МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Економічний факультет

Кафедра економіки, менеджменту та комерційної діяльності

Методичні рекомендації

до вивчення дисципліни
«Управління інформаційною безпекою в ІТ сфері»
для здобувачів спеціальності 073 – «Менеджмент»;
другий (магістерський) рівень вищої освіти
освітньо-професійна програма
«Менеджмент ІТ у глобальному бізнес-середовищі»

Затверджено на засіданні кафедри
«Економіка, менеджмент та комерційна діяльність»,
протокол № 1 від 28.08. 2024 р.

Кропивницький – 2024

Методичні рекомендації до вивчення дисципліни «Управління інформаційною безпекою в ІТ сфері» для здобувачів спеціальності 073 – «Менеджмент»; другий (магістерський) рівень вищої освіти, освітньо-професійна програма «Менеджмент ІТ у глобальному бізнес-середовищі» // Укл.: Рябоволик Т.Ф. – Кропивницький: ЦНТУ, 2024. – 56 с.

Укладач: Рябоволик Т.Ф., к.е.н., доцент кафедри економіки, менеджменту та комерційної діяльності Центральноукраїнського національного технічного університету

Рецензенти: Горпинченко О.В., к.е.н., доцент кафедри економіки, менеджменту та комерційної діяльності Центральноукраїнського національного технічного університету

Андрощук І.О., к.е.н., доцент кафедри економіки, менеджменту та комерційної діяльності Центральноукраїнського національного технічного університету

Коваленко О.В., д-р техн. наук, проф., доцент кафедри кібербезпеки та програмного забезпечення

ЗМІСТ

ВСТУП

Інформаційна безпека стає єдиною з ключових складових ефективної діяльності підприємств і організацій у сучасному цифровому світі. З огляду на стрімкий розвиток інформаційних технологій та загальну цифровізацію бізнес-процесів, управління інформаційною безпекою є критично важливою для забезпечення захисту інформаційних активів, мінімізації ризиків потоку даних і запобігання кіберзагрозам.

Дисципліна «Управління інформаційною безпекою в ІТ-сфері» має на меті надати здобувачам вищої освіти спеціальності 073 «Менеджмент» за другим (магістерським) рівень вищої освіти освітньо-професійної програми «Менеджмент ІТ у глобальному бізнес-середовищі», комплексні знання та практичні навички, необхідні для формування, підтримки та оптимізації системи управління інформаційною безпекою на підприємствах, що функціонують у сфері інформаційних технологій. Вивчення основних принципів захисту даних, оцінки ризиків, управління інцидентами та впровадження відповідних заходів безпеки дозволяє підготувати висококваліфікованих спеціалістів, здатних ефективно забезпечити безпеку інформаційних систем у різних організаційних середовищах.

Методичні рекомендації призначені для полегшення засвоєння матеріалу дисципліни та організації самостійної роботи студентів. В методичних рекомендаціях подано огляд ключових тем, описано методи практичного застосування теоретичних знань, наведено приклад тестових завдань, критерії оцінювання які спрямовані на закріплення матеріалу. Крім того, увага приділяється сучасним стандартам і технологіям, які використовуються в галузі інформаційної безпеки, що є необхідним для адаптації до нових викликів в сфері ІТ.

Застосування набутих знань сприятиме підвищенню професійної компетентності майбутніх фахівців у галузі інформаційної безпеки та ІТ, а також дозволяє їм бути готовими до вирішення складних і нестандартних завдань, пов’язаних із забезпеченням кібербезпеки в умовах сучасної інформації.

З метою ґрунтовного засвоєння поданого матеріалу, а також перевірки і систематизації знань здобувачів у методичних вказівках після кожної теми запропоновані питання для самоконтролю, а по результатах вивчення всіх тем курсу – запропоновано скласти підсумковий тест.

1. МЕТА, ЗМІСТ І ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Управлінні інформаційною безпекою в ІТ сфері» є формування у студентів знань, навичок та вмінь, необхідних для ефективного управління процесами забезпечення інформаційної безпеки в організаціях. Це включає розуміння сучасних загроз інформаційній безпеці, методів захисту даних, політик безпеки, а також впровадження процедур і технологій для запобігання, виявлення та реагування на інциденти безпеки.

Завданнями вивчення дисципліни є теоретична підготовка здобувачів та поглиблене ознайомлення з такими питаннями як:

- принципи та стандарти інформаційної безпеки;
- розвиток навичок аналізу ризиків і управління ними;
- вивчення методів захисту інформації, включаючи криптографію, контроль доступу, моніторинг і аудит безпеки;
- навчаються розробці політик та процедур інформаційної безпеки;
- формують розуміння юридичних і етичних аспектів управління інформаційною безпекою.

Предметом вивчення навчальної дисципліни «Управління інформаційною безпекою в ІТ-сфері» є процеси, методи та інструменти управління інформаційною безпекою в контексті інформаційних технологій, включаючи: основи інформаційної безпеки (вивчення загроз, вразливостей та ризиків, пов'язаних із захистом інформації в ІТ-системах); методи забезпечення безпеки (криптографічні, технічні та організаційні методи захисту даних); стандарти та нормативні акти (міжнародні стандарти (наприклад, ISO/IEC 27001), законодавчі вимоги та регулювання у сфері інформаційної безпеки); управління ризиками (ідентифікація, оцінка та мінімізація ризиків у сфері ІТ); політика безпеки (розробка, впровадження та контроль виконання політики безпеки на підприємствах ІТ-сфери); аудит та моніторинг безпеки (проведення аудиту інформаційної безпеки, моніторинг інформаційних систем та реагування на інциденти); управління інцидентами (організація та процедура реагування на кіберзагрози та інші інциденти в інформаційній сфері); захист персональних даних (забезпечення конфіденційності, цільності та доступності інформації в ІТ-середовищі).

Зміст дисципліни складає вивчення таких понять: безпека, збиток, ймовірність, операційні ризики, захист інформації, об’єкт, активи, загроза інформаційній безпеці, діяльність, telecommunications, electronic engineering, computing machinery, internet engineering taskforce, ICSA, computationally secure, internet security, bureau, conference, lead, study, datanetwork, communication system,

архітектура безпеки, системи автентифікації, інформаційне суспільство, computer society, technical committee, workshop, special interest group, SIG, CCS, communication security, electronic commerce, інформаційна безпека, модель систем менеджменту, стандарт, управління ризиками, керівні вказівки, процес ний підхід, об'єднання, мережа, значення, управління інформаційною безпекою, контроль, аналіз, вразливість, PDA, Windows CE, Pocket, безпека розробки, secure programming, CERT, computationally secure, incident, порушення інформаційної безпеки, загроза інформаційній безпеці, безпека розробки, аналіз вразливостей, група реагування, internet security, ISS, CVE, аналіз загроз та ін.

У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати:

- основи інформаційної безпеки, ключові принципи та стандарти (ISO/IEC 27001, NIST);
- типи загроз та вразливостей інформаційних систем;
- методи та засоби захисту інформації, включаючи криптографію, автентифікацію та управління доступом;
- основи управління ризиками інформаційної безпеки;
- політики, процедури та нормативно-правові акти у сфері інформаційної безпеки;
- методи моніторингу, виявлення та реагування на інциденти безпеки;
- юридичні та етичні аспекти захисту інформації.

