами у цій сфері. Особливу увагу слід приділити стандартам серії ISO/IEC 27000, які визначають вимоги до систем управління інформаційною безпекою.

Під час підготовки до підсумкового контролю доцільно систематизувати отримані знання щодо основних процесів управління інформаційною та кібербезпекою, їх взаємозв’язку та ролі у забезпеченні захисту інформаційних систем. Здобувачам рекомендується звернути увагу на практичне застосування отриманих знань для аналізу сучасних кіберзагроз та розроблення заходів щодо їх нейтралізації.

Таким чином, опрацювання теми сприяє формуванню у здобувачів системного розуміння процесів управління інформаційною безпекою, розвитку аналітичного мислення та здатності застосовувати сучасні підходи до забезпечення захисту інформаційних ресурсів. Отримані знання є важливою складовою професійної підготовки фахівців у сфері

кібербезпеки та необхідні для подальшої практичної діяльності, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 5
Управління інформаційною та/або кібербезпекою.

1. Що розуміється під управлінням інформаційною та кібербезпекою і які його основні завдання?

2. Яку роль відіграє політика інформаційної безпеки у системі управління інформаційною безпекою організації?

3. Які основні етапи процесу управління ризиками у сфері інформаційної безпеки?

4. Які принципи застосовуються під час організації системи управління інформаційною безпекою?

5. Які механізми використовуються для управління доступом до інформаційних ресурсів?

6. Яку роль відіграє моніторинг інформаційних систем у процесі управління кібербезпекою?

7. Що розуміється під інцидентом інформаційної безпеки та які основні етапи реагування на нього?

8. Яке значення має аудит інформаційної безпеки у системі управління інформаційною безпекою?

9. Яким чином людський фактор впливає на рівень інформаційної безпеки організації?

10. Яку роль відіграють міжнародні стандарти у формуванні систем управління інформаційною безпекою?

ТЕМА 6. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.

Теоретичні засади криптографічного захисту інформації.

Симетричні та асиметричні криптографічні алгоритми у системах захисту інформації.

Електронний підпис, хешування та інфраструктура відкритих ключів у забезпеченні безпеки інформації.

Організаційно-правові та практичні аспекти застосування криптографічного захисту інформації.

У сучасному інформаційному суспільстві інформація виступає одним із ключових ресурсів, від якого залежить ефективність функціонування державних інституцій, економіки, фінансових систем, наукових установ та інших сфер суспільного життя. Активний розвиток інформаційно-комунікаційних технологій, глобальних комп'ютерних мереж, хмарних сервісів та цифрових платформ значно розширив можливості створення, обробки та передачі інформації. Водночас широке використання електронних інформаційних систем супроводжується зростанням кількості кіберзагроз, пов'язаних із несанкціонованим доступом до даних, їх модифікацією, перехопленням, викраденням або знищенням. У таких умовах особливо важливого значення набуває застосування криптографічних методів захисту інформації, які дозволяють забезпечити надійний захист інформаційних ресурсів.

Криптографічний захист інформації являє собою сукупність методів і засобів перетворення інформації за допомогою спеціальних математичних алгоритмів з метою забезпечення її конфіденційності, цілісності, автентичності та невідмовності. Основою криптографічного захисту є використання криптографічних алгоритмів, які перетворюють інформацію у зашифрований вигляд. Така інформація може бути відновлена лише за допомогою спеціального криптографічного ключа, що забезпечує обмеження доступу до даних для сторонніх осіб.

Одним із ключових завдань криптографічного захисту інформації є забезпечення конфіденційності даних. Конфіденційність означає, що інформація доступна лише тим особам, які мають відповідні повноваження для її використання. Для забезпечення конфіденційності використовується процес шифрування, який передбачає перетворення відкритого тексту у зашифрований текст за допомогою криптографічного алгоритму та спеціального ключа. У разі перехоплення зашифрованого повідомлення сторонніми особами вони не можуть отримати доступ до змісту інформації без відповідного ключа дешифрування.

Крім забезпечення конфіденційності, криптографічні методи використовуються для забезпечення цілісності інформації. Цілісність означає, що дані не були змінені під час їх передачі або зберігання без відповідного дозволу. Для забезпечення цілісності інформації застосовуються криптографічні хеш-функції, які дозволяють створювати унікальні цифрові відбитки інформації[11]. Будь-яка зміна навіть незначної частини інформації призводить до суттєвої зміни хеш-значення, що дозволяє своєчасно виявити факт несанкціонованого втручання у дані.

Важливим завданням криптографічного захисту інформації є забезпечення автентичності даних. Автентичність означає підтвердження того, що інформація була створена або передана саме тим користувачем, який заявляє про це. Для цього використовуються механізми цифрового підпису, які дозволяють перевірити справжність електронного документа або повідомлення. Цифровий підпис створюється за допомогою криптографічних алгоритмів та спеціального приватного ключа користувача. Отримувач інформації може перевірити дійсність підпису за допомогою відповідного відкритого ключа.

Ще одним важливим елементом криптографічного захисту є забезпечення невідмовності. Невідмовність означає, що користувач не може заперечувати факт виконання певної дії, наприклад відправлення електронного документа або проведення електронної транзакції. Завдяки використанню цифрових підписів та спеціальних протоколів криптографічного захисту можна забезпечити фіксацію факту передачі інформації та підтвердження участі сторін у процесі обміну даними.

Криптографічні методи захисту інформації поділяються на кілька основних видів залежно від принципів використання криптографічних ключів. Найбільш поширеним видом криптографічного захисту є симетричне шифрування. У симетричних криптографічних системах для шифрування та дешифрування інформації використовується один і той самий криптографічний ключ. Такий метод характеризується високою швидкістю обробки інформації та ефективністю при роботі з великими обсягами даних. До найбільш відомих алгоритмів симетричного шифрування належать алгоритми AES, DES та Triple DES.

Іншим важливим видом криптографічного захисту є асиметричне шифрування. На відміну від симетричних алгоритмів, асиметричні криптографічні системи використовують два різні ключі – відкритий та закритий. Відкритий ключ може бути доступний для всіх користувачів та використовується для шифрування інформації, тоді як закритий ключ зберігається у власника та використовується для дешифрування повідомлень. Такий підхід значно підвищує рівень безпеки інформаційного обміну, особливо під час передачі даних через відкриті мережі. Найбільш поширеними алгоритмами асиметричного шифрування є RSA, ElGamal та алгоритми на основі еліптичних кривих.

У сучасних інформаційних системах широко використовуються комбіновані криптографічні системи, які поєднують переваги симетричного та асиметричного шифрування. У таких системах асиметричні алгоритми використовуються для обміну криптографічними ключами, а симетричні алгоритми застосовуються для безпосереднього шифрування великих обсягів інформації. Такий підхід дозволяє поєднати високий рівень безпеки з ефективністю обробки даних.

Важливим елементом криптографічного захисту інформації є система управління криптографічними ключами. Надійність криптографічного захисту значною мірою залежить від безпечного зберігання та використання криптографічних ключів. Процес управління ключами включає генерацію ключів, їх розподіл між користувачами, зберігання, використання, заміну та знищення після завершення терміну їх дії. У великих інформаційних системах використовуються спеціальні системи управління ключами, які дозволяють автоматизувати процеси роботи з криптографічними ключами.

