МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Кафедра Комп'ютерної інженерії та інноваційних технологій
Кафедра комп'ютерних наук

Йона Л.Г., Педяш В.В., Русу О.П.

ІНФОРМАЦІЙНА БЕЗПЕКА ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ

Методичні рекомендації для самостійної роботи здобувачів

Одеса 2024

Затверджено Вченою Радою Міжнародного гуманітарного університету (протокол № 13 від 16.08.2024 р.)

Йона Л.Г., Педяш В.В., Русу О.П.

Інформаційна безпека інноваційної діяльності: методичні рекомендації для самостійної роботи здобувачів [Електронне видання]. / **Йона Л.Г., Педяш В.В., Русу О.П.** Кафедра Комп'ютерної інженерії та інноваційних технологій, Кафедра комп'ютерних наук Міжнародного гуманітарного університету. Одеса, 2024. – 34 с.

Методичні рекомендації з курсу «**Інформаційна безпека інноваційної діяльності**» розроблено відповідно до навчального плану. Матеріали складаються з навчальної програми курсу, методичних рекомендацій з проведення практичних занять і завдань для самостійної роботи здобувачів, списку рекомендованої літератури. Призначено для студентів другого (магістерського) рівня вищої освіти факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету.

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="6">Кількість кредитів – 4, загальна кількість годин – 120</td><td rowspan="6">Галузь 12 – Інформаційні технології
Спеціальність – 125 «Кібербезпека та захист інформації»</td><td colspan="2">обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>2-й</td></tr>
<tr><td rowspan="12">Мова навчання – українська</td><td rowspan="12">Рівень вищої освіти – другий (магістерський) рівень</td><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>6год</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>22 год.</td><td>6 год</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>76 год.</td><td>108год</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Дисципліна **«Інформаційна безпека інноваційної діяльності»** формує у здобувачів необхідний обсяг теоретичних і практичних знань про основні технології, що реалізуються концепцією захисту інформації, яка зберігається та передається у телекомунікаційних системах та мережах від порушення її властивостей, а саме конфіденційності, цілісності та доступності, надання знань фахівцям з сучасних методів захисту інформаційного середовища інноваційних підприємств, тенденцій в галузі захисту інноваційної діяльності, аналіз загроз та ризиків витоку конфіденційної інформації для забезпечення конкурентних переваг інноваційних підприємств, особливостей формування і роботи систем інформаційної безпеки в інноваційних підприємствах та організаціях.

Метою викладання навчальної дисципліни «Інформаційна безпека інноваційної діяльності» є забезпечення здобувачів знаннями з питань попередження, прогнозування та мінімізації втрат від несанкціонованого доступу до конфіденційної інформації при інноваційній діяльності у системах комунікацій з урахуванням сучасного стану та перспективних напрямів розвитку систем та технологій захисту інформації; сформувати у здобувача здатність досліджувати,

розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Передумови для вивчення дисципліни – знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки.

ЗАПЛАНОВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ ЗА НАВЧАЛЬНОЮ ДИСЦИПЛІНОЮ

Обов’язкова навчальна дисципліна формує у здобувачів наступні компетентності, переджбачені освітньою програмою.

Інтегральна компетентність

ІК. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

У результаті вивчення цієї навчальної дисципліни здобувач має набути такі компетентності.

Знати:

– основи державного регулювання інноваційної діяльності в Україні;

– загрози та ризики витоку конфіденційної інформації для забезпечення конкурентних переваг інноваційних підприємств;

– методи захисту конфіденційної інформації при інноваційній діяльності;

– сучасні тенденції в галузі захисту інформації інноваційного підприємства;

– засоби одержання несанкціонованого доступу до конфіденційної інформації;

– організацію системи промислової та економічної контррозвідки в інноваційних організаціях;

– основні положення політики інформаційної безпеки при інноваційної діяльності;

– основні функції служби захисту інформації інноваційної організації;

– особливості моніторингу системи інформаційної безпеки в інноваційних організаціях.

Вміти:

– враховувати загрози та ризики витоку конфіденційної інформації з метою забезпечення конкурентних переваг інноваційної діяльності;

– використовувати основні методи захисту конфіденційної інформації при інноваційній діяльності;

– використовувати сучасні тенденції в галузі захисту інформації інноваційного підприємництва;

– враховувати засоби одержання несанкціонованого доступу до конфіденційної інформації;

– враховувати особливості нормативно-правового регулювання інноваційної діяльності;

– враховувати організацію системи промислової та економічної контррозвідки в інноваційних організаціях;

– враховувати основні положення політики інформаційної безпеки в інноваційних організаціях;

– використовувати основні функції служби захисту інформації інноваційної організації та особливості моніторингу системи інформаційної безпеки в інноваційних організаціях.

2 ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основні поняття та визначення. Інноваційні процеси та їх класифікація. Стан сучасної кібербезпеки та шляхи розвитку на майбутнє. Конкурентні переваги при інноваційній діяльності.

Тема 2. Загрози та ризики витоку конфіденційної інформації. Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.

Тема 3. Сучасні тенденції в галузі захисту інформації інноваційного підприємництва. Комерційна інформація та комерційна таємниця.

Тема 4. Структура і завдання політики інформаційної безпеки. Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства. Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT).

Тема 5. Соціальна інженерія. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.

Тема 6. Управління контролем доступу. Основна функція управління контролю доступом.

Тема 7. Перспективи систем забезпечення інформаційної безпеки кіберпростору. Кібербезпека комунікаційних систем і мереж.

Тема 8. Засоби захисту від витоку інформації в Інтернет. Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.

Тема 9. Протокол захисту електронних транзакцій TLS. Порівняння версій протоколів TLS 2.0 та 3.0.

Тема 10. Захист електронної пошти. Боротьба зі спамом та фішингом.