вміти:

- ідентифікувати та аналізувати загрози інформаційній безпеці;
- розробляти та впроваджувати політики і процедури інформаційної безпеки;
- здійснювати оцінку ризиків і застосовувати відповідні заходи для їх зниження.
- використовувати засоби криптографічного захисту даних;
- налаштовувати системи контролю доступу та управління привілеями користувачів.
- організовувати моніторинг інформаційної інфраструктури для виявлення інцидентів безпеки.
- розробляти плани дій при інцидентах і забезпечувати безперервність бізнес-процесів.

набути соціальних навичок(soft-skills):

- здійснювати професійну комунікацію IT-індустрії;
- ефективно пояснювати і презентувати матеріал;
- працювати в команді діяльності та виділяти авторський внесок;
- взаємодіяти в професійному IT-середовищі з питань інформаційної безпеки та комерційної таємниці.

2. ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ «УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ІТ СФЕРІ»

Теми	Кількість годин відведених на:			Години
	Лекції	Практичні заняття	Самостійну роботу	Всього
1	2	3	4	6
Змістовий модуль 1. Теоретичні засади менеджменту інформаційною безпекою в ІТ сфері				
Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки.	2	1	4	7
Тема 2. Діяльність міжнародних організацій в сфері інформаційної безпеки.	2	1	4	7
Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки.	2	1	4	7
Тема 4. Роботи спеціалізованих міжнародних ІТ-організацій та об'єднань в галузі інформаційної безпеки.	2	1	4	7
Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.	1	1	5	6
Змістовий модуль 2. Практичні засади управління інформаційною безпекою в ІТ сфері				
Тема 6. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США	1	1	4	6
Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України	1	1	5	6
Тема 8. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту)	1		4	6
Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту)	2		4	7

Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки	2	1	4	7
Змістовний модуль 3. Політика та моніторинг інформаційної безпеки в ІТ-сфері				
Тема 11. Зміст деталізованої політики безпеки	1		5	6
Тема 12. Департамент інформаційної безпеки і робота з персоналом	1	1	4	6
Тема 13. Організація реагування на надзвичайні ситуації (інциденти).	1		6	7
Тема 14. Аудит стану інформаційної безпеки на підприємстві.	1	1	5	7
Тема 15. Надання послуг у сфері інформаційної безпеки.	1		6	7
Тема 16. Надання послуг у сфері інформаційної безпеки (страхування).	1	1	5	7
Тема 17. Міжнародний стандарт ISO/IEC 27001.	1		6	7
Тема 18. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей.	1	1	5	7
Всього за семестр	**24**	**12**	**84**	**120**

3. ЗМІСТ ПРОГРАМИ ДИСЦИПЛІНИ «УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ІТ СФЕРІ»

Змістовий модуль 1. Теоретичні засади менеджменту інформаційною безпекою в ІТ сфері

Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки

План:

1.1. Загальні відомості.

1.2. Ризики, їх класифікація.

1.3. Способи порушення інформаційної безпеки.

1.4. Організаційне забезпечення інформаційної безпеки.

Тема 2. Діяльність міжнародних організацій в сфері інформаційної безпеки

План:

2.1. Загальні відомості.

2.2. Робота міжнародних професійних об'єднань.

2.3. International Telecommunication Union (ITU) – Міжнародний союз електрозв’язку.

2.4. Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки.

2.5. Association for Computing Machinery (ACM) – Асоціація обчислювальної техніки.

2.6. World Wide Web Consortium (W3C) – Консорціум Всесвітньої Павутини.

2.7. NIST – Національний інститут стандартів і технологій.

2.8. International Organization for Standardization (ISO) – Міжнародна організація з стандартизації.

Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки

План:

3.1. Вступ

3.2. Вимоги до розроблюваних стандартів

3.3. Типи стандартів

3.4. Елементи стандартів

3.5. Огляд стандартів РГ 1

Тема 4. Роботи спеціалізованих міжнародних IT-організацій та об'єднань в галузі інформаційної безпеки

План:

4.1. Вступ.

4.2. CERT Coordination Center (CERT/CC) – Координаційний центр CERT.

4.3. X-Force security intelligence team – Дослідницька група X-Force.

4.4. Альянси великих технологічних компаній.

4.5. Smart Card Alliance (SCA) – Альянс за смарт-картками.

4.6. Internet Security Alliance (ISA) – Альянс з безпеки мережі Інтернет.

4.7. The International Biometric Industry Association (IBIA) – Міжнародна асоціація компаній-виробників біометричного устаткування.

Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем

План:

5.1. Загальна методологія організаційного забезпечення інформаційної безпеки на рівні великих постачальників інформаційних систем.

5.2. Організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній.

Змістовий модуль 2. Практичні засади управління інформаційною безпекою в ІТ сфері

Тема 6. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США

План:

6.1. Загальна політика США у сфері інформаційної безпеки.

6.2. Структура органів державної влади, що забезпечують інформаційну безпеку в США.

6.3. Федеральні програми та ініціативи, підтримувані державою.

Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України

План:

7.1. Визначення інформаційної безпеки, об’єкти, суб’єкти, основні складові.

7.2. Система забезпечення інформаційної безпеки.

7.3. Загрози інформаційній безпеці України у контексті діяльності Держспецзв'язку.

7.4. Історія створення Держспецзв’язку.

7.5. Державна служба спеціального зв’язку та захисту інформації України (Держспецзв'язку).

7.6 Організаційна структура Держспецзв'язку.

Тема 8. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту)

План:

8.1. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

8.2. Криптографічний захист інформації.

8.3. Науково-технічна діяльність.

Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту)

План:

9.1. Технічний захист інформації в Україні, основні аспекти.

9.2. Побудова і організаційна структура системи ТЗІ в Україні.
9.3. Ліцензування діяльності у галузі ТЗІ.
9.4. Сертифікація засобів ТЗІ.
9.5. Державна експертиза у сфері ТЗІ.
9.6. Система підготовки та перепідготовки фахівців у галузі ТЗІ.
9.7. Державний контроль стану КТЗІ.

Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки

План:

10.1. Передумови розвитку менеджменту в сфері інформаційної безпеки на рівні підприємств.

10.2. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства.

10.3. Формування політики інформаційної безпеки на підприємстві.

Змістовний модуль 3. Політика та моніторинг інформаційної безпеки в IT-сфері

Тема 11. Зміст деталізованої політики безпеки

План:

11.1. Організація внутрішньооб'єктного режиму і охорони приміщень. 11.2. Фізичний захист.

11.3. Організація режиму секретності в установах і на підприємствах.

Тема 12. Департамент інформаційної безпеки і робота з персоналом

План:

12.1. Департамент інформаційної безпеки

12.2. Організаційна структура та персонал департаменту інформаційної безпеки

12.3. Робота з персоналом підприємства

Тема 13. Організація реагування на надзвичайні ситуації (інциденти)

План:

13.1. Вступ

13.2. Виявлення атак і розпізнавання вторгнень

13.3. Локалізація та усунення наслідків

13.4. Ідентифікація нападника (або джерела розповсюдження шкідливих програм)

13.5. Оцінка і подальший аналіз процесу нападу

Тема 14. Аудит стану інформаційної безпеки на підприємстві

План:

14.1. Аудит, види аудиту.