Криптографічні методи широко застосовуються у різних сферах діяльності. Вони використовуються для захисту інформації у банківських системах, електронній комерції,

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

системах електронного документообігу, телекомунікаційних мережах, державних інформаційних системах та системах захисту критичної інфраструктури. Наприклад, криптографічні алгоритми застосовуються для захисту мережевих з'єднань у мережі Інтернет за допомогою протоколів SSL та TLS, які забезпечують захищений обмін даними між користувачами та вебсерверами[12].

Особливе значення криптографічний захист інформації має у системах електронного документообігу. Використання електронного цифрового підпису дозволяє забезпечити юридичну значущість електронних документів, підтвердити їх справжність та гарантувати цілісність інформації. У багатьох країнах використання електронного підпису регулюється спеціальними нормативно-правовими актами, які визначають порядок його застосування у сфері електронного документообігу.

Сучасний розвиток криптографії пов'язаний із появою нових викликів у сфері інформаційної безпеки. Одним із таких викликів є розвиток квантових обчислень, які потенційно можуть знизити ефективність традиційних криптографічних алгоритмів. У зв'язку з цим активно розробляються нові криптографічні алгоритми, стійкі до квантових атак. Такий напрям розвитку криптографії отримав назву постквантова криптографія.

Крім того, у сучасних системах криптографічного захисту активно застосовуються технології апаратного шифрування, криптографічні модулі безпеки, а також спеціалізовані пристрої для захисту криптографічних ключів. Використання таких технологій дозволяє значно підвищити рівень захищеності інформаційних систем.

Отже, криптографічний захист інформації є важливою складовою сучасної системи інформаційної та кібернетичної безпеки. Використання криптографічних методів дозволяє забезпечити конфіденційність, цілісність, автентичність та невідмовність інформації, що обробляється в інформаційних системах. Розвиток криптографічних технологій сприяє підвищенню рівня захищеності інформаційних ресурсів та створенню ефективних механізмів протидії сучасним кіберзагрозам.

Практичне заняття 6
Криптографічний захист інформації.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Сутність та основні завдання криптографічного захисту інформації.
2. Основні принципи забезпечення конфіденційності, цілісності та автентичності інформації за допомогою криптографії.
3. Класифікація криптографічних методів захисту інформації.
4. Симетричні криптографічні алгоритми та особливості їх застосування.
5. Асиметричні криптографічні системи та принципи використання відкритих ключів.
6. Криптографічні хеш-функції та їх роль у забезпеченні цілісності інформації.
7. Цифровий підпис як механізм забезпечення автентичності електронних документів.
8. Система управління криптографічними ключами у криптографічних системах захисту інформації.

ІІ. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Нормативно-правове регулювання криптографічного захисту інформації в Україні.

12 Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

2. Використання криптографічних технологій у системах електронного документообігу.

3. Сучасні криптографічні алгоритми та їх застосування у кібербезпеці.

4. Захищені протоколи передачі даних у комп'ютерних мережах.

5. Використання криптографії у системах електронної комерції та банківських операціях.

6. Роль криптографії у забезпеченні безпеки мережевих комунікацій.

7. Постквантова криптографія як перспективний напрям розвитку криптографічних технологій.

8. Апаратні засоби криптографічного захисту інформації в сучасних інформаційних системах.

III. Розв'язати тестові завдання:

1. Криптографічний захист інформації – це:

А) процес архівування даних

Б) сукупність методів перетворення інформації для забезпечення її захисту

В) процес копіювання інформації

Г) передавання інформації через мережу

2. Основною метою криптографічного захисту інформації є:

А) збільшення швидкості передачі даних

Б) забезпечення конфіденційності, цілісності та автентичності інформації

В) зменшення обсягу інформації

Г) оптимізація роботи комп'ютерної мережі

3. Процес перетворення відкритого тексту у зашифрований називається:

А) дешифрування

Б) шифрування

В) компресія

Г) архівування

4. Який криптографічний метод використовує один і той самий ключ для шифрування і дешифрування інформації?

А) асиметричне шифрування

Б) симетричне шифрування

В) хешування

Г) цифровий підпис

5. Який криптографічний метод використовує два ключі – відкритий та закритий?

А) симетричне шифрування

Б) асиметричне шифрування

В) хешування

Г) компресія

6. Який алгоритм належить до симетричних алгоритмів шифрування?

А) AES

Б) RSA
В) ElGamal
Г) DSA

7. Який алгоритм належить до асиметричних алгоритмів шифрування?
А) AES
Б) DES
В) RSA
Г) Blowfish

8. Який механізм використовується для перевірки цілісності інформації?
А) хеш-функція
Б) маршрутизація
В) кешування
Г) балансування

9. Яка технологія використовується для підтвердження авторства електронного документа?
А) цифровий підпис
Б) компресія
В) архівування
Г) резервне копіювання

10. Який криптографічний протокол використовується для захисту веб-з'єднань у мережі Інтернет?
А) TLS
Б) FTP
В) DNS
Г) SNMP

11. Під час передачі інформації через мережу використовується алгоритм шифрування, що забезпечує високий рівень захисту та широко застосовується у сучасних криптографічних системах. Який це алгоритм?
А) AES
Б) MD5
В) SHA-1
Г) CRC

12. У криптографічній системі використовується відкритий ключ для шифрування повідомлення та закритий ключ для його дешифрування. Який тип криптографічної системи використовується?
А) симетрична
Б) асиметрична
В) хеш-функція
Г) компресійна

13. Під час перевірки цілісності повідомлення використовується алгоритм, що формує унікальний цифровий відбиток даних. Який метод застосовується?

А) хешування

Б) маршрутизація

В) балансування

Г) резервування

14. У системі електронного документообігу використовується механізм, що забезпечує підтвердження авторства документа та гарантує його незмінність. Яка технологія використовується?

А) цифровий підпис

Б) кешування

В) компресія

Г) маршрутизація

15. У криптографічній системі безпеки використовується спеціальна процедура генерації, розподілу та зберігання криптографічних ключів. Як називається цей процес?

А) управління ключами

Б) маршрутизація

В) балансування

Г) кешування

16. Під час передачі інформації у мережі Інтернет використовується протокол, що забезпечує захищене з’єднання між браузером і сервером. Який це протокол?

А) TLS

Б) FTP

В) SMTP

Г) DHCP

17. Під час криптографічного захисту інформації використовується метод, при якому змінюється навіть найменша частина хеш-значення у разі зміни даних. Яку властивість забезпечує цей метод?

А) цілісність інформації

Б) доступність

В) масштабованість

Г) резервування

18. У криптографічній системі використовується алгоритм, що дозволяє виконувати шифрування великих обсягів даних з високою швидкістю. Який тип алгоритму застосовується?

А) симетричний

Б) асиметричний

В) хеш-функція

Г) цифровий підпис

19. Під час криптографічного захисту інформації використовується технологія, яка забезпечує неможливість заперечення факту відправлення повідомлення. Яку властивість забезпечує ця технологія?

А) невідмовність

Б) масштабованість

В) оптимізацію

Г) резервування

20. Під час кібератаки зловмисник намагається отримати доступ до криптографічного ключа, що використовується для дешифрування інформації. Який елемент криптографічної системи потребує посиленого захисту?