Тема 11. Безпека мережі з програмованими параметрами SDN.

Тема 12. Додаткові методи підвищення безпеки мережі ІКТ.

3 СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	практ.	сам. роб.		лекц.	прак	сам. роб.
Тема 1. Основні поняття та визначення. Інноваційні процеси та їх класифікація. Стан сучасної кібербезпеки та шляхи розвитку на майбутнє. Конкурентні переваги при інноваційній діяльності.	10	2	0	8	10	2	0	8
Тема 2. Загрози та ризики витоку конфіденційної інформації. Загрози інформаційної безпеки держави в соціальних мережах. Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.	10	2	2	6	10	0	2	8
Тема 3. Сучасні тенденції в галузі захисту інформації інноваційного підприємництва. Комерційна інформація та комерційна таємниця.	10	2	2	6	10	0	0	10
Тема 4. Структура і завдання політики інформаційної безпеки. Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства. Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT).	10		2	8	10	0	2	8
Тема 5. Соціальна інженерія. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.	10	2	2	6	10	0	0	10
Тема 6. Управління контролем доступу. Основна функція управління контролю доступом.	10	2	2	6	10	2	0	8
Тема 7. Перспективи систем забезпечення інформаційної безпеки кіберпростору. Кібербезпека комунікаційних систем і мереж.	10	2	2	6	10	0	0	10
Тема 8. Засоби захисту від витоку інформації в Інтернет. Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.	10	2	2	6	10	0	2	8
Тема 9. Протокол захисту електронних транзакцій TLS. Порівняння версій протоколів TLS 2.0 та 3.0	10	2	2	6	10	2	0	8
Тема 10. Захист електронної пошти. Боротьба зі спамом та фішингом.	10	2	2	6	10	0	0	10
Тема 11. Безпека мережі з програмованими параметрами SDN.	10	2	2	6	10	0	0	10
Тема 12. Додаткові методи підвищення безпеки мережі ІКТ.	10	2	2	6	10	0	0	10
Усього годин	**120**	**22**	**22**	**76**	**120**	**6**	**6**	**108**
Підсумковий контроль – залік								

4 ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Аналіз методів стимулювання інноваційної діяльності [с. 26-32]	2	
2	Дослідження методів захисту інформації при інноваційній діяльності [с. 46-53]	4	2
3	Вивчення алгоритму формування систем інформаційної безпеки [с. 71-83]	2	
4	Дослідження основ теорії інформаційної безпеки [с. 95-101]	4	
5	Аналіз методів формування рейтингових систем інформаційної безпеки інноваційних процесів та підприємств [с. 102-113]	4	2
6	Дослідження алгоритму розробки показників надійності кібербезпеки [с. 160-177]	2	
7	Аналіз взаємодії видів безпеки в інноваціях на прикладі економічної безпеки [с. 33-41]	4	2
	Всього	22	6

5 САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «**Інформаційна безпека інноваційної діяльності»** включаються наступні тематики завдання.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.** Вивчення Положення закону «Про національну безпеку України»	8	8
2	**Тема 2.** Вивчення Положення закону України «Про інноваційну діяльність».	6	8
3	**Тема 3.** Дослідження впливу витоку конфіденційної інформації на стан розвитку сучасного підприємсива.	6	10
4	**Тема 4.** Дослідження методів захисту від недоброчесної конкуренції та шпигунства**.** Дослідження програми навчання працівників у сфері кібербезпеки (SAT).	8	8
5	**Тема 5.** Класифікація кіберзагроз та види кібератак.	6	10
6	**Тема 6.** Дослідження мережевих систем виявлення вторгнень.	6	8
7	**Тема 7.** Дослідження комплексного підходу виявлення вторгнень заснований на аналізі трафіка.	6	10
8	**Тема 8.** Дослідження порівняльної характеристики сучасних криптосистем, що використовуються для захисту конфіденційної інформації**.**	6	8
9	**Тема 9.** Дослідження протоколу захисту електронних транзакцій 3D-Secur для додаткового кроку автентифікації**.**	6	8
10	**Тема 10.** Класифікація загроз та правила поведінки працівників в корпоративній мережі.	6	10
11	**Тема 11.** Дослідження Віртуальних спільнот, як суб'єктів інформаційної безпеки Держави.	6	10
12	**Тема 12.** Дослідження моделі забезпечення безпеки в комп'ютерних системах.	6	10
	Всього	**76**	**108**

Теми доповідей

1. Ризики інформаційної безпеки в інноваційній діяльності: основні аспекти та методи їх оцінки.

2. Вплив штучного інтелекту на інформаційну безпеку інноваційних проектів.

3. Захист конфіденційності даних в умовах інноваційного бізнесу: практичні підходи.

4. Аналіз загроз інформаційній безпеці в стартапах: проблеми та рішення.

5. Інформаційні технології та їх роль у забезпеченні безпеки інноваційних продуктів.

6. Методи управління ризиками інформаційної безпеки в інноваційних проектах.

7. Кібербезпека в умовах цифрової трансформації бізнесу: виклики та можливості.

8. Впровадження системи інформаційної безпеки: від теорії до практики.

9. Роль криптографії у захисті інформаційних ресурсів інноваційних компаній.

10. Аудит інформаційної безпеки: методи та інструменти для інноваційних підприємств.

11. Соціальна інженерія: загрози та заходи захисту в контексті інноваційної діяльності.

12. Кіберзахист критичної інфраструктури в умовах інноваційного розвитку.

13. Використання блокчейн-технологій для забезпечення інформаційної безпеки.

14. Розробка та впровадження політик інформаційної безпеки в інноваційних компаніях.

15. Етичні аспекти інформаційної безпеки: виклики для інноваційної діяльності.