14.2. Етапи проведення аудиту.

Тема 15. Надання послуг у сфері інформаційної безпеки

План:

15.1. Передумови розвитку ринку послуг із забезпечення інформаційної безпеки і його структура.

15.2. Особливості деяких видів послуг.

15.3. Інфраструктура публічних ключів.

Тема 16. Надання послуг у сфері інформаційної безпеки (страхування)

План:

16.1. Страхування інформаційних ризиків. Основи методології страхування інформаційних ресурсів.

16.2. Ринок страхових послуг.

Тема 17. Міжнародний стандарт ISO/IEC 27001

План:

17.1. Розгляд міжнародного стандарту ISO/IEC 27001.

Тема 18. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей

План:

18.1. Захисні заходи і їх цілі

4. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИВЧЕННЯ ТЕМ ДИСЦИПЛІНИ

ТЕМА 1. ПЕРЕДУМОВИ ТА ОСНОВНІ НАПРЯМКИ РОЗВИТКУ МЕНЕДЖМЕНТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В темі визначаються цілі, завдання, передумови та напрямки організаційної та управлінської роботи у сфері інформаційної безпеки. Розглядаються такі поняття як ризик і загроза та представлено їх класифікацію. Наведено основні найбільш поширені на практиці способи порушення інформаційної безпеки та сучасні

технології захисту інформації. Пояснюється загальна структура курсу – яка включає в себе розгляд основних форм і прийомів організації роботи щодо забезпечення інформаційної безпеки на основних рівнях (рівень міжнародних професіональних організацій; рівень великих постачальників технічних (програмних і апаратних) засобів обробки і передачі інформації; рівень державних органів; рівень окремих підприємств, установ та організацій).

Основні поняття:

безпека, збиток, ймовірність, операційні ризики, захист інформації, об'єкт, активи, загроза інформаційній безпеці.

Питання для самоконтролю з теми 1:

1. Дайте визначення поняття інформаційна безпека. Назвіть основні чинники, які на неї негативно впливають, та методи, завдяки яким цьому можна запобігти.
2. Що таке загроза?
3. Назвіть види загроз.
4. Дайте визначення поняття ризик.
5. Назвіть види ризиків.
6. Назвіть основні способи порушення інформаційної безпеки.
7. Дайте визначення поняття СУІБ.
8. Прокоментуйте модель PDCA.

ТЕМА 2. ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В темі розкриваються цілі, принципи та специфіка роботи міжнародних незалежних організацій у сфері інформаційної безпеки. Наводиться змасштабована класифікація і перераховуються напрямки роботи таких структур. Описується робота організацій широкого профілю, таких як Міжнародний союз електрозв'язку, Інститут інженерів з електроніки та електротехніки, Асоціація обчислювальної техніки, Консорціум Всесвітньої Павутини, Міжнародна організація з стандартизації, що надають фундаментальний вплив на стан і розвиток інфраструктури мереж передачі даних і глобальних механізмів захисту інформації.

***Основні поняття*:**

діяльність, telecommunications, electronic engineering, computing machinery, internet engineering taskforce, ICSA, computationally secure, internet security, bureau, conference, lead, study, datanetwork, communication system, архітектура безпеки, системи автентифікації, інформаційне суспільство, computer society, technical committee, workshop, special interest group, SIG, CCS, communication security, electronic commerce.

Питання для самоконтролю з теми 2:

1. Що є елементами організаційної роботи на рівні міжнародних структур?
2. Назвіть основні найбільш великі і відомі міжнародні об'єднання, пов'язані з питаннями інформаційної безпеки.
3. Назвіть основні завдання Консорціуму Всесвітньої Павутини.
4. Назвіть головні завдання Міжнародної організації по стандартизації.

ТЕМА 3. СТАНДАРТИЗАЦІЯ В СФЕРІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У темі розглянуто сучасний стан стандартизації одного з найважливіших напрямків у захисті інформації – менеджменту інформаційної безпеки. Стандартизація є інструментом забезпечення якості продукції, робіт і послуг – важливого аспекту багатогранної комерційної діяльності. Мета стандартизації – досягнення оптимального ступеня упорядкування в тій чи іншій області за допомогою широкого і багаторазового використання встановлених положень, вимог, норм для вирішення реально існуючих, що плануються або потенційних завдань. *Розглянуто* серію стандартів ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою».

***Основні поняття*:**

інформаційна безпека, модель систем менеджменту, стандарт, управління ризиками, керівні вказівки, процес ний підхід

Питання для самоконтролю з теми 3:

1. Що таке стандартизація?
2. Що є найважливішими результатами стандартизації?
3. Назвіть основні вимоги до стандартів, що розробляються.
4. Які типи стандартів ви знаєте?
5. З яких елементів складається стандарт?
6. Назвіть стандарти серії 27000.

ТЕМА 4. РОБОТИ СПЕЦІАЛІЗОВАНИХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ОБ'ЄДНАНЬ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В темі перераховуються альянси великих технологічних компаній, організації, що займаються дослідницькою та інформаційною роботою в масштабі всієї спільноти фахівців у сфері інформаційної безпеки, таких як Координаційний центр CERT, Дослідницька група X-Force, Альянси великих технологічних компаній,

Альянс за смарт-картками, Альянс з безпеки мережі Інтернет, Міжнародна асоціація компаній-виробників біометричного устаткування. Описуються принципи побудови таких організацій, які вирішуються завдання, напрямки роботи.

Основні поняття:

управління інформаційною безпекою, об'єднання, CERT, computationally secure, incident, порушення інформаційної безпеки, загроза інформаційній безпеці, безпека розробки, аналіз вразливостей, група реагування, internet security, ISS, vulnerability, exposure, CVE, аналіз загроз

Питання для самоконтролю з теми 4:

1. Які існують альянси великих технологічних компаній, організації, що займаються дослідницькою та інформаційною роботою у сфері інформаційної безпеки.
2. Назвіть основні напрями організаційної роботи в сфері інформаційної безпеки Координаційного центру CERT.
3. Назвіть напрями діяльності Альянсу за смарт-картками.
4. Перерахуйте основні напрями діяльності Альянсу з безпеки мережі Інтернет

ТЕМА 5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА РІВНІ ВЕЛИКИХ ПОСТАЧАЛЬНИКІВ ІНФОРМАЦІЙНИХ СИСТЕМ

У темі розглядається роль великих постачальників інформаційних систем, що роблять найбільш серйозний вплив на розвиток інформаційних технологій та інфраструктуру інформаційних систем. Описується специфічна для них організаційна робота, яка спрямована на забезпечення безпечного функціонування інформаційних систем та вдосконалення власних продуктів і послуг, пропонованих на ринку. Розглянуто організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній, а саме на рівні Корпорації Microsoft яка є найбільшим у світі виробником програмного забезпечення та Компанії Cisco Systems, що є світовим лідером у виробництві обладнання для мереж передачі даних.

***Основні поняття*:**

об'єднання, мережа, значення, управління інформаційною безпекою, контроль, аналіз, вразливість, PDA, Windows CE, Pocket, безпека розробки, secure programming

Питання для самоконтролю з теми 5:

1. Назвіть основні прийоми зовнішньої організаційної роботи у сфері інформаційної безпеки на рівні великих компаній-постачальників інформаційних систем.