А) система управління криптографічними ключами

Б) маршрутизатор

В) кеш пам’яті

Г) балансувальник навантаження

Методичні рекомендації

Опрацювання теми, присвяченої криптографічному захисту інформації, є важливою складовою професійної підготовки здобувачів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». У сучасних умовах стрімкого розвитку інформаційних технологій, глобальних комп’ютерних мереж та цифрових сервісів питання забезпечення конфіденційності, цілісності та автентичності інформації набуває особливого значення. Криптографічні методи захисту інформації є одним із ключових інструментів забезпечення інформаційної та кібербезпеки, що широко застосовуються у державних інформаційних системах, банківських установах, системах електронного документообігу, електронної комерції та інших сферах.

Під час вивчення теми здобувачам рекомендується насамперед звернути увагу на сутність і призначення криптографічного захисту інформації. Необхідно усвідомити, що криптографія є науковою галуззю, яка досліджує методи перетворення інформації з метою забезпечення її захисту від несанкціонованого доступу. При цьому важливо зрозуміти основні завдання криптографічного захисту, зокрема забезпечення конфіденційності інформації, гарантування її цілісності, підтвердження автентичності даних та забезпечення невідмовності під час обміну електронними повідомленнями.

Особливу увагу слід приділити вивченню основних криптографічних методів захисту інформації. У межах теми необхідно розглянути особливості симетричних та асиметричних криптографічних алгоритмів, їх принципи функціонування, переваги та недоліки. Здобувачам доцільно проаналізувати відмінності між цими методами, а також сфери їх застосування у сучасних інформаційних системах.

Під час опрацювання теми необхідно також приділити увагу криптографічним хеш-функціям та їх використанню для забезпечення цілісності інформації. Здобувачам рекомендується розглянути принципи формування хеш-значень, їх властивості та роль у системах контролю цілісності даних. Особливу увагу слід звернути на застосування хеш-функцій у системах електронного підпису та у протоколах захищеного обміну даними.

Важливим елементом криптографічного захисту інформації є використання цифрових підписів. У межах вивчення теми здобувачам необхідно ознайомитися з принципами

створення та перевірки цифрового підпису, а також з його значенням у забезпеченні автентичності електронних документів. Доцільно також розглянути практичні аспекти застосування електронного підпису у системах електронного документообігу та електронних сервісах.

Особливу увагу слід приділити системам управління криптографічними ключами. Здобувачам необхідно зрозуміти, що ефективність криптографічного захисту значною мірою залежить від надійності генерації, зберігання та використання криптографічних ключів. У межах теми доцільно розглянути основні принципи управління ключами, зокрема їх генерацію, розподіл між користувачами, оновлення та знищення після завершення терміну дії.

Під час підготовки до практичних занять здобувачам рекомендується проаналізувати приклади використання криптографічних технологій у сучасних інформаційних системах. Особливу увагу слід приділити використанню криптографії у мережевих протоколах захищеного обміну даними, зокрема у протоколах SSL та TLS, які застосовуються для забезпечення безпечного передавання інформації у мережі Інтернет.

У процесі самостійної роботи здобувачам рекомендується опрацювати навчальну та наукову літературу, що стосується сучасних криптографічних технологій, а також ознайомитися з нормативно-правовими актами, які регулюють питання криптографічного захисту інформації. Доцільно також звернути увагу на сучасні тенденції розвитку криптографії, зокрема на дослідження у сфері постквантової криптографії.

Під час підготовки до підсумкового контролю необхідно систематизувати отримані знання щодо основних принципів криптографічного захисту інформації, типів криптографічних алгоритмів, механізмів забезпечення цілісності та автентичності даних, а також принципів управління криптографічними ключами. Особливу увагу слід приділити розумінню ролі криптографічних технологій у забезпеченні комплексної системи кіберзахисту.

Таким чином, опрацювання теми сприяє формуванню у здобувачів системного уявлення про сучасні криптографічні методи захисту інформації, розвиткові аналітичного мислення та здатності застосовувати криптографічні технології у практичній діяльності. Отримані знання є важливою складовою професійної підготовки фахівців у сфері кібербезпеки та необхідні для подальшої роботи у галузі захисту інформаційних систем, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. . Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 6
Криптографічний захист інформації.

1. Що розуміється під криптографічним захистом інформації та які його основні завдання?

2. Які основні принципи забезпечення конфіденційності, цілісності та автентичності інформації за допомогою криптографічних методів?

3. У чому полягають особливості симетричного шифрування та які його переваги і недоліки?

4. Які принципи лежать в основі асиметричних криптографічних систем?

5. Яке призначення криптографічних хеш-функцій та у яких сферах вони застосовуються?

6. Яким чином цифровий підпис забезпечує автентичність та юридичну значущість електронних документів?

7. Які основні етапи управління криптографічними ключами в інформаційних системах?

8. Які криптографічні протоколи використовуються для захищеної передачі інформації в комп’ютерних мережах?

9. Які сучасні загрози існують для криптографічних систем захисту інформації?

10. Які перспективи розвитку криптографічних технологій у сфері інформаційної та кібербезпеки?

ТЕМА 7. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.

Теоретичні засади та об'єкти технічного захисту інформації.
Технічні канали витоку інформації та загрози її безпеці.
Засоби, методи та системи технічного захисту інформації.
Організація, контроль та оцінювання ефективності технічного захисту інформації.

У сучасному інформаційному суспільстві інформація є одним із найважливіших стратегічних ресурсів держави, суспільства та окремих організацій. Вона використовується у процесах державного управління, фінансово-економічної діяльності, наукових досліджень, функціонування критичної інфраструктури, оборонної сфери, банківської системи, систем електронного урядування та інших сфер суспільного життя. Активний розвиток інформаційно-комунікаційних технологій, комп'ютерних мереж, цифрових сервісів і хмарних платформ значно розширив можливості створення, обробки, зберігання та передачі інформації. Водночас цифровізація суспільства супроводжується появою нових загроз інформаційній безпеці, зокрема несанкціонованого доступу до інформації, її перехоплення, модифікації, знищення або витоку через технічні канали. У таких умовах особливо важливого значення набуває технічний захист інформації, який є одним із ключових напрямів забезпечення інформаційної та кібербезпеки.

Технічний захист інформації являє собою комплекс організаційних, інженерно-технічних, програмно-технічних та спеціальних заходів, спрямованих на запобігання витоку інформації через технічні канали, несанкціонованому доступу до інформаційних ресурсів, а також на забезпечення безпеки інформації під час її обробки, зберігання та передачі в інформаційних системах. Основною метою технічного захисту інформації є створення таких умов функціонування інформаційних систем, за яких сторонні особи не можуть отримати доступ до інформації або здійснити несанкціонований вплив на інформаційні процеси.

Одним із ключових напрямів технічного захисту інформації є запобігання витоку інформації технічними каналами. Технічні канали витоку інформації виникають унаслідок фізичних процесів, що супроводжують роботу технічних засобів обробки інформації. До таких процесів належать електромагнітні випромінювання, акустичні коливання, вібрації, оптичні сигнали та інші фізичні явища[13]. За допомогою спеціальних технічних засобів такі сигнали можуть бути перехоплені та використані для відновлення інформації, що обробляється у відповідних інформаційних системах.

13 Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

Одним із найбільш небезпечних каналів витоку інформації є електромагнітний канал. Під час роботи комп'ютерної техніки, телекомунікаційного обладнання та інших електронних пристроїв виникають електромагнітні випромінювання, які можуть містити інформацію про оброблювані дані. Спеціальні технічні засоби дозволяють перехоплювати такі випромінювання на значній відстані та здійснювати їх аналіз з метою відновлення інформації. Для запобігання такому витоку інформації застосовуються спеціальні технічні заходи, зокрема екранування технічних засобів, використання спеціальних захищених приміщень, застосування фільтрів електромагнітних випромінювань та інші методи захисту.