16. Аналіз інцидентів інформаційної безпеки в стартапах: випадки та уроки.

17. Вплив мобільних технологій на інформаційну безпеку інноваційних підприємств.

18. Тренди в інформаційній безпеці: нові виклики для інноваційних організацій.

19. Роль інформаційної безпеки у забезпеченні конкурентоспроможності інноваційних підприємств.

20. Впровадження технологій машинного навчання для покращення інформаційної безпеки.

6 ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю		**Складові оцінювання**
поточний контроль, який здійснюється у ході: проведення практичних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань.		**80%**
підсумковий контроль, який здійснюється у ході проведення заліку.		**20%**
Методи діагностики знань (контролю)	фронтальне опитування; доповідь, усне повідомлення, індивідуальне опитування; робота на практичних заняттях, залік	

Питання до підсумкового контролю

1. Що таке інформаційна безпека і які її основні складові?
2. Які основні загрози інформаційній безпеці існують?
3. Як класифікуються загрози інформаційній безпеці інноваційних проєктів?
4. Що таке конфіденційність інформації?
5. Що таке цілісність інформації?
6. Що таке доступність інформації?
7. Як поняття інформаційної безпеки застосовується до інноваційних продуктів?
8. Які нормативно-правові акти регулюють інформаційну безпеку в Україні?
9. Які міжнародні стандарти інформаційної безпеки є найбільш поширеними?
10. Що таке GDPR і як він впливає на інформаційну безпеку інноваційної діяльності?
11. Які вимоги до захисту персональних даних існують у рамках законодавства України?
12. Які етичні аспекти необхідно враховувати при забезпеченні інформаційної безпеки?
13. Які основні технічні засоби забезпечення інформаційної безпеки існують?
14. Що таке криптографія і яку роль вона відіграє в захисті інформації?
15. Які різновиди антивірусного програмного забезпечення існують?

16. Як застосовуються системи виявлення і попередження вторгнень у інноваційній діяльності?

17. Які сучасні технології застосовуються для забезпечення безпеки мережевих інноваційних систем?

18. Що таке політика інформаційної безпеки і як її формують?

19. Які основні складові політики інформаційної безпеки інноваційних компаній?

20. Як розробляється політика резервного копіювання інформації?

21. Які заходи потрібно вжити для захисту інформації під час інноваційного проєкту?

22. Що таке інцидент інформаційної безпеки і як з ним боротися?

23. Як забезпечити інформаційну безпеку на всіх етапах життєвого циклу інноваційного продукту?

24. Які особливості інформаційної безпеки у сфері стартапів?

25. Як здійснюється захист інформаційних активів інноваційних компаній?

26. Як нові технології (наприклад, блокчейн) можуть вплинути на інформаційну безпеку інноваційних проєктів?

27. Як захистити інтелектуальну власність у сфері інноваційної діяльності?

28. Яку роль відіграє людський фактор у забезпеченні інформаційної безпеки?

29. Які методи соціальної інженерії використовують для викрадення інформації?

30. Як можна підвищити обізнаність співробітників щодо загроз інформаційній безпеці?

31. Які засоби захисту від інсайдерських загроз застосовуються у компаніях?

32. Як проводити навчання працівників щодо політик інформаційної безпеки?

33. Які типи інформаційних атак існують?

34. Як відрізняються DDoS-атаки від інших мережевих атак?

35. Які методи використовуються для виявлення та запобігання фішинговим атакам?

36. Що таке атаки нульового дня і як з ними боротися?

37. Які заходи безпеки необхідно вжити для захисту інноваційного продукту від кібератак?

38. Які методи використовуються для захисту програмного забезпечення від несанкціонованого доступу?

39. Що таке уразливості програмного забезпечення і як їх можна уникнути?

40. Як забезпечити безпеку мобільних додатків у інноваційних проєктах?

41. Які сучасні виклики та тенденції в галузі інформаційної безпеки інновацій?

42. Як впливають технології штучного інтелекту на інформаційну безпеку?

43. Яку роль відіграє хмарне зберігання даних у забезпеченні інформаційної безпеки?

44. Як впливають великі дані (Big Data) на інформаційну безпеку інноваційних проєктів?

45. Які вимоги до захисту персональних даних існують у рамках законодавства України?

7 КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи та активність у науково-дослідній роботі;

- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи;

- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має

неповний конспект з завданнями до самостійної роботи.

- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів. Студент не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	**Шкала за ECTS**	**За національною шкалою**	
		екзамен	**залік**
90-100 (10-12)	A	Відмінно	зараховано
82-89 (8-9)	B	Добре	
74-81(6-7)	C		
64-73 (5)	D	Задовільно	
60-63 (4)	E		
35-59 (3)	Fx	незадовільно	не зараховано
1-34 (2)	F		

8 ПЛАН–КОНСПЕКТ ЛЕКЦІЙ

Тема 1. Основні поняття та визначення. Інноваційні процеси та їх класифікація. Стан сучасної кібербезпеки та шляхи розвитку на майбутнє. Конкурентні переваги при інноваційній діяльності.

Інноваційні процеси – це сукупність дій, спрямованих на створення, впровадження та поширення нових ідей, продуктів або технологій. Вони включають кілька стадій: від генерації ідеї до її комерціалізації. Інноваційні процеси можна класифікувати за різними ознаками: за рівнем новизни (базисні інновації, поліпшуючі інновації, модифікаційні інновації) та за типом змін (продуктові інновації, технологічні інновації, соціальні інновації).