2. Назвіть основні прийоми внутрішньої організаційної роботи у сфері інформаційної безпеки на рівні великих компаній-постачальників інформаційних систем.

3. Організаційне забезпечення інформаційної безпеки на рівні Корпорації Cisco Systems.

4. Організаційне забезпечення інформаційної безпеки на рівні Microsoft.

ТЕМА 6. ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА США

Відповідно до загальної політики, а також наявної базової інфраструктури і сформованої практики державного управління в США протягом декількох років була організована і постійно вдосконалюється система державних органів, що здійснюють діяльність у сфері інформаційної безпеки: були створені спеціальні відомства та розширені завдання та повноваження раніше існуючих. Таким чином, в темі викладаються основні положення державної політики США у сфері інформаційної безпеки, а також описується структура і принципи діяльності основних державних органів, які працюють у цій сфері.

Основні поняття:

загроза інформаційній безпеці, обмін інформацією, оцінка вразливостей, інформаційні сиситема, безпека персоналу

Питання для самоконтролю з теми 6:

1. 1. Назвіть ключові напрями розвитку інформаційної безпеки США.

2. 2. Яка структура органів державної влади, що забезпечують інформаційну безпеку в США?

3. 3. Який структурний підрозділ у складі законодавчої гілки влади США займається питаннями інформаційної безпеки?

ТЕМА 7. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ

Державна політика національної безпеки в інформаційній сфері має створювати умови для реалізації конституційного права громадян своєї держави вільно отримувати і використовувати інформацію для вирішення таких важливих завдань, як формування національного інформаційного простору, включення його до світового інформаційного простору на засадах забезпечення інформаційного суверенітету та інформаційної безпеки і формування демократично орієнтованої свідомості. Головною метою державної політики національної безпеки в інформаційній сфері є створення необхідних економічних і соціокультурних умов,

правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів у всіх сферах життєдіяльності особи, суспільства і держави як органічного організму. В темі розглядаються основні положення державної політики України в сфері інформаційної безпеки, а також описується структура і принципи діяльності основних державних органів, що працюють в цій сфері.

Основні поняття:

інформаційна безпека, об'єкт, суб'єкт, загроза, захист інформації, Держспецзв**'**язку

Питання для самоконтролю з теми 7:

1. Що таке інформаційна безпека?
2. Назвіть об'єкти і суб'єкти інформаційної безпеки.
3. Назвіть основні складові інформаційної безпеки.
4. Перерахуйте основні функції системи забезпечення інформаційної діяльності.
5. Назвіть основні загрози національній безпеці України.
6. Яка державна структура є головною з питань криптографічного та технічного захисту інформації.
7. Основні завдання Держспецзв'язку.

ТЕМА 8. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ
(криптографічні методи захисту)

Серед всього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи. Криптографія – наука про математичні методи забезпечення конфіденційності і автентичності інформації. Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства. В темі розглядаються основні положення державної політики України в сфері інформаційної безпеки, а саме розглядається один з найважливіших напрямів діяльності у сфері забезпечення безпеки інформації – захист інформації криптографічними методами.

***Основні поняття*:**

інформаційна безпека, захист інформації, інформаційно-телекомунікаційні системи, криптографічний захист, шифрування, криптосистема

Питання для самоконтролю з теми 8:

1. Що таке криптографія?
2. Що таке криптографічний захист інформації?
3. Перерахуйте основні завдання криптографічного захисту інформації.

ТЕМА 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (технічні методи захисту)

Серед загроз інформації за своїми небезпечними наслідками особливе місце займають: а) здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку; б) несанкціонований доступ до інформації, яка обробляється та циркулює в інформаційних та телекомунікаційних системах в) витік інформації з обмеженим доступом технічними каналами. Для протидії зазначеним загрозам в державі створена, функціонує та розвивається система технічного захисту інформації, яка є сукупністю організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази. В темі розглядається реалізація державної політики України в сфері технічного захисту інформації (ТЗІ), а саме організаційна структура ТЗІ, ліцензування, сертифікація і державна експертиза в галузі ТЗІ.

Основні поняття: інформаційна безпека, захист інформації, технічний захист, ліцензування, сертифікація, експертиза, державний контроль, державна політика, науково-технічна діяльність

Питання для самоконтролю з теми 9:

1. Що таке технічний захист інформації?
2. Назвіть основні аспекти технічного захисту інформації в Україні.
3. Організаційна структура системи технічного захисту інформації в Україні.
4. Підготовка та перепідготовки фахівців у галузі технічного захисту інформації.

ТЕМА 10. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ПІДПРИЄМСТВА: ОСНОВНІ НАПРЯМКИ І СТРУКТУРА ПОЛІТИКИ БЕЗПЕКИ

Забезпечення власної інформаційної безпеки на підприємствах, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань та має велике значення не тільки для стратегічного

розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика, тощо. В темі перераховуються основні напрями управлінської (організаційної) роботи у сфері інформаційної безпеки на рівні окремого підприємства. Розкривається загальна структура політики інформаційної безпеки підприємства як основного організуючого документа в цій галузі.

***Основні поняття*:** ділова репутація, державна таємниця, банківська таємниця, управління інформаційною безпекою, ISO/IEC 27002

Питання для самоконтролю з теми 10:

1. Основні етапи розробки політики безпеки підприємства?
2. Назвіть основні аспекти управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства.
3. Назвіть основні кроки загального життєвого циклу політики інформаційної безпеки підприємства.

ТЕМА 11. ЗМІСТ ДЕТАЛІЗОВАНОЇ ПОЛІТИКИ БЕЗПЕКИ

Політика інформаційної безпеки – набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації. Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора – організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

В темі описується основний зміст розділів політики безпеки за окремими напрямами захисту інформації.

Основні поняття:

загроза інформаційній безпеці, розмежування доступу, ідентифікація, політика безпеки, пошук, доступ, державна таємниця, інформація, мережа, Інтернет, ідентифікація і аутентифікація, інформаційні системи, аутсорсинг, політика використання, передача даних, CDMA, PDA, бази даних, апаратні засоби, прийняття рішень

Питання для самоконтролю з теми 11:

1. Організація внутрішньооб'єктного режиму.
2. Що ви можете сказати про фізичний захист забезпечення інформаційної

безпеки.

3. Побудова політики інформаційної безпеки на підприємстві.

ТЕМА 12. ДЕПАРТАМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І РОБОТА З ПЕРСОНАЛОМ

В темі описується робота департаменту інформаційної безпеки як основної структурної одиниці, що відповідає за комплексний захист інформації на підприємстві. Розкривається внутрішня структура департаменту, основні завдання та напрями його діяльності, методи роботи. Також розкриваються основні аспекти роботи з персоналом підприємства, спрямованої на захист інформаційних активів (як в частині підбору і розстановки співробітників, пов'язаних з обробкою інформації, так і в частині поточної роботи з персоналом).