Ще одним видом технічних каналів витоку інформації є акустичний канал. У процесі роботи технічних пристроїв можуть виникати звукові сигнали, які містять інформацію про виконувані операції або про дані, що обробляються у системі. Крім того, інформація може бути перехоплена під час розмов у приміщеннях за допомогою спеціальних технічних засобів прослуховування. Для запобігання витоку інформації через акустичні канали використовуються спеціальні технічні засоби шумового маскування, звукоізоляційні матеріали, а також пристрої, що генерують додаткові акустичні перешкоди.

Окрім електромагнітних та акустичних каналів витоку інформації існують також оптичні, вібраційні та інші технічні канали. Наприклад, оптичні канали витоку можуть виникати у випадках використання оптичних пристроїв або світлових сигналів, які можуть бути зафіксовані спеціальними технічними засобами. Вібраційні канали пов'язані з механічними коливаннями конструкцій будівель або технічних пристроїв, які можуть передавати інформацію про діяльність, що здійснюється у відповідних приміщеннях.

Важливим напрямом технічного захисту інформації є забезпечення безпеки інформаційних систем і телекомунікаційних мереж. Для цього використовуються різноманітні програмно-технічні засоби захисту, зокрема міжмережеві екрани, системи виявлення вторгнень, системи запобігання вторгненням, антивірусні програми, системи моніторингу мережевого трафіку та інші інструменти кіберзахисту. Використання таких засобів дозволяє контролювати доступ до інформаційних ресурсів, виявляти спроби несанкціонованого доступу та своєчасно реагувати на кібернетичні загрози.

Важливу роль у системі технічного захисту інформації відіграє фізичний захист інформаційної інфраструктури. Фізичний захист передбачає застосування комплексу технічних засобів, що забезпечують контроль доступу до приміщень, у яких розміщені інформаційні системи, серверне обладнання та інші технічні засоби обробки інформації. До таких засобів належать системи контролю та управління доступом, системи відеоспостереження, охоронна сигналізація, системи біометричної ідентифікації та інші технічні засоби безпеки[14].

Особливе значення має захист каналів зв'язку, через які передається інформація між різними інформаційними системами. Під час передачі інформації через телекомунікаційні мережі існує ризик її перехоплення або модифікації сторонніми особами. Для запобігання таким загрозам використовуються різні технічні засоби захисту, зокрема криптографічні методи шифрування інформації, використання захищених мережевих протоколів, застосування спеціалізованого мережевого обладнання та інші технології забезпечення безпеки мережевих комунікацій.

У сучасних умовах технічний захист інформації тісно пов'язаний із впровадженням комплексних систем захисту інформації. Такі системи поєднують організаційні, технічні та програмні заходи, спрямовані на забезпечення багаторівневого захисту інформаційних ресурсів. Комплексний підхід дозволяє враховувати різні види загроз інформаційній безпеці та забезпечувати ефективну протидію сучасним кіберзагрозам.

Важливою складовою технічного захисту інформації є проведення спеціальних технічних перевірок інформаційних систем. Такі перевірки здійснюються з метою виявлення можливих каналів витоку інформації, технічних вразливостей та інших факторів, що можуть

14 Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

негативно впливати на рівень інформаційної безпеки. У процесі таких перевірок використовуються спеціальні технічні засоби, що дозволяють оцінити рівень захищеності інформаційної інфраструктури.

Сучасний розвиток інформаційних технологій зумовлює необхідність постійного вдосконалення методів технічного захисту інформації. Поява нових технічних засобів обробки інформації, розвиток бездротових мереж, використання мобільних пристроїв, Інтернету речей та хмарних технологій створюють нові виклики у сфері інформаційної безпеки. У зв'язку з цим важливим завданням є розроблення нових технологій технічного захисту інформації та вдосконалення існуючих механізмів забезпечення безпеки інформаційних систем.

Отже, технічний захист інформації є важливою складовою сучасної системи забезпечення інформаційної та кібербезпеки. Використання технічних засобів захисту дозволяє запобігати витоку інформації через технічні канали, забезпечувати безпечне функціонування інформаційних систем та ефективно протидіяти сучасним загрозам інформаційній безпеці. Подальший розвиток технологій технічного захисту інформації є необхідною умовою забезпечення стабільного функціонування інформаційної інфраструктури держави, захисту інформаційних ресурсів та підвищення рівня кібербезпеки в умовах цифрової трансформації суспільства.

Практичне заняття 7
Технічний захист інформації.

ЗАВДАННЯ

І. Підготувати відповіді на теоретичні питання:

1. Сутність та основні завдання технічного захисту інформації.
2. Класифікація технічних каналів витоку інформації та їх характеристика.
3. Електромагнітні випромінювання як канал витоку інформації та методи їх нейтралізації.
4. Акустичні канали витоку інформації та засоби їх технічного блокування.
5. Фізичний захист інформаційної інфраструктури та контроль доступу до технічних засобів обробки інформації.
6. Програмно-технічні засоби забезпечення технічного захисту інформації в інформаційних системах.
7. Організація технічного захисту інформації у комп'ютерних мережах і телекомунікаційних системах.
8. Проведення спеціальних технічних перевірок для виявлення каналів витоку інформації.

ІІ. Підготувати реферати (доповіді) або презентації на запропоновану тематику:

1. Нормативно-правове регулювання технічного захисту інформації в Україні.
2. Інженерно-технічні заходи забезпечення захисту інформації у сучасних інформаційних системах.
3. Захист інформації від витоку через електромагнітні випромінювання.
4. Технології забезпечення фізичної безпеки інформаційної інфраструктури.
5. Використання систем відеоспостереження та контролю доступу у системах захисту інформації.

6. Засоби виявлення технічних пристроїв несанкціонованого зняття інформації.

7. Захист інформації у бездротових мережах та мобільних комунікаційних системах.

8. Перспективи розвитку технологій технічного захисту інформації в умовах цифрової трансформації.

ІІІ. Розв'язати тестові завдання:

1. Технічний захист інформації – це:

А) система архівування даних

Б) комплекс технічних і організаційних заходів, спрямованих на запобігання витоку інформації

В) процес резервного копіювання інформації

Г) передавання інформації через мережу

2. Основною метою технічного захисту інформації є:

А) підвищення швидкості обробки даних

Б) забезпечення захисту інформації від несанкціонованого доступу та витоку

В) зменшення обсягу інформації

Г) оптимізація роботи серверів

3. Канал витоку інформації, що виникає внаслідок електромагнітних випромінювань технічних пристроїв, називається:

А) акустичний канал

Б) електромагнітний канал

В) оптичний канал

Г) механічний канал

4. До технічних каналів витоку інформації належить:

А) електромагнітний

Б) акустичний

В) оптичний

Г) усі перелічені

5. Засоби контролю та управління доступом використовуються для:

А) шифрування інформації

Б) контролю доступу до приміщень і технічних засобів

В) компресії даних

Г) передачі інформації

6. Який із засобів використовується для захисту комп'ютерних мереж від несанкціонованого доступу?

А) міжмережевий екран

Б) архіватор

В) текстовий редактор

Г) медіаплеєр

7. Який засіб використовується для виявлення спроб несанкціонованого доступу до інформаційної системи?