Сучасна кібербезпека стикається з численними викликами, такими як зростання кількості кібератак, розвиток шкідливого програмного забезпечення та необхідність захисту конфіденційної інформації. Основні напрями розвитку включають впровадження новітніх криптографічних методів, удосконалення систем виявлення загроз та підвищення рівня обізнаності користувачів. Шляхи розвитку кібербезпеки на майбутнє включають використання штучного інтелекту та машинного навчання для виявлення та запобігання загрозам, розробку нових алгоритмів шифрування для забезпечення безпеки даних, а також підвищення рівня обізнаності користувачів про кіберзагрози та методи захисту.

Інноваційна діяльність надає підприємствам конкурентні переваги, такі як підвищення ефективності виробництва, поліпшення якості продукції та зниження витрат. Впровадження нових технологій дозволяє підприємствам швидше адаптуватися до змін на ринку та задовольняти потреби споживачів.

Тема 2. Загрози та ризики витоку конфіденційної інформації. Загрози інформаційної безпеки держави в соціальних мережах. Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях.

Загрози та ризики витоку конфіденційної інформації включають несанкціонований доступ до даних, їх модифікацію або знищення. Основні причини витоків можуть бути пов’язані з людським фактором, технічними збоями або

зловмисними діями. Загрози інформаційної безпеки держави в соціальних мережах включають поширення дезінформації, кібератаки на державні ресурси та маніпуляції громадською думкою. Соціальні мережі можуть бути використані для збору розвідувальної інформації та організації кібератак.

Аналіз проблеми оперативного виявлення і реагування на інциденти кібербезпеки в телекомунікаціях показує, що важливо мати ефективні системи моніторингу та реагування, які дозволяють швидко виявляти та нейтралізувати загрози. Це включає використання сучасних технологій, таких як штучний інтелект та машинне навчання, для аналізу трафіку та виявлення аномалій.

Тема 3. Сучасні тенденції в галузі захисту інформації інноваційного підприємництва. Комерційна інформація та комерційна таємниця.

Сучасні тенденції в галузі захисту інформації інноваційного підприємництва включають впровадження новітніх технологій для забезпечення безпеки даних та захисту від кібератак. Однією з ключових тенденцій є використання штучного інтелекту та машинного навчання для виявлення загроз та запобігання їм. Також важливим є розвиток криптографічних методів захисту інформації, що дозволяє забезпечити конфіденційність та цілісність даних.

Комерційна інформація та комерційна таємниця є важливими аспектами для інноваційних підприємств. Комерційна інформація включає дані про продукти, послуги, клієнтів та ринки, які мають комерційну цінність. Комерційна таємниця, в свою чергу, охоплює інформацію, яка не підлягає розголошенню та захищена від несанкціонованого доступу. Захист комерційної таємниці є критично важливим для збереження конкурентних переваг підприємства.

Якщо вам потрібна додаткова інформація або допомога з конкретними аспектами, будь ласка, дайте знати!

Тема 4. Структура і завдання політики інформаційної безпеки. Кадрова політика, моніторинг і контроль. Захист від недоброчесної конкуренції та шпигунства. Створення та впровадження програми навчання працівників у сфері кібербезпеки (SAT).

Політика інформаційної безпеки (ІБ) є ключовим документом, який визначає стратегію і методи захисту інформаційних активів організації. Її структура включає кілька основних елементів. Мета політики полягає в загальних цілях ІБ, які мають відповідати стратегії організації. Завдання політики конкретизують кроки та заходи для забезпечення інформаційної безпеки. Принципи ІБ визначають основні правила та керівні принципи для захисту інформації. Відповідальність за ІБ розподіляється між співробітниками та підрозділами, щоб забезпечити ефективну координацію зусиль. Оцінка ризиків охоплює методи і процеси для визначення й оцінки можливих загроз і вразливостей. Політика контролю доступу визначає права доступу до інформаційних ресурсів для різних категорій користувачів. Нарешті, процеси відновлення після інцидентів окреслюють заходи реагування на інциденти та плани дій на випадок надзвичайних ситуацій.

Кадрова політика в сфері інформаційної безпеки є важливим елементом, оскільки працівники можуть бути як найсильнішим захистом, так і найбільшою вразливістю організації. Основні аспекти цієї політики включають набір, навчання та моніторинг працівників. Критично важливо здійснювати перевірку потенційних працівників на надійність і доброчесність, а також проводити регулярне навчання з питань інформаційної безпеки для поточного персоналу. Створення середовища, яке підтримує свідоме ставлення працівників до безпеки, зменшує ризики пов'язані з людським фактором.

Моніторинг і контроль в інформаційній безпеці зосереджуються на відстеженні доступу до систем і виявленні потенційно підозрілої активності. Важливими аспектами є регулярне ведення журналів дій користувачів і застосування автоматизованих інструментів для моніторингу системи в режимі реального часу. Ці заходи допомагають виявити можливі порушення, шпигунство чи зловживання інформаційними активами.

Захист від недоброчесної конкуренції та шпигунства також є важливою складовою політики ІБ. Це передбачає запровадження заходів щодо захисту комерційних таємниць, конфіденційної інформації та технологій від несанкціонованого доступу або передачі конкурентам. Організації повинні забезпечити як технічні, так і організаційні заходи для мінімізації цих ризиків.

Створення та впровадження програми навчання працівників у сфері кібербезпеки (Security Awareness Training, SAT) є важливою частиною загальної стратегії інформаційної безпеки. Метою такої програми є підвищення обізнаності співробітників щодо основних загроз у сфері кібербезпеки, навчання їх правильної поведінки та реакції на потенційні атаки. Програма має охоплювати як теоретичну частину, так і практичні тренінги для того, щоб кожен працівник знав, як захистити дані й уникнути поширених помилок, що можуть призвести до витоку або компрометації інформації.

Тема 5. Соціальна інженерія. Загрози кіберсистемам. Використання методів соціальної інженерії для захисту інноваційної діяльності від кібератак.