Основні поняття:

управління інформаційної безпекою, CISO, джерело загрози, інформаційні системи, державна таємниця, державна стратегія, аналіз, контроль поведінки, розподіл функцій, доступ, зловмисник

Питання для самоконтролю з теми 12:

1. Назвіть основні завдання департаменту інформаційної безпеки на підприємстві.
2. Які підрозділи можуть входити до складу департаменту інформаційної безпеки на підприємстві?
3. Яким чином підбирається персонал до департаменту інформаційної безпеки на підприємстві?

ТЕМА 13. ОРГАНІЗАЦІЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ (ІНЦИДЕНТИ)

Реагування на виникаючі надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким же важливим напрямком роботи, як і побудова системи захисту та запобігання порушень. Під інцидентом, як правило, розуміється будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди. В темі описуються основні розділи регламентів реагування на інциденти (надзвичайні ситуації) у сфері інформаційної безпеки.

Детально розкриваються типові дії, які повинні виконуватися персоналом підприємства при виникненні таких ситуацій.

***Основні поняття*:**

порушення інформаційної безпеки, збиток, виявлення порушень, аналіз, програмні засоби, група реагування, інформаційний сервіс, ділова репутація, distributed, service, ddos, Інтернет, сервер, прийняття рішень, інформаційні системи, атака, ймовірність

Питання для самоконтролю з теми 13:

1. Що таке атака?
2. Назвіть основні кроки процесу реагування на інцидент.
3. Виявлення атак і розпізнавання вторгнень.
4. Яким чином відбувається ідентифікація нападника?

ТЕМА 14. АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства і надійності засобів захисту інформації. Однак ми виходимо з того, що аудит інформаційної безпеки є комплексним дослідженням всіх аспектів інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо). В темі описуються цілі аудитів інформаційної безпеки, їх класифікації за типами, передбачувані результати роботи, а також детально розкривається процес проведення аудиту всіх основних етапів.

Основні поняття:

аудит, оцінка безпеки, управління інформаційною безпекою, контроль, безпека, шкода, камера відеоспостереження, поточний контроль, інформація, фізична захищеність

Питання для самоконтролю з теми 14:

1. Що таке аудит?
2. Назвіть основні етапи проведення аудиту.
3. Які основні роботи проводяться на етапі збору інформації та проведенні обстеження аудиторами.

ТЕМА 15. НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В темі розглядаються організаційні питання надання різних послуг, пов'язаних із забезпеченням інформаційної безпеки: аудиторських, консультаційних, послуг з впровадження технічних засобів захисту, а також послуг зі страхування інформаційних ризиків.

Основні поняття:

аутсорсинг, криптографічні засоби, загроза інформаційній безпеці, порушення інформаційної безпеки, Public Key Infrastructure, PKI, сервіс безпеки, діяльність, атака, збиток, аналіз, цифровий сертифікат, інформаційні технології, ділова репутація, електронний документообіг

Питання для самоконтролю з теми 15:

1. Що таке аутсорсинг?
2. Що таке інфраструктура публічних ключів?
3. Як розвивається ринок послуг із забезпечення інформаційної безпеки?

ТЕМА 16. НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СТРАХУВАННЯ)

Світова практика страхування інформаційних ризиків почала складатися в дев'яностих роках і отримала свій розвиток після 2000-го року, коли ризики інформаційної безпеки стали більш серйозними, В темі розглядаються організаційні питання надання різних послуг, пов'язаних із забезпеченням інформаційної безпеки: аудиторських, консультаційних, послуг з впровадження технічних засобів захисту, а також послуг зі страхування інформаційних ризиків.

Основні поняття:

аутсорсинг, криптографічні засоби, загроза інформаційній безпеці, порушення інформаційної безпеки, Public Key Infrastructure, PKI, сервіс безпеки, діяльність, атака, збиток, аналіз, досвід, цифровий сертифікат, технології, електронний документообіг

Питання для самоконтролю з теми 16:

1. Що є об’єктами страхування інформаційних ризиків?
2. Назвіть основні стадії процесу страхування інформаційних ризиків.
3. Назвіть найбільші світові компанії, що надають послуги зі страхування інформаційних ризиків.

ТЕМА 17. МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001

В темі розглядаються основні аспекти та положення, а саме інформаційні технології, методи забезпечення безпеки, системи менеджменту інформаційної безпеки, міжнародного стандарту ISO/IEC 27001.

ISO/IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації. Він також включає в себе вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації. Вимоги, викладені в ISO/IEC 27001 є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру.

Входить в групу стандартів ISO 27000 – СУІБ та тісно пов'язаний із стандартом ISO/IEC 27002.

Основні поняття:

інформаційна безпека, менеджмент, міжнародний стандарт, політика інформаційної безпеки, ризики, компетентність, моніторинг, аудит

Питання для самоконтролю з теми 17:

1. Що таке інформаційна безпека?
2. Що таке менеджмент інформаційної безпеки?
3. Що таке політика інформаційної безпеки?
4. Дайте визначення поняттю компетентність.
5. Що таке аудит?

ТЕМА 18. МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001. ПЕРЕЛІК ЗАХИСНИХ ЗАХОДІВ ТА ЇХ ЦІЛЕЙ

У темі наводиться перерахування ряду захисних заходів (політики в сфері інформаційної безпеки, організація інформаційної безпеки, безпека, пов'язана з людським фактором, управління активами, керування доступом, криптографія, фізична безпека, безпека комунікацій тощо), які були безпосередньо взяті і повністю відповідають перерахуванню, вказаному у стандарті ISO/IEC 27002: 2013.

Основні поняття:

політика інформаційної безпеки, захист інформації, активи, класифікація інформації, доступ, управління доступом, аудит, інформаційні системи, стандарт, тестові дані, менеджмент

Питання для самоконтролю з теми 18:

1. Що таке ризик?
2. Перерахуйте захисні дії в сфері інформаційної безпеки.

5. КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ

Протягом семестру здобувач може отримати max. 100 балів, у тому числі: перший рубіжний контроль – 50 балів, другий рубіжний контроль – 50 балів. По поточному контролю здобувач може набрати бали за активність на лекційних та практичних заняттях, виявлення рівня підготовки здобувачів із зазначеної теми під час опитування, тестування, презентації індивідуальних завдань, вирішення практичних ситуацій та кейсів, виконання практичних завдань.

Таблиця 1

Мінімальні та максимальні пороги встановлення максимальної кількості балів для конкретних видів робіт

Види робіт	Мінімальний поріг	Максимальний поріг
Відповіді на питання під час поточного опитування, участь у дискусії та виконання практичних завдань	0,5 балів	5,5 балів
Тести	0,5 балів	2,5 бали

Таблиця 2

Оцінювання видів робіт під час поточного оцінювання

Види робіт	Максимальна кількість балів під час поточного оцінювання	Максимальна кількість балів за один вид робіт	Орієнтовна кількість робіт, яку має виконати здобувач аби отримати максимальну кількість балів за поточним оцінюванням при оцінюванні кожного виду робіт максимальною кількістю балів	В тому числі розподіл за рубіжними контролями, враховуючи розподіл балів	
				I	II
Відповіді на питання під час поточного опитування, участь у дискусії та виконання практичних завдань	5,5	2,75	2 відповідей	27,5 балів	27,5 балів
Тестування	2,5	0,5	18 тестів	22,5 балів	22,5 балів
Разом	100 балів			50 балів	50 балів

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю студентів, усне опитування, тестовий контроль.