А) система виявлення вторгнень

Б) антивірус

В) компілятор

Г) браузер

8. Захист приміщень, у яких розміщено інформаційні системи, належить до:

А) фізичного захисту інформації

Б) криптографічного захисту

В) програмного захисту

Г) мережевого адміністрування

9. Який технічний засіб використовується для спостереження за приміщеннями?

А) система відеоспостереження

Б) текстовий редактор

В) маршрутизатор

Г) архіватор

10. Захист інформації у мережах передачі даних забезпечується за допомогою:

А) захищених протоколів зв’язку

Б) графічних редакторів

В) офісних програм

Г) комп’ютерних ігор

11. Під час роботи комп’ютерного обладнання виникають електромагнітні сигнали, які можуть бути перехоплені спеціальними пристроями. Який канал витоку інформації описано?

А) електромагнітний

Б) акустичний

В) оптичний

Г) програмний

12. У приміщенні встановлено систему генерації шуму для ускладнення перехоплення розмов. Який тип захисту реалізовано?

А) акустичний захист інформації

Б) криптографічний захист

В) програмний захист

Г) мережевий захист

13. У системі безпеки використовується обладнання, що обмежує фізичний доступ до серверної кімнати за допомогою електронних карток. Який тип захисту реалізується?

А) фізичний захист інформації

Б) криптографічний захист

В) логічний захист

Г) програмний захист

14. Організація проводить перевірку інформаційної системи з метою виявлення технічних каналів витоку інформації. Як називається такий процес?

А) спеціальна технічна перевірка

Б) резервне копіювання

В) дефрагментація

Г) компіляція

15. Який технічний засіб використовується для фільтрації мережевого трафіку та контролю доступу до мережі?

А) міжмережевий екран

Б) модем

В) архіватор

Г) принтер

16. У мережі використовується система, яка аналізує мережевий трафік та повідомляє адміністратора про можливі атаки. Яка система використовується?

А) система виявлення вторгнень

Б) система архівування

В) система резервного копіювання

Г) система стиснення

17. Під час роботи інформаційної системи здійснюється постійний аналіз мережевої активності з метою запобігання атакам. Який процес реалізується?

А) моніторинг безпеки

Б) компіляція програм

В) форматування диска

Г) архівування

18. Захист інформації шляхом екранування обладнання та зниження електромагнітних випромінювань належить до:

А) технічного захисту інформації

Б) криптографічного захисту

В) програмного захисту

Г) адміністративного управління

19. У системі безпеки використовуються камери відеоспостереження, датчики руху та сигналізація. Який тип захисту реалізується?

А) фізичний захист інформаційної інфраструктури

Б) криптографічний захист

В) програмний захист

Г) логічний контроль доступу

20. Який із перелічених підходів передбачає використання різних методів і засобів захисту інформації одночасно?

А) комплексний захист інформації

Б) локальний захист
В) частковий захист
Г) базовий захист

Методичні рекомендації

Вивчення теми, присвяченої технічному захисту інформації, є важливою складовою професійної підготовки здобувачів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». У сучасних умовах цифровізації суспільства, активного використання інформаційно-комунікаційних технологій та зростання кількості кіберзагроз особливого значення набуває забезпечення надійного захисту інформаційних ресурсів від несанкціонованого доступу, перехоплення та витоку через технічні канали. Технічний захист інформації є одним із ключових напрямів забезпечення інформаційної та кібербезпеки, оскільки він передбачає використання спеціальних технічних засобів і методів для запобігання витоку інформації та забезпечення безпечного функціонування інформаційних систем.

Під час опрацювання теми здобувачам рекомендується насамперед зосередити увагу на розумінні сутності технічного захисту інформації, його місця у загальній системі забезпечення інформаційної безпеки та основних завдань, що вирішуються у межах цього напряму. Важливо усвідомити, що технічний захист інформації передбачає комплексне застосування інженерно-технічних, програмно-технічних та організаційних заходів, спрямованих на запобігання витоку інформації через технічні канали та на забезпечення безпеки інформаційних систем.

Особливу увагу під час вивчення теми необхідно приділити класифікації технічних каналів витоку інформації. Здобувачам рекомендується розглянути основні види таких каналів, зокрема електромагнітні, акустичні, оптичні та вібраційні канали витоку інформації. Необхідно зрозуміти фізичну природу виникнення таких каналів, а також можливі способи їх використання для перехоплення інформації.

Важливим аспектом опрацювання теми є вивчення технічних засобів запобігання витоку інформації. До таких засобів належать системи екранування технічних пристроїв, спеціальні фільтри електромагнітних випромінювань, засоби акустичного маскування, системи генерації шуму, а також інші технічні пристрої, що дозволяють зменшити ризик витоку інформації через технічні канали.

Здобувачам також рекомендується приділити увагу питанням фізичного захисту інформаційної інфраструктури. У межах цієї теми необхідно розглянути використання систем контролю та управління доступом, систем відеоспостереження, охоронної сигналізації та інших технічних засобів, що забезпечують захист приміщень і технічних засобів обробки інформації від несанкціонованого доступу.

Під час вивчення теми важливо також ознайомитися з програмно-технічними засобами забезпечення технічного захисту інформації в інформаційних системах і комп’ютерних мережах. До таких засобів належать міжмережеві екрани, системи виявлення вторгнень, системи запобігання вторгненням, антивірусні програми та інші інструменти кіберзахисту, що дозволяють контролювати доступ до інформаційних ресурсів і виявляти потенційні загрози інформаційній безпеці.

Окрему увагу під час опрацювання теми необхідно приділити організації технічного захисту інформації в інформаційно-комунікаційних системах. Здобувачам рекомендується

проаналізувати принципи побудови систем технічного захисту інформації, етапи їх створення та впровадження, а також роль комплексного підходу до забезпечення інформаційної безпеки.

У процесі самостійної роботи здобувачам доцільно опрацювати навчальні та наукові джерела, що стосуються сучасних технологій технічного захисту інформації, а також ознайомитися з нормативно-правовими актами, які регулюють питання захисту інформації в інформаційно-телекомунікаційних системах. Особливу увагу слід приділити аналізу сучасних технічних загроз інформаційній безпеці та методів їх нейтралізації.

Під час підготовки до підсумкового контролю необхідно систематизувати знання щодо основних принципів технічного захисту інформації, видів технічних каналів витоку інформації, засобів їх виявлення та нейтралізації, а також методів забезпечення безпеки інформаційних систем. Важливо розуміти взаємозв'язок між технічними, організаційними та програмними заходами забезпечення інформаційної безпеки.

Таким чином, опрацювання теми сприяє формуванню у здобувачів системного уявлення про технічні методи захисту інформації, розвиткові навичок аналізу технічних загроз інформаційній безпеці та здатності застосовувати сучасні технічні засоби захисту інформації у практичній діяльності. Отримані знання є важливою складовою професійної підготовки фахівців у сфері кібербезпеки та необхідні для подальшої роботи у галузі захисту інформаційних систем, а також для успішного складання єдиного державного кваліфікаційного іспиту.

***Перелік посилань*:**

1. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Самостійна робота 7
Технічний захист інформації.