Соціальна інженерія є однією з найбільш поширених та ефективних методик, що використовуються зловмисниками для здійснення кіберзлочинів. Вона полягає в маніпуляції людьми з метою отримання доступу до конфіденційної інформації або ресурсів. Основною метою атак соціальної інженерії є викликати в жертви певні емоції, такі як страх, довіра або цікавість, що змушує її виконати дії, вигідні зловмиснику, наприклад, передати паролі або інші особисті дані.

Загрози кіберсистемам, зумовлені соціальною інженерією, включають різні типи атак, такі як фішинг, вішинг (телефонні атаки), смішинг (атаки через SMS), а також різні види шахрайства, що використовують психологічні трюки для отримання доступу до систем або даних. Фішинг, наприклад, є одним із найпоширеніших методів, коли зловмисники надсилають підроблені електронні листи або повідомлення, що виглядають як офіційні, для того щоб отримати від користувача конфіденційну інформацію.

Ще однією суттєвою загрозою є атаки на інноваційну діяльність організацій, особливо коли йдеться про інтелектуальну власність, нові розробки або комерційні таємниці. Соціальна інженерія може бути використана для проникнення в компанії з метою отримання доступу до таких ресурсів через співробітників або навіть керівництво, які можуть ненавмисно передати конфіденційну інформацію внаслідок добре спланованої атаки.

Для захисту інноваційної діяльності від кібератак за допомогою методів соціальної інженерії важливо вживати низку заходів. По-перше, потрібно проводити регулярні навчання працівників щодо сучасних загроз і методів соціальної інженерії. Це дозволить підвищити обізнаність та здатність розпізнавати потенційні загрози. По-друге, запровадження багатофакторної аутентифікації та обмеження доступу до чутливих даних допомагає мінімізувати ризики. Нарешті, варто розробляти й застосовувати чіткі протоколи для обробки інформації, що зменшують ймовірність передачі критичної інформації внаслідок шахрайських дій.

Тема 6. Управління контролем доступу. Основна функція управління контролю доступом.

Основна функція управління контролем доступу (Access Control Management) полягає в обмеженні та регулюванні доступу користувачів або систем до ресурсів, даних та сервісів. Її головною метою є забезпечення безпеки інформаційних систем та гарантування того, що доступ до конфіденційної інформації отримують лише уповноважені користувачі або процеси. Управління контролем доступу спрямоване на досягнення трьох основних цілей: конфіденційності, яка передбачає захист інформації від несанкціонованого доступу; цілісності, що запобігає несанкціонованій модифікації даних; і доступності, яка забезпечує надання доступу до інформації лише авторизованим користувачам. Серед основних типів контролю доступу виділяють дискреційний контроль доступу (Discretionary Access Control, DAC), при якому користувачі можуть передавати доступ іншим; мандатний контроль доступу (Mandatory Access Control, MAC), де доступ визначається централізовано за суворими правилами; рольовий контроль доступу (Role-Based Access Control, RBAC), що визначає доступ на основі призначених ролей; та атрибутивний контроль доступу (Attribute-Based Access Control, ABAC), який контролює доступ на основі атрибутів користувача, ресурсу або контексту. Завдяки управлінню контролем доступу організації можуть ефективно контролювати, хто має право на доступ до ресурсів і в якому обсязі, що значно знижує ризики несанкціонованого доступу або порушень безпеки.

Тема 7. Перспективи систем забезпечення інформаційної безпеки кіберпростору. Кібербезпека комунікаційних систем і мереж.

Перспективи систем забезпечення інформаційної безпеки кіберпростору безпосередньо пов'язані з розвитком технологій та збільшенням загроз у цифровому середовищі. Кібербезпека комунікаційних систем і мереж стає все більш важливою через стрімке зростання кількості пристроїв, що підключені до мережі, і збільшення обсягу переданих даних. Інформаційна безпека спрямована на захист конфіденційності, цілісності та доступності даних у цифрових комунікаційних системах.

Однією з головних перспектив є розвиток технологій штучного інтелекту (ШІ) та машинного навчання, які використовуються для автоматизації виявлення загроз і аналізу кіберінцидентів у реальному часі. ШІ здатен ідентифікувати аномалії в мережевому трафіку, прогнозувати можливі атаки та підвищувати ефективність захисних заходів.

Інша важлива тенденція — впровадження блокчейн-технологій для захисту даних і забезпечення цілісності інформації в мережах. Блокчейн забезпечує розподілену структуру зберігання даних, що ускладнює маніпуляції з ними або несанкціонований доступ.

Також розвиваються технології шифрування, які забезпечують захист комунікацій від перехоплення. Використання квантової криптографії відкриває нові можливості для підвищення рівня захищеності даних, оскільки квантові ключі надзвичайно важко зламати сучасними методами.

Інтернет речей (IoT) створює нові виклики для кібербезпеки через велику кількість підключених пристроїв, що можуть бути використані зловмисниками для атак на мережі. Перспективи кібербезпеки в цьому контексті полягають у розробці нових підходів до захисту IoT-систем, включаючи стандартизацію безпеки та розвиток захисних механізмів на рівні апаратного забезпечення.

Загалом, кібербезпека комунікаційних систем і мереж продовжує вдосконалюватися, враховуючи нові загрози та технологічні зміни. Інновації у сфері штучного інтелекту, блокчейну, квантових технологій і захисту IoT є ключовими напрямками розвитку інформаційної безпеки кіберпростору.

Тема 8. Засоби захисту від витоку інформації в Інтернет. Програмно-апаратні системи шифрування, брандмауери, системи попередження вторгнення.