Форма підсумкового контролю: залік.

Семестровий залік полягає в оцінці рівня засвоєння здобувачем вищої освіти навчального матеріалу на лекційних, практичних, семінарських або лабораторних заняттях і виконання індивідуальних завдань за стобальною та дворівневою («зараховано», «не зараховано») та шкалою ЄКТС результатів навчання.

Критерії оцінки заліку:

- «**зараховано**» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

- «**не зараховано**» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
		для заліку
90-100	**A**	зараховано
82-89	**B**	
74-81	**C**	
64-73	D	
60-63	**E**	
35-59	FX	не зараховано з можливістю повторного складання
1-34	F	не зараховано з обов'язковим повторним вивченням дисципліни

6. ТЕСТИ ДЛЯ КОНТРОЛЮ ЗНАНЬ

1. Що з зазначеного є основним завданням інформаційної безпеки в IT-сфері?
a) Захист конфіденційності інформації від фізичного знищення
b) Захист конфіденційності, цілісності та доступності інформації
c) Збільшення кількості користувачів IT-системи
d) Оптимізація роботи програмного забезпечення
e) правильна відповідь відсутня

2. Яке з цих вимог вимагає "конфіденційності" в інформаційній безпеці?
a) Доступ до інформації дозволений лише авторизованим користувачам
b) Дані не можуть бути змінені без дозволу
c) Інформація завжди доступна для використання
d) Програмне забезпечення працює без помилок
e) правильна відповідь відсутня

3. Який із зазначених ризиків відносять до категорії «технічних ризиків» в IT-сфері?
a) Вірусні атаки
b) Неправомірний доступ до інформації співробітників
c) Порушення внутрішньої політики безпеки
d) Невірно налаштована організаційна структура
e) правильна відповідь відсутня

4. Що з зазначеного є прикладом «організаційних ризиків» в інформаційній безпеці?
a) Використання серверного обладнання
b) Недостатня компетентність співробітників
c) Застарілого програмного забезпечення
d) Недосконалість системи резервного копіювання
e) правильна відповідь відсутня

3. Який термін використовують для опису ризиків, пов'язаних із «недоліками в програмному забезпеченні»?
a) Логічні ризики
b) Фізичні ризики
c) Вразливості програмного забезпечення

d) Криптографічні ризики
e) правильна відповідь відсутня

4. Який із наступних прикладів застосовувати «фізичних ризиків» в інформаційній безпеці? Використання:
a) Хакерська атака на сервер
b) Збої в електрооживленні обробки даних
c) Слабких паролів
d) Атаки типу "відмова в обслуговуванні" (DDoS)
e) правильна відповідь відсутня

5. Як трактують поняття «рибалка» в інформаційній безпеці IT сектору?
a) Атака, при якій зловмисник намагається отримати конфіденційну інформацію за допомогою підготовлених електронних листів або веб-сайтів.
b) Атака фізична.
c) Проникнення.
d) Виманювання інформації шляхом обману.
e) правильна відповідь відсутня

6. Який метод атак виникає у зломі паролів шляхом підбору можливих комбінацій?
a) Інженерний
b) Маніпуляційний
c) Атака «грубої сили»
d) Метод обману
e) правильна відповідь відсутня

7. Що таке атака типу "відмова в обслуговуванні" (DoS)?
a) Зловмисник блокує доступ до веб-сайту чи сервісу, перевантажуючи його запитами
b) Зловмисник маніпулює вашою піблічною інформацією
c) Зловмисник зламує паролі
d) Зловмисник використовує боти
e) правильна відповідь відсутня

8. Що таке «соціальна інженерія» в контексті інформаційної безпеки?
a) Використання фізичної сили
b) Маніпуляція
c) Випитування
d) Атака
e) правильна відповідь відсутня

9. Який з наступних видів загроз належить до фізичних загроз ?

a) Шкідливе програмне забезпечення
b) Пожежа
c) Вірус
d) Невірний пароль
e) правильна відповідь відсутня

10. Який із наведених прикладів є внутрішньою загрозою ?
a) Природна катастрофа
b) Помилка працівників
c) Кібер атаки
d) Шкідливі звички
e) правильна відповідь відсутня

11. Яка організація відповідає за захист критичної інформаційної інфраструктури в Європейському Союзі?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ISO (Міжнародна організація зі стандартизації)
d) INTERPOL
e) правильна відповідь відсутня

12. Яка міжнародна організація розробляє рекомендації щодо управління інцидентами кібербезпеки?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ISO (Міжнародна організація зі стандартизації)
d) INTERPOL
e) правильна відповідь відсутня

13. Яка організація займається розробкою стандартів інформаційної безпеки, таких як ISO 27001?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ISO (Міжнародна організація зі стандартизації)
d) INTERPOL
e) правильна відповідь відсутня

14. Яка структура координує міжнародне співробітництво з кіберзлочинності?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ISO (Міжнародна організація зі стандартизації)
d) INTERPOL
e) правильна відповідь відсутня

15. Яка міжнародна організація керує стандартами телекомунікацій?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ITU (Міжнародний союз електрозв'язку)
d) INTERPOL
e) правильна відповідь відсутня

16. Яка організація відповідає за глобальну координацію роботи інтернет-провайдерів та доменних імен?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ITU (Міжнародний союз електрозв'язку)
d) ICANN
e) правильна відповідь відсутня

17. Яка міжнародна організація підтримує національні стратегії кібербезпеки держав-членів?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) ITU (Міжнародний союз електрозв'язку)
d) НАТО
e) правильна відповідь відсутня

18. Яка організація координує міжнародні операції з виявлення та розслідування кіберзлочинів?
a) ENISA (Європейське агентство з мережевої та інформаційної безпеки)
b) CERT (Computer Emergency Response Team)
c) INTERPOL
d) НАТО
e) правильна відповідь відсутня

19. Яка структура координує роботу з інтернет-безпеки в США?
a) CISA (Агентство з кібербезпеки та інфраструктурної безпеки)
b) CERT (Computer Emergency Response Team)
c) INTERPOL
d) НАТО
e) правильна відповідь відсутня

20. Яка організація розробляє стандарти телекомунікацій та інформаційної безпеки?
a) CISA
b) CERT

c) INTERPOL
d) ITU
e) правильна відповідь відсутня

21. Що таке стандартизація?
a) Процес створення нових технологій для виробництва продукції
b) Процес розробки та встановлення правил і норм для забезпечення єдності в різних сферах діяльності
c) Процес автоматизації виробництва для підвищення ефективності праці
d) Процес контролю якості продукції на всіх етапах виробництва
e) Процес укладання міжнародних угод у сфері торгівлі
)
22. Які з наведених результатів є найважливішими наслідками стандартизації?
a) Підвищення якості продукції
b) Зниження витрат на виробництво
c) Зменшення конкурентоспроможності компаній
d) Спрощення процесів сертифікації
e) Збільшення розмаїття продуктів на ринку

23. Які з наведених вимог є основними при розробці стандартів?
a) Наявність чітких і зрозумілих формулювань
b) Відсутність перевірок і тестувань
c) Забезпечення відповідності міжнародним нормам
d) Вимоги, що не підлягають змінам
e) правильна відповідь a) та c)