1. Що розуміється під технічним захистом інформації та які його основні завдання?
2. Які основні види технічних каналів витоку інформації існують?
3. У чому полягає сутність електромагнітного каналу витоку інформації?
4. Які технічні засоби застосовуються для запобігання витоку інформації через електромагнітні випромінювання?
5. Яким чином може здійснюватися витік інформації через акустичні канали?
6. Які технічні методи використовуються для захисту інформації від витоку через акустичні канали?
7. Яку роль відіграє фізичний захист інформаційної інфраструктури у системі технічного захисту інформації?
8. Які програмно-технічні засоби застосовуються для забезпечення технічного захисту інформаційних систем?
9. Яким чином здійснюється контроль доступу до технічних засобів обробки інформації?
10. Які сучасні технічні загрози існують для інформаційних систем і які методи використовуються для їх нейтралізації?

ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Сутність інформаційної безпеки та її роль у забезпеченні національної безпеки держави.
2. Основні складові інформаційної безпеки та їх характеристика.
3. Законодавча база України у сфері інформаційної та кібербезпеки.
4. Міжнародні стандарти та практики у сфері інформаційної безпеки.
5. Основні принципи організації системи кібербезпеки в інформаційних системах.
6. Державна політика у сфері кібербезпеки та захисту інформації.
7. Нормативно-правове регулювання захисту інформації в інформаційно-телекомунікаційних системах.
8. Основні поняття та категорії інформаційних технологій у сфері кібербезпеки.
9. Роль інформаційних технологій у забезпеченні безпеки інформаційних ресурсів.
10. Архітектура сучасних інформаційних систем та її значення для забезпечення безпеки.
11. Загрози інформаційній безпеці в інформаційно-комунікаційних системах.
12. Основні принципи захисту інформаційно-комунікаційних систем.
13. Механізми забезпечення конфіденційності, цілісності та доступності інформації.
14. Методи ідентифікації та автентифікації користувачів в інформаційних системах.
15. Управління доступом до інформаційних ресурсів.
16. Захист інформації в комп’ютерних мережах.
17. Міжмережеві екрани та їх роль у забезпеченні кібербезпеки.
18. Системи виявлення та запобігання вторгненням у комп’ютерних мережах.
19. Захист інформації у бездротових мережах.
20. Безпека мережевих протоколів та захищених каналів передачі даних.
21. Комплексні системи захисту інформації та принципи їх побудови.
22. Основні етапи створення комплексних систем захисту інформації.
23. Організаційні заходи у системі забезпечення інформаційної безпеки.
24. Технічні засоби забезпечення захисту інформації.
25. Програмні засоби захисту інформаційних систем.
26. Управління інформаційною безпекою в організаціях.
27. Політика інформаційної безпеки та її роль у системі управління безпекою.
28. Управління ризиками у сфері інформаційної безпеки.
29. Процеси моніторингу та аудиту інформаційної безпеки.
30. Управління інцидентами інформаційної безпеки.
31. Основні принципи криптографічного захисту інформації.
32. Симетричні криптографічні алгоритми та їх застосування.
33. Асиметричні криптографічні алгоритми та системи відкритих ключів.
34. Криптографічні хеш-функції та їх роль у забезпеченні цілісності інформації.
35. Цифровий підпис та його застосування в електронному документообігу.
36. Управління криптографічними ключами у системах захисту інформації.
37. Захищені криптографічні протоколи передачі інформації.
38. Технічний захист інформації та його основні завдання.
39. Класифікація технічних каналів витоку інформації.
40. Захист інформації від витоку через електромагнітні випромінювання.
41. Акустичні канали витоку інформації та методи їх нейтралізації.

42. Фізичний захист інформаційної інфраструктури.
43. Засоби контролю та управління доступом до інформаційних ресурсів.
44. Використання систем відеоспостереження у забезпеченні безпеки інформаційних систем.
45. Захист інформації у телекомунікаційних мережах.
46. Проведення технічних перевірок інформаційних систем.
47. Сучасні кіберзагрози та методи протидії їм.
48. Комплексний підхід до забезпечення інформаційної та кібербезпеки.
49. Перспективи розвитку технологій кібербезпеки в умовах цифровізації.
50. Роль фахівців з кібербезпеки у забезпеченні захисту інформаційних ресурсів.
51. Кіберризики: поняття, види та підходи до їх оцінювання.
52. Соціальна інженерія як загроза інформаційній безпеці та способи протидії їй.
53. Шкідливе програмне забезпечення: види, ознаки та методи захисту від нього.
54. Резервне копіювання даних та його значення для забезпечення безперервності діяльності.
55. Хмарні технології та особливості забезпечення безпеки даних у хмарному середовищі.
56. Безпека мобільних пристроїв і мобільних застосунків.
57. Інциденти витоку персональних даних та механізми їх запобігання.
58. Безпека електронного документообігу та електронних комунікацій.
59. Кібергігієна користувачів як елемент системи інформаційної безпеки.
60. Міжнародне співробітництво у сфері протидії кіберзлочинності та забезпечення кібербезпеки.

ТЕСТОВІ ЗАВДАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Основною метою кібербезпеки є:

А) зменшення обсягу інформації

Б) захист інформаційних систем та даних від кіберзагроз

В) оптимізація роботи програм

Г) збільшення швидкості Інтернету

2. До основних властивостей інформаційної безпеки належать:

А) масштабованість, продуктивність, стабільність

Б) конфіденційність, цілісність, доступність

В) архівація, резервування, синхронізація

Г) компресія, кодування, кешування

3. Який державний орган координує питання кібербезпеки в Україні?

А) Державна служба спеціального зв’язку та захисту інформації України

Б) Міністерство фінансів

В) Міністерство освіти

Г) Національний банк України

4. Основною метою автентифікації користувача є:

А) перевірка справжності користувача

Б) шифрування даних

В) створення резервних копій

Г) стиснення інформації

5. Який механізм дозволяє визначити, які ресурси доступні користувачу після автентифікації?

А) авторизація

Б) маршрутизація

В) кешування

Г) архівація

6. Який компонент системи безпеки контролює мережевий трафік між мережами?

А) проксі-сервер

Б) міжмережевий екран

В) браузер

Г) компілятор

7. Який тип атаки передбачає перевантаження сервера великою кількістю запитів?

А) SQL-ін’єкція

Б) DDoS-атака

В) фішинг

Г) spoofing

8. Яка технологія використовується для безпечного зберігання резервних копій даних?

А) резервне копіювання

Б) дефрагментація

В) компіляція

Г) оптимізація

9. Яка система призначена для централізованого збору та аналізу подій безпеки?

А) SIEM

Б) DNS

В) FTP

Г) SMTP

10. Який тип програмного забезпечення призначений для виявлення шкідливих програм?

А) антивірус

Б) текстовий редактор

В) компілятор

Г) браузер

11. Яка модель безпеки передбачає обмеження доступу до інформації відповідно до рівня секретності?

А) модель Белла-ЛаПадули

Б) модель OSI

В) модель TCP/IP

Г) модель ISO

12. Яка технологія використовується для ізоляції програм у середовищі виконання?

А) sandbox

Б) кешування

В) архівування

Г) компресія

13. Який механізм використовується для багатофакторної автентифікації?

А) використання кількох незалежних методів перевірки

Б) використання одного пароля

В) використання одного токена

Г) використання однієї IP-адреси

14. Який протокол використовується для захищеного віддаленого доступу до серверів?