Засоби захисту від витоку інформації в Інтернеті є важливою складовою забезпечення конфіденційності, цілісності та доступності даних. Зі зростанням обсягів переданої інформації через мережі збільшується і кількість загроз, пов'язаних з несанкціонованим доступом, перехопленням або викраденням даних. Основними засобами захисту виступають програмно-апаратні системи шифрування, брандмауери та системи попередження вторгнень (Intrusion Prevention Systems, IPS). Програмно-апаратні системи шифрування забезпечують захист даних шляхом їх перетворення в зашифрований формат, доступний лише авторизованим користувачам. Використовуючи криптографічні алгоритми, такі як AES або RSA, ці системи гарантують, що навіть у разі перехоплення дані залишаться непридатними для використання без ключа розшифрування. Шифрування може бути як програмним, так і інтегрованим у апаратні пристрої, що підвищує рівень безпеки, особливо для захисту чутливої інформації. Брандмауери (firewalls) контролюють вхідний і вихідний трафік на основі заданих правил безпеки, запобігаючи несанкціонованому доступу до мережі, хакерським атакам та фільтруючи шкідливий трафік. Вони можуть бути апаратними або програмними і допомагають встановлювати політики доступу, що захищають мережі від зовнішніх загроз. Системи попередження вторгнень (IPS) доповнюють функції брандмауерів та систем виявлення вторгнень (IDS), активуючи захист у режимі реального часу. На відміну від IDS, які лише фіксують та повідомляють про підозрілу активність, IPS не тільки виявляють аномалії або підозрілі дії, але й блокують потенційно небезпечний трафік або ізолюють його. Ці системи автоматично реагують на загрози, забезпечуючи ефективний захист від спроб вторгнення та інших видів атак. Усі ці засоби, працюючи разом, створюють багаторівневий захист від витоку інформації, допомагаючи запобігти несанкціонованому доступу до даних, а також мінімізувати ризики їх викрадення або пошкодження.

Тема 9. Протокол захисту електронних транзакцій TLS. Порівняння версій протоколів TLS 2.0 та 3.0

Протокол захисту електронних транзакцій TLS (Transport Layer Security) є ключовим механізмом для забезпечення безпечної передачі даних через Інтернет. Він використовується для шифрування даних, автентифікації серверів і клієнтів, а також для забезпечення цілісності інформації. TLS є спадкоємцем протоколу SSL (Secure Sockets Layer) і на сьогодні виступає стандартом захисту інтернет-з'єднань, зокрема під час використання HTTPS. Протокол дозволяє захищати конфіденційні дані, такі як паролі, фінансова інформація або особисті дані, від несанкціонованого доступу та викрадення. Версії TLS пройшли кілька етапів розвитку, і порівняння версій TLS 1.2 (неофіційно TLS 2.0) та TLS 1.3 (TLS 3.0) демонструє суттєві покращення в безпеці та продуктивності. TLS 1.2 підтримує ширший набір криптографічних алгоритмів, включаючи застарілі й менш безпечні варіанти, як-от RC4 або SHA-1. Клієнт і сервер обирають алгоритми на основі пріоритету, що робить процес складнішим і менш надійним. Натомість TLS 1.3 значно спростив цей вибір, виключивши застарілі алгоритми і залишивши лише більш безпечні, як-от AES-GCM або ChaCha20, що підвищило загальний рівень безпеки та пришвидшило роботу протоколу. У TLS 1.2 процес рукостискання, під час якого клієнт і сервер узгоджують параметри з'єднання, є довшим і складнішим, що збільшує час встановлення з'єднання. У TLS 1.3 цей процес був оптимізований, скорочуючи кількість обмінів повідомленнями, що значно прискорює підключення та зменшує затримки. Що стосується безпеки, TLS 1.3 покращив захист, запровадивши механізм Forward Secrecy, який гарантує, що навіть у разі зламу ключа сесії, це не вплине на безпеку попередніх або майбутніх сесій. Крім того, нова версія усуває можливість атак типу «downgrade», коли зловмисники змушують клієнта і сервер використовувати менш безпечні алгоритми. Продуктивність TLS 1.3 також вища, оскільки спрощений процес рукостискання та зменшена кількість криптографічних обчислень знижують навантаження на систему, що є важливим для мереж з високим трафіком. Однак, TLS 1.2 забезпечує більшу сумісність із застарілими системами, оскільки підтримує старі криптографічні алгоритми. У той час як TLS 1.3 орієнтований на сучасні системи, що може викликати труднощі з його

використанням на застарілому обладнанні або програмному забезпеченні. Таким чином, TLS 1.3 є більш безпечним і продуктивним порівняно з TLS 1.2 завдяки видаленню застарілих алгоритмів, оптимізації процесу рукостискання та посиленню захисту від атак. TLS 1.2 все ще використовується, але поступово витісняється новішою версією через зростаючі вимоги до безпеки сучасних інформаційних систем.

Тема 10. Захист електронної пошти. Боротьба зі спамом та фішингом.

Захист електронної пошти є важливою складовою інформаційної безпеки, оскільки електронна пошта є одним із основних каналів комунікації та часто використовується для передачі конфіденційної інформації. Проте цей канал залишається вразливим до різних загроз, таких як спам і фішинг, які можуть призводити до втрати даних, компрометації систем або фінансових збитків.

Спам є небажаними повідомленнями, які надсилаються користувачам без їхньої згоди. Спамери використовують різні методи для розсилки великої кількості повідомлень, часто з рекламною метою або для поширення шкідливого програмного забезпечення. Основними засобами боротьби зі спамом є фільтри електронної пошти, які автоматично аналізують вміст вхідних повідомлень і визначають, чи є вони спамом. Для цього використовуються методи аналізу ключових слів, визначення підозрілих доменів або IP-адрес, а також алгоритми машинного навчання для покращення точності фільтрації.