24. Які з наведених типів стандартів ви знаєте?
a) Технічні стандарти
b) Стандарти якості
c) Екологічні стандарти
d) Стандарти безпеки
e) всі відповіді вірні

25. З яких елементів складається стандарт?
a) Вимоги та рекомендації
b) Оцінка якості та рейтинг
c) Стратегії розвитку
d) Відомості про ринок
e) правильна відповідь відсутня

26. Який стандарт належить до серії 27000?
a) ISO 9001
b) ISO 14001

c) ISO 27001
d) ISO 45001
e) всі відповіді вірні

27. Вибери елементи стандартів?
a) політика та планування
b) реалізація та експлуатація
c) оцінювання та покращення
d) правильна відповідь відсутня
e) всі відповіді вірні

28. Стандарти типу С?
a) стандарт, що стосується надання настановчих вказівок
b) суміжний стандарт
c) стандарт, що стосується вимог
d) термінологічний стандарт
e) правильна відповідь відсутня

29. Стандарти типу А?
a) стандарт, що стосується надання настановчих вказівок
b) суміжний стандарт
c) стандарт, що стосується вимог
d) термінологічний стандарт
e) правильна відповідь відсутня

30. Стандарти типу В?
a) стандарт, що стосується надання настановчих вказівок
b) суміжний стандарт
c) стандарт, що стосується вимог
d) термінологічний стандарт
e) правильна відповідь відсутня

31. Яка організація відповідає за управління глобальною інформаційною безпекою?
a) ITU
b) NATO
c) WHO
d) ISO
e) WTO

32. Який стандарт ISO має пряме відношення до управління інформаційною безпекою?
a) ISO 9001

b) ISO 27001
c) ISO 14001
d) ISO 20000
e) ISO 45001

33. Яка організація займається формуванням політик кібербезпеки на глобальному рівні?
a) UNESCO
b) ICANN
c) IMF
d) OECD
e) ITU

34. Яка з наступних організацій розробляє рекомендації щодо кібербезпеки для урядів?
a) CTBTO
b) ISO
c) ENISA
d) ICRC
e) UNDP

35. Яка міжнародна організація відповідає за стандартизацію в галузі інформаційних технологій?
a) ISO
b) IEC
c) ITU
d) IEEE
e) W3C

36. Яка програма НАТО спрямована на вдосконалення кібербезпеки союзників?
a) Partnership for Peace
b) Cyber Defence Initiative
c) Open Door Policy
d) Collective Defence Policy
e) NATO Response Force

37. Яка із зазначених організацій не є спеціалізованою установою ООН?
a) WHO
b) ITU
c) WIPO
d) UNESCO
e) ICANN

38. Який документ визначає концепцію управління інформаційною безпекою в підприємствах?
a) ISO 9001
b) NIST SP 800-53
c) ITIL
d) COBIT
e) ISO 14001

39. Яка організація пропонує ресурси та тренінги з кібербезпеки для малих і середніх підприємств?
a) SANS Institute
b) IEEE
c) ISACA
d) ENISA
e) NIST

40. Яка міжнародна організація активно займається дослідженнями в галузі кіберзагроз?
a) ECC
b) CERT
c) ITU
d) NATO
e) ISO

41. Який документ найчастіше використовується для управління інформаційною безпекою в організаціях?
a) ISO 27001
b) NIST SP 800-53
c) COBIT
d) ITIL
5. GDPR

42. Яка роль Chief Information Security Officer (CISO) в управлінні інформаційною безпекою в компанії?
a) Відповідає за технічну підтримку
b) Розробляє стратегію інформаційної безпеки
c) Контролює фінансові витрати на IT
d) Здійснює продажі IT-рішень
e) Веде кадрову політику

43. Що є основною метою управління інформаційною безпекою?
a) Підвищення обсягів продажу

b) Захист інформаційних активів
c) Зменшення витрат на IT
d) Вдосконалення програмного забезпечення
e) Розширення ринку

44. Який із зазначених ризиків найчастіше пов'язаний з інформаційною безпекою?
a) Втрати даних через крадіжку
b) Збільшення витрат на енергію
c) Погіршення якості продукту
d) Втрата клієнтів
e) Неплатоспроможність

45. Який з методів є найбільш ефективним для захисту інформаційних систем?
a) Антивірусне програмне забезпечення
b) Фізичний захист серверів
c) Регулярні навчання персоналу
d) Введення політики паролів
e) Використання системи контролю доступу

46. Яка роль політики управління інформаційною безпекою в компанії?
a) Зменшення витрат
b) Встановлення правил та процедур
c) Залучення інвесторів
d) Розвиток нових продуктів
e) Моніторинг ринку

47. Які з наступних дій є частиною процесу ризик-менеджменту в інформаційній безпеці?
a) Ідентифікація, оцінка, управління ризиками
b) Збільшення продажів
c) Розробка нових продуктів
d) Кадрові зміни
e) Проведення маркетингових досліджень

48. Яка з наступних загроз є прикладом кібербезпеки?
a) Фізичне знищення серверів
b) Фішинг-атаки
c) Неправильне зберігання документації
d) Погіршення умов праці
e) Втрата бізнес-контрактів

49. Яка технологія найбільш поширена для шифрування даних в інформаційних системах?
a) AES (Advanced Encryption Standard)
b) DES (Data Encryption Standard)
c) RSA (Rivest-Shamir-Adleman)
d) SHA (Secure Hash Algorithm)
e) ECC (Elliptic Curve Cryptography)

50. Яка система підтримки прийняття рішень часто використовується для оцінки загроз у інформаційній безпеці?
a) ERP
b) CRM
c) SIEM
d) DLP
e) HRM

51. Який державний орган у США несе основну відповідальність за координацію кібербезпеки на національному рівні?
a) Міністерство оборони
b) Департамент енергетики
c) Департамент національної безпеки (DHS)
d) Міністерство юстиції
e) ФБР

52. Який документ встановлює основні принципи кібербезпеки на національному рівні в США?
a) Національна стратегія безпеки
b) Стратегія кібербезпеки США
c) Виконавчий указ 13800 (Executive Order 13800)
d) Національний план захисту інфраструктури
e) Закон про захист особистих даних

53. Яка агенція відповідає за розробку стандартів та рекомендацій у сфері інформаційної безпеки в США?
a) ФБР
b) Центральне розвідувальне управління (CIA)
c) Агенція національної безпеки (NSA)
d) Національний інститут стандартів і технологій (NIST)
e) Федеральна комісія з комунікацій (FCC)

54. Яка структура у США координує відповіді на інциденти кібербезпеки на державному рівні?
a) Комітет національної безпеки
b) Національне агентство з кібербезпеки
c) US-CERT (United States Computer Emergency Readiness Team)
d) Рада з кіберзахисту
e) Комітет захисту критичної інфраструктури

55. Який закон США регулює діяльність приватних компаній щодо захисту конфіденційних даних клієнтів?
a) Закон про свободу інформації
b) Закон Патріот
c) Закон про кібербезпеку 2015 року
d) Закон про електронні комунікації
e) Закон про захист особистих даних (Privacy Act)

56. Яка роль Національної безпекової ради (National Security Council) у сфері інформаційної безпеки США?
a) Розробка технічних стандартів
b) Координація політики національної безпеки
c) Здійснення операцій з кіберзахисту
d) Розслідування інцидентів кібербезпеки
e) Розробка законодавчих ініціатив

57. Яка ініціатива була впроваджена для захисту критичної інфраструктури від кіберзагроз?
a) Програма захисту мережі уряду
b) Програма кіберрозвідки
c) Ініціатива захисту критичної інфраструктури (Critical Infrastructure Protection Initiative)
d) Ініціатива боротьби з кібертероризмом
e) Програма моніторингу комунікацій

58. Який підрозділ Міністерства оборони США відповідає за військові кібероперації?
a) Кіберкомандування США (USCYBERCOM)
b) Агенція кіберзахисту США
c) Рада з кібербезпеки при Пентагоні
d) Бюро інформаційних технологій
e) Офіс кіберінфраструктури

59. Який закон США дозволяє державним і приватним організаціям обмінюватися інформацією про кіберзагрози?
a) Закон про електронну приватність
b) Закон про захист даних
c) Закон про обмін інформацією з кібербезпеки (CISA - Cybersecurity Information Sharing Act)
d) Закон про захист кібермереж
e) Закон про національну безпеку

60. Яка система у США відповідає за моніторинг кіберзагроз і попередження про них на державному рівні?
a) Федеральна система кіберзахисту
b) Програма безпеки інтернету
c) EINSTEIN (Система моніторингу кібербезпеки)
d) Національна система попередження загроз
e) Програма контролю безпеки

61. Який орган державної влади в Україні відповідає за координацію діяльності у сфері кібербезпеки?
a) Міністерство оборони
b) Служба безпеки України
c) Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)
d) Національний банк України
e) Міністерство внутрішніх справ

62. Який закон України регулює питання кібербезпеки?
a) Закон про захист персональних даних
b) Закон про інформацію
c) Закон України "Про основні засади забезпечення кібербезпеки України"
d) Закон про доступ до публічної інформації
e) Закон про електронні комунікації

63. Який документ визначає основні принципи забезпечення кібербезпеки в Україні?
a) Програма кіберзахисту уряду
b) Стратегія кібербезпеки України
c) Закон про інформаційні технології
d) Національна програма захисту інфраструктури
e) Закон про телекомунікації

64. Який державний орган в Україні відповідає за розробку стандартів інформаційної безпеки?
a) Національний банк України
b) Міністерство цифрової трансформації
c) Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)
d) Верховна Рада України
e) Міністерство юстиції

65. Яка структура в Україні координує взаємодію між державними органами та приватним сектором у сфері кібербезпеки?
a) Міністерство оборони
b) Комітет національної безпеки і оборони
c) Національний координаційний центр кібербезпеки (НКЦК)
d) Офіс Президента
e) Служба безпеки України

66. Який закон України регулює захист персональних даних?
a) Закон України "Про кібербезпеку"
b) Закон України "Про захист персональних даних"
c) Закон України "Про інформацію"
d) Закон України "Про електронні документи та електронний документообіг"
e) Закон України "Про державні таємниці"

67. Яка організація в Україні відповідає за реагування на кіберінциденти?
a) Служба безпеки України
b) Міністерство оборони

c) МВС
d) CERT-UA (Computer Emergency Response Team of Ukraine)
e) Генеральний штаб

68. Який орган здійснює контроль за критичною інформаційною інфраструктурою в Україні?
a) Міністерство оборони
b) Міністерство цифрової трансформації
c) Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)
d) Рада національної безпеки і оборони (РНБО)
e) Верховна Рада України

69. Який документ є основним у регулюванні державної політики інформаційної безпеки України?
a) Закон України "Про державну службу"
b) Закон України "Про телекомунікації"
c) Закон України "Про інформацію"
d) Стратегія національної безпеки України
e) Закон України "Про захист державних таємниць"

70. Який підрозділ РНБО відповідає за координацію діяльності в сфері кібербезпеки?
a) Департамент кібербезпеки
b) Комітет захисту інформаційних технологій
c) Національний координаційний центр кібербезпеки (НКЦК)
d) Державна служба захисту критичної інфраструктури
e) Центр протидії інформаційним загрозам

71. Який орган в Україні відповідає за розробку та впровадження криптографічних методів захисту інформації?
a) Служба безпеки України
b) Національний банк України
c) Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)
d) Міністерство цифрової трансформації
e) Генеральний штаб України

72. Який закон України регулює застосування криптографічних засобів захисту інформації?
a) Закон України "Про електронні комунікації"
b) Закон України "Про захист персональних даних"
c) Закон України "Про державну таємницю"
d) Закон України "Про криптографічний захист інформації"
e) Закон України "Про телекомунікації"

73. Яка організація в Україні сертифікує криптографічні засоби захисту інформації?
a) Служба безпеки України
b) Міністерство внутрішніх справ
c) Міністерство цифрової трансформації

d) Адміністрація Держспецзв'язку
e) Департамент захисту інформаційних систем

74. Що є основним принципом криптографічного захисту інформації?
a) Фізична ізоляція систем
b) Надійне шифрування даних
c) Захист від вірусних атак
d) Використання ключів для шифрування і дешифрування інформації
e) Захист від соціальної інженерії

75. Яка технологія є основою криптографічного захисту інформації в Україні?
a) Мультифакторна автентифікація
b) Захист мережевих протоколів
c) Шифрування даних за допомогою симетричних та асиметричних алгоритмів
d) Використання антивірусного програмного забезпечення
e) VPN-з'єднання

76. Що таке цифровий підпис у контексті криптографії?
a) Електронний ключ для шифрування даних
b) Електронний аналог власноручного підпису, який забезпечує автентичність документів
c) Спосіб захисту мережевих з'єднань
d) Алгоритм шифрування файлів
e) Засіб захисту від несанкціонованого доступу

77. Який алгоритм шифрування використовується в Україні для забезпечення конфіденційності інформації?
a) DES (Data Encryption Standard)
b) ДСТУ ГОСТ 28147-2009
c) RSA
d) AES (Advanced Encryption Standard)
e) SHA-256

78. Що таке сертифікат відкритого ключа?
a) Програма для шифрування даних
b) Алгоритм для генерації ключів
c) Електронний документ, який підтверджує відповідність відкритого ключа певній особі або організації
d) Метод автентифікації користувачів
e) Інструмент для перевірки автентичності повідомлень

79. Яка служба в Україні відповідає за управління криптографічними ключами?
a) Національний банк України
b) Адміністрація Держспецзв'язку
c) Служба безпеки України
d) Міністерство цифрової трансформації
e) Верховна Рада України

80. Який вид шифрування застосовується для забезпечення конфіденційності в урядових системах України?

a) Одноразові паролі
b) Симетричне та асиметричне шифрування
c) Відкриті мережі
d) Захист на рівні мережевих протоколів
e) Пряме кодування без ключів

81. Який державний орган в Україні відповідає за впровадження технічних методів захисту інформації?
a) Міністерство оборони України
b) Служба безпеки України
c) Міністерство цифрової трансформації
d) Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)
e) Національний банк України

82. Що таке міжмережевий екран (файрвол)?
a) Програма для шифрування файлів
b) Протокол передачі даних
c) Антивірусне програмне забезпечення
d) Засіб для контролю і фільтрації трафіку між мережами
e) Мережевий комутатор

83. Який стандарт у сфері інформаційної