А) SSH

Б) HTTP

В) FTP
Г) Telnet

15. Яка технологія використовується для ізоляції мережевого трафіку у віртуальних мережах?
А) VLAN
Б) BIOS
В) RAM
Г) DNS

16. Який метод використовується для перевірки цілісності файлів?
А) контрольні суми
Б) архівація
В) маршрутизація
Г) кешування

17. Який тип програмного забезпечення використовується для аналізу мережевого трафіку?
А) аналізатор пакетів
Б) компілятор
В) текстовий редактор
Г) медіаплеєр

18. Яка технологія використовується для захисту веб-додатків від атак типу SQL injection?
А) параметризовані запити
Б) кешування
В) маршрутизація
Г) компресія

19. Який компонент забезпечує фільтрацію електронної пошти від спаму?
А) антиспам-фільтр
Б) проксі-сервер
В) маршрутизатор
Г) браузер

20. Яка технологія використовується для створення захищених тунелів у мережі?
А) VPN
Б) DHCP
В) ARP
Г) DNS

21. У системі безпеки використовується модель, яка забороняє користувачам читати інформацію з вищим рівнем секретності. Яку модель описано?
А) модель Белла-ЛаПадули
Б) модель Біба

В) модель Кларка-Вілсона
Г) модель Харрісона

22. Під час аналізу мережі виявлено підміну IP-адреси джерела трафіку. Який тип атаки відбувається?

А) IP spoofing
Б) phishing
В) ransomware
Г) brute force

23. Який принцип безпеки передбачає надання користувачам лише мінімально необхідних прав доступу?

А) принцип мінімальних привілеїв
Б) принцип відкритого доступу
В) принцип повного контролю
Г) принцип резервування

24. У системі кібербезпеки використовується метод аналізу поведінки користувачів для виявлення аномалій. Який тип системи застосовується?

А) система поведінкового аналізу
Б) система резервування
В) система компресії
Г) система архівації

25. У процесі тестування безпеки спеціалісти імітують атаки на систему для виявлення її вразливостей. Як називається такий процес?

А) penetration testing
Б) резервне копіювання
В) архівація
Г) дефрагментація

26. Який тип шкідливого програмного забезпечення блокує доступ до даних та вимагає викуп?

А) ransomware
Б) spyware
В) adware
Г) rootkit

27. У системі безпеки використовується механізм, який дозволяє централізовано керувати доступом до ресурсів у мережі. Яку технологію застосовано?

А) управління ідентифікацією та доступом
Б) резервне копіювання
В) компресія
Г) кешування

28. Під час атаки зловмисник перехоплює мережевий трафік між двома користувачами. Який тип атаки описано?

А) Man-in-the-Middle

Б) DoS

В) brute force

Г) phishing

29. Який принцип безпеки передбачає регулярну перевірку ефективності засобів захисту інформації?

А) аудит безпеки

Б) резервування

В) оптимізація

Г) дефрагментація

30. У системі кібербезпеки використовується підхід, при якому жоден користувач або пристрій не вважається довіреним за замовчуванням. Яка модель використовується?

А) Zero Trust

Б) Open Network

В) Trusted Network

Г) Local Security

31. Основним призначенням системи управління інцидентами інформаційної безпеки є:

А) підвищення швидкості обробки даних

Б) виявлення, аналіз та усунення наслідків кіберінцидентів

В) архівування інформації

Г) оптимізація мережевого трафіку

32. Який метод використовується для пошуку вразливостей у програмному забезпеченні?

А) сканування вразливостей

Б) резервне копіювання

В) архівування

Г) дефрагментація

33. Який інструмент використовується для фіксації подій, що відбуваються у системі?

А) журнал подій

Б) текстовий редактор

В) компілятор

Г) браузер

34. Яка технологія дозволяє відновити дані у разі їх втрати або пошкодження?

А) резервне копіювання

Б) маршрутизація

В) кешування
Г) компресія

35. Який основний ризик існує під час використання хмарних технологій?
А) перевищення обсягу пам’яті
Б) несанкціонований доступ до даних
В) зменшення швидкості процесора
Г) дефрагментація диска

36. Який підхід застосовується для управління мобільними пристроями у корпоративних мережах?
А) MDM (Mobile Device Management)
Б) DNS
В) FTP
Г) HTTP

37. Яка атака передбачає впровадження шкідливого коду у вебсторінку для виконання у браузері користувача?
А) XSS-атака
Б) DDoS-атака
В) SQL-ін’єкція
Г) brute force

38. Яка процедура передбачає регулярне встановлення оновлень програмного забезпечення для усунення вразливостей?
А) управління патчами
Б) резервне копіювання
В) маршрутизація
Г) кешування

39. Яка особливість систем Інтернету речей створює додаткові ризики для безпеки?
А) велика кількість підключених пристроїв
Б) використання клавіатури
В) використання моніторів
Г) використання принтерів

40. Який тип системи використовується для управління доступом користувачів до баз даних?
А) система управління базами даних
Б) текстовий редактор
В) браузер
Г) медіаплеєр

41. Яка функція журналювання подій є ключовою для забезпечення кібербезпеки?

А) фіксація дій користувачів і системних подій
Б) підвищення швидкості мережі
В) архівування документів
Г) оптимізація програм

42. Який тип загроз виникає з боку співробітників організації?
А) внутрішні загрози
Б) зовнішні загрози
В) мережеві загрози
Г) технічні загрози

43. Який механізм використовується для захисту облікових записів користувачів?
А) багатофакторна автентифікація
Б) архівування
В) кешування
Г) дефрагментація

44. Який метод використовується для підвищення стійкості інформаційних систем до збоїв?
А) резервування ресурсів
Б) компресія
В) дефрагментація
Г) маршрутизація

45. Який засіб використовується для захисту внутрішньої мережі організації?
А) система мережевого захисту
Б) текстовий редактор
В) компілятор
Г) браузер

46. Яка технологія використовується для захисту електронної пошти від шкідливих повідомлень?
А) антиспам-фільтрація
Б) маршрутизація
В) кешування
Г) архівація

47. Яка технологія штучного інтелекту використовується для виявлення аномальної активності у мережах?
А) машинне навчання
Б) компіляція
В) дефрагментація
Г) компресія

48. Яка технологія дозволяє автоматизувати реагування на кіберінциденти?

А) SOAR
Б) FTP
В) HTTP
Г) DNS

49. Який об’єкт належить до критичної інформаційної інфраструктури?
А) енергетичні системи
Б) текстові редактори
В) ігрові програми
Г) медіаплеєри

50. Який принцип забезпечує багаторівневий захист інформаційних систем?
А) принцип глибокої оборони
Б) принцип відкритого доступу
В) принцип централізації
Г) принцип спрощення

□

РЕКОМЕНДОВАНИЙ ПЕРЕЛІК ДЖЕРЕЛ

Нормативно-правові акти

1. Конституція України: Закон України від 28. 06. 1996 р. № 254к/96-ВР/ Верховна Рада України.URL : https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. Про інформацію: Закон України «Про інформацію» від 02.10.1992 № 2657-XII/ Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Про державну таємницю : Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII/ Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12/ed20230331#Text
4. Про захист інформації в інформаційно-комунікаційних системах : Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР/ Верховна Рада України. URL: https://zakon.rada.gov.ua/go/80/94-вр
5. Про основні засади забезпечення кібербезпеки України: Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII/ Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19
6. Про затвердження Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 року № 373/ Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/go/373-2006-п
7. Питання забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах : Постанова Кабінету Міністрів України від 8 лютого 2021 р. № 92 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/go/92-2021-п
8. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 8 жовтня 1997 р. № 1126 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/go/1126-97-п
9. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29 грутня 2021 р. №14261126 / Кабінет Міністрів України. URL: https://zakon.rada.gov.ua/go/1426-2021-п
10. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229/99 / Президент України. URL: https://zakon.rada.gov.ua/go/1229/99
11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України; Стратегія від 26.08.2021 № 447/2021 / Президент України. URL: https://zakon.rada.gov.ua/go/447/2021
12. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016/ Президент України. URL: https://zakon.rada.gov.ua/go/242/2016
13. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI/ Верховна Рада України. URL : https://zakon.rada.gov.ua/go/4651-17
14. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III/ Верховна Рада України. URL : https://zakon.rada.gov.ua/go/2341-14
15. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001/ Рада Європи. URL : https://zakon.rada.gov.ua/go/994_575

Основні джерела

1. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ : Юрінком Інтер, 2025. 236 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. Одеса.: ОНАЗ ім. О.С. Попова, 320 с.