Додатково використовуються так звані «чорні списки» (blacklists), які містять домени та IP-адреси, відомі як джерела спаму. Провайдери електронної пошти можуть блокувати повідомлення з таких джерел, запобігаючи їх попаданню у скриньку. Інші методи боротьби зі спамом включають впровадження CAPTCHA при реєстрації нових користувачів або під час надсилання великої кількості повідомлень, що запобігає автоматизованим системам масової розсилки.

Фішинг є шахрайською діяльністю, коли зловмисники намагаються обманом змусити користувачів надати конфіденційну інформацію, таку як паролі або фінансові дані. Фішингові атаки зазвичай виглядають як легітимні повідомлення від відомих організацій, наприклад, банків або сервісних провайдерів, і містять

посилання на підроблені вебсайти. Для захисту від фішингу застосовуються різні методи, зокрема фільтри для виявлення підозрілих листів, аналіз тексту і посилань у повідомленнях, а також автентифікація відправника за допомогою протоколів SPF, DKIM та DMARC, які перевіряють автентичність домену відправника.

Важливу роль у боротьбі з фішингом відіграє підвищення обізнаності користувачів. Більшість фішингових атак спрямовані на людську довірливість, тому навчання розпізнаванню підозрілих електронних листів, посилань та вкладень є ефективним способом запобігання шахрайству. Деякі сервіси також впроваджують двофакторну автентифікацію, яка додає додатковий рівень захисту, оскільки навіть при витоку пароля зловмисники не зможуть отримати доступ до облікового запису без додаткового підтвердження.

Загалом, захист електронної пошти від спаму та фішингу вимагає комплексного підходу, який включає технічні засоби, такі як фільтри та автентифікація, а також навчання користувачів. Таке поєднання заходів може значно знизити ризик витоку інформації та інших кіберзагроз, пов'язаних з електронною поштою.

Тема 11. Безпека мережі з програмованими параметрами SDN.

Безпека мережі з програмованими параметрами (Software-Defined Networking, SDN) є одним із ключових аспектів сучасної мережевої архітектури, яка дозволяє централізовано керувати мережею, абстрагуючи фізичні компоненти від логічного рівня управління. Це надає гнучкість у налаштуванні мережевих параметрів і підвищує ефективність управління трафіком. Однак, як і будь-яка інноваційна технологія, SDN має свої ризики та вразливості, що вимагає спеціальних заходів для забезпечення її безпеки.

Однією з основних особливостей SDN є відокремлення контрольного рівня (control plane) від рівня даних (data plane). Контрольний рівень, що відповідає за прийняття рішень про маршрутизацію трафіку, керується централізованим контролером, який має повний огляд усієї мережі. Така архітектура надає можливість гнучкого і динамічного управління, але водночас створює потенційну точку вразливості. Якщо контролер буде зламаний або компрометований,

зловмисники зможуть отримати повний доступ до управління мережею, що може призвести до серйозних атак, таких як перенаправлення трафіку або вимкнення мережевих сегментів.

Для захисту SDN-мереж важливо забезпечити надійний захист контролера. Основні методи включають автентифікацію і авторизацію для доступу до контролера, а також шифрування зв'язку між контролером і мережевими елементами. Протоколи, які використовуються для обміну даними між контролером і мережевими пристроями (наприклад, OpenFlow), також повинні бути захищені за допомогою шифрування та механізмів аутентифікації, щоб запобігти атакам на комунікаційний канал.

Ще одним аспектом безпеки SDN є захист від загроз, пов'язаних з динамічним налаштуванням мережі. Оскільки SDN дозволяє швидко змінювати мережеву конфігурацію, існує ризик внесення помилкових або шкідливих налаштувань, які можуть порушити нормальну роботу мережі або створити додаткові вразливості. Для запобігання цьому застосовуються методи автоматизованого моніторингу та аналізу конфігурацій з метою виявлення аномалій або потенційно небезпечних змін.

Окрім цього, в SDN-мережах використовуються технології сегментації мережі, які дозволяють ізолювати критично важливі ресурси від менш захищених частин мережі. Такий підхід дозволяє зменшити ризик поширення атак у разі компрометації одного з сегментів. Важливо також забезпечити засоби для швидкого виявлення і реагування на загрози, такі як системи виявлення вторгнень (IDS) і захист від DDoS-атак.

Таким чином, безпека мережі з програмованими параметрами SDN вимагає комплексного підходу, який охоплює захист контролера, шифрування комунікацій, моніторинг конфігурацій і сегментацію мережі. Ці заходи дозволяють мінімізувати ризики, пов'язані з використанням SDN, і забезпечити надійну роботу мережевої інфраструктури навіть в умовах постійно зростаючих загроз.

Тема 12. Додаткові методи підвищення безпеки мережі ІКТ.

Додаткові методи підвищення безпеки мережі інформаційно-комунікаційних технологій (ІКТ) є важливим аспектом сучасного управління інформаційною

безпекою. З огляду на постійно зростаючі загрози з боку кіберзловмисників, впровадження комплексного підходу до забезпечення безпеки мережі стає критично необхідним. Окрім основних методів захисту, таких як брандмауери і антивірусні програми, існує ряд додаткових заходів, які можуть значно покращити безпеку мережі.

Одним з найефективніших методів є використання технології сегментації мережі. Сегментація передбачає поділ мережі на менші, ізольовані сегменти, що дозволяє обмежити доступ до чутливих даних і ресурсів. Це зменшує ймовірність поширення шкідливого програмного забезпечення, оскільки зловмисникам буде важче переміщатися між сегментами у разі компрометації одного з них. Сегментація також дозволяє реалізувати різні політики безпеки для різних сегментів, що підвищує контроль над доступом.

Крім того, важливо впроваджувати регулярні оновлення програмного забезпечення та систем безпеки. Системи та програми, які не оновлюються, можуть стати вразливими до нових загроз. Постійний моніторинг та застосування оновлень дозволяє закривати вразливості, які можуть бути використані зловмисниками. Автоматизація процесу оновлення може значно спростити цей процес і зменшити ймовірність помилок.

Ще одним важливим методом є впровадження двофакторної автентифікації (2FA) для доступу до критичних систем і даних. Двофакторна автентифікація забезпечує додатковий рівень захисту, оскільки вимагає не лише введення пароля, але й підтвердження особи за допомогою додаткового фактору, наприклад, кодом, надісланим на мобільний телефон. Це ускладнює доступ до системи зловмисникам, навіть якщо їм вдалося отримати пароль.

Моніторинг мережі та аналіз подій безпеки також є важливими аспектами підвищення безпеки. Системи виявлення вторгнень (IDS) і системи запобігання вторгнень (IPS) можуть виявляти аномальні активності в реальному часі, що дозволяє оперативно реагувати на загрози. Впровадження рішень для аналізу поведінки користувачів (UEBA) допомагає виявляти підозрілі дії, що можуть свідчити про спробу атаки.

Крім того, регулярні аудити безпеки та тестування на проникнення допомагають виявити вразливості в системі. Ці процедури дозволяють оцінити ефективність існуючих заходів безпеки та виявити потенційні слабкі місця до того, як ними скористаються зловмисники. Тестування на проникнення може проводитися як внутрішніми, так і зовнішніми спеціалістами з безпеки.

Нарешті, важливим аспектом підвищення безпеки мережі ІКТ є освіта та підвищення обізнаності співробітників. Людський фактор часто стає причиною багатьох інцидентів безпеки, тому навчання персоналу основам кібербезпеки, розпізнаванню фішингових атак і належному використанню корпоративних ресурсів може суттєво знизити ризики.

Отже, підвищення безпеки мережі ІКТ вимагає впровадження комплексних і багаторівневих методів. Сегментація мережі, регулярні оновлення, двофакторна автентифікація, моніторинг безпеки, аудити та навчання співробітників є важливими елементами в створенні надійної системи безпеки, яка здатна протистояти сучасним кіберзагрозам.

9 РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Кононович В.Г., Стайкуца С.В., Бердніков О.М., Севастєєв Є.О., Швець О.В. Інформаційна безпека інноваційної діяльності в інфокомунікаціях : підручник та дистанційний практикум для освітньо-професійної підготовки магістрів за спеціальністю 125 «Кібербезпека та захист інформації» . За ред. д.т.н., проф. В.В.Корчинського. Передмова д.т.н., проф. Є. В. Василіу. Післямова д.т.н., проф. С.О.Гнатюка. - Вид.2-ге, випр., доп. - Одеса: Астропринт, 2023. 380 с. (для аудиторного та дистанційного навчання, мова: укр., англ).

2. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

3. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

Додаткова

2. Криптографічний захист інформації: Навч. посіб./ Йона Л.Г., Онацький О.В., Бєлова Ю.В.. - Одеса: ДУІТЗ, 2023. – 250 с., ел.вар.

3. Сосновська О.О. Інформаційна безпека як стратегічна складова економічної безпеки підприємства. Стратегічні пріоритети соціально-економічного розвитку в умовах інституційних перетворень глобального середовища: матеріали VIII Міжнародної наук. – прак. конференції (м. Одеса, 28-29 вересня 2018 р.). Одеса: ОНУ імені І. І. Мечникова, 2018. С. 77-80.

4. Круглов В. В. Цифрова трансформація як спосіб побудови смарт-суспільства. Сучасні виклики сталого розвитку бізнесу: тези виступів Міжнар. наук. конф. Житомир: Житомирська політехніка, 2020. С. 335.

Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / за ред. Бебика В.М. ; Відкр. міжнар. ун-т розвитку людини «Україна». Київ : Університет «Україна», 2019. 177 с.

Інформаційні ресурси

1 Наказ МОН № 332 від 18.03.2021 року Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. URL: https://osvita.ua/legislation/Vishya_osvita.

2 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.

3 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/

4 Портал урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua/

5 Radivilova, L. Kirichenko, M. Tawalbeh, P. Zinchenko, V. Bulakh, «Балансування самоподібного трафіку в мережних системах виявлення вторгнень », Кібербезпека: освіта, наука, техніка, Том. 3, вип. 7, с. 17-30, Бер 2020. DOI: https://doi.org/10.28925/2663-4023.2020.7.1730 (Радівілова, Л. Кириченко, М. Тавалбе, П. Зінченко, В. Булах, «Балансування самоподібного трафіку в мережевих системах виявлення вторгнень», Кібербезпека: освіта, наука, техніка, Том. 3, вип. 7, с. 17-30, Бер 2020. DOI: https://doi.org/10.28925/2663-4023.2020.7.1730)

6 Радівілова Т.А., Ільков А.А., Тавалбех М.Х. Комплексний метод виявлення вторгнень заснований на статистичному та динамічному підходах аналізу трафіка. Радіоелектроніка та інформатика. № 01. 2020. С. С.17-25.

7 Комплекс навчально-методичного забезпечення навчальної дисципліни "Захист систем електронної комерції та мультисервісних систем", освітньо-кваліфікаційний рівень бакалавр для спеціальності 125 - Кібербезпека [Електронний ресурс] : освітня програма підготовки "Управління інформаційною безпекою" / ХНУРЕ ; розроб. Т.А. Радівілова. – Харків, 2019. – 397 с. - pdf / 13,03 Mb.

ЗМІСТ

Навчальне видання

Йона Л.Г., Педяш В.В., Русу О.П.

ІНФОРМАЦІЙНА БЕЗПЕКА ІННОВАЦІЙНОЇ ДІЯЛЬНОСТІ

Методичні рекомендації для самостійної роботи здобувачів

Українською мовою