4. Державно-правовий експеримент в галузі інформатизації: монографія / Я.Ю. Дорогий, І. О. Бердиченко, О. О. Кульчій. Полтава : ПУЕТ, 2022. 137 с.

5. Інформаційна безпека та кібербезпека держави: навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська; за заг.ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.

6. Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

7. Основи кіберпростору, кібербезпеки та кіберзахисту: навч. посібник /В. М. Богуш, В.В. Богуш, В. Д. Бровко, В. П. Настрадін; під ред. В. М. Богуша. Київ : Видавництво Ліра-К, 2022. 554 с.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монографія. Київ ; Одеса : Фенікс, 2020. 400 с.

9. Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України : автореф. дис. ... докт. юрид. наук : 12.00.07; Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 38 с.

Допоміжні джерела

1. Аркуша Л.І. Чернов О. В., Хижняк Є.С. Деякі особливості вилучення та автентифікації цифрових доказів із мобільних пристроїв при розслідуванні фішингових атак. *Наукові праці Міжрегіональної Академії управління персоналом*. Випуск 1 (77). 2026. С. 6-15. DOI https://doi.org/10.32689/2522-4603.2026.1.1 URL: https://journals.maup.com.ua/index.php/law/article/view/5608/5901

2. Аркуша Л.І., Чернов О.В., Мейта К.В. Цифрова криміналістика як інструмент ідентифікації суб'єктів та механізмів реалізації інформаційно-психологічних операцій в мережевому середовищі. *Держава та регіони*. Серія Право. 2026. № 1 (91). С. 80-87. URL: https://law.stateandregions.zp.ua/archive/1_2026/13.pdf DOI https://doi.org/10.32782/1813-338X-2026.1.11

3. Аркуша Л.І., Чернов О. В., Дикий О.В. Криміналістичні аспекти виявлення та фіксації цифрових слідів фінансового шахрайства в платіжних системах. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2026 № 79. С. 120-127. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc79/25.pdf DOI https://doi.org/10.32782/2307-1745.2026.79.23

4. Аркуша Л.І., Чернов О. В., Дикий О.В. Ідентифікація суб'єктів кіберзлочинів шляхом інтелектуального аналізу поведінкових цифрових слідів. *Правова позиція.* № 1 (50), 2026. С. 68-74. URL: https://www.legalposition.umsf.in.ua/archive/2026/1/15.pdf, DOI https://doi.org/10.32782/2521-6473.2026-1.13

5. Бердиченко І. О. Законодавчі новації в сфері кіберзахисту критичної інформаційної інфраструктури, шляхи подальшого удосконалення. Кібербезпека в сучасному світі: матеріали II Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. Одеса : Видавничий дім «Гельветика», 2020. С. 8-13.

6. Бердиченко І. О. Питання дотримання балансу інтересів при законодавчому врегулюванні механізмів протидії кіберзагрозам. VII Юридичні могилянські читання : Всеукр. наук.- практ. конф.: програма та тези / ЧНУ ім. Петра Могили. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2021. С.74-78

7. Біленчук П. Д. Кібербезпека радіаційних випробувань космічних апаратів: правові засади, регламентні вимоги та стан їх інноваційного забезпечення. *Юридичний вісник. Повітряне і космічне право*. 2020. № 4. С. 156-162. URL: http://nbuv.gov.ua/UJRN/Npnau_2020_4_24 15.

8. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий журнал*. 2023. № 1. С. 267-270.

9. Грубінко А. В. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. *Актуальні проблеми правознавства*. 2021. Вип. 1. С. 5-10. URL: http://nbuv.gov.ua/UJRN/aprpr_2021_1_3

10. Мандзюк О.А. Роль аналітичної діяльності та аналітичних центрів у формуванні й реалізації кібербезпекової політики. URL: http://goal-int.org/rol-analitichnoi-diyalnosti-ta-analitichnix-centriv-u-formuvanni-j-realizacii-kiberbezpekovoi- politiki/

11. Островий О.В. Інструменти державної політики забезпечення кібернетичної безпеки. URL: https://www.inter-nauka.com/uploads/public/15596540123683.pdf

12. Семенченко А. І. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку. *Проблеми програмування*. 2020. № 2-3. С. 278-286

13. Філінович В. В. Кібербезпека та Інтернет речей: правовий аспект. *Юридичний вісник. Повітряне і космічне право*. 2020. № 4. С. 122-127. URL: http://nbuv.gov.ua/UJRN/Npnau_2020_4_19

14. CERT-UA: швидка кібердопомога URL: https://www.pcweek.ua/themes/detail.php?ID=147850

15. Larysa Arkusha, Oleh Dykyi, Mykhailo Kosiuta, Nataliia Fedchun, Mariia Diachkova, Bogdan Osadchyi. The Impact of Digitalization on the Level of Crime during the Pandemic. *International Journal of Computer Science and Network Security.* Vol. 22 No. 11 pp. 399-404. http://paper.ijcsns.org/07_book/202211/20221157.pdf

Ресурси відкритого доступу

1. www.president.gov.ua – Президент України
2. www.kmu.gov.ua – Єдиний веб-портал послуг
3. www.nabu.gov.ua – Національне антикорупційне бюро України
4. www.tzi.com.ua – Технічний захист інформації
5. www.sbu.gov.ua – Служба безпеки України
6. www.cyberpolice.gov.ua – Департамент кіберполіції Національної поліції України

7. www.cip.gov.ua/ua – Державна служба спеціального зв’язку та захисту інформації України
8. https://cip.gov.ua/ua/news/perelik-aktiv-zakonodavstva-u-sferi-tekhnichnogo-zakhistu-informaciyi – Державної служби спеціального зв’язку та захисту інформації України (перелік актів законодавства у сфері технічного захисту інформації)
9. https://scpc.gov.ua/uk – Державний центр кіберзахисту та протидії кіберзагрозам
10. http://dspace.onua.edu.ua – eNUOLAIR – депозитарій (архів) НУ «ОЮА»
11. https://www.scopus.com/ – База даних SCOPUS
12. http://ipscience.thomsonreuters.com – База даних Thomson Reuters Web of Science

НАВЧАЛЬНО-МЕТОДИЧНЕ ВИДАННЯ

Лариса Ігорівна Аркуша
Олександр Віталійович Чернов
Олег Вікторович Дикий
Ірина Юріївна Пишненко

КІБЕРБЕЗПЕКА (підготовка до ЄДКІ)

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»/ F5 «Кібербезпека та захист інформації»

Електронне видання

В авторській редакції

Формат 60х84/16. Ум-друк. арк. …..

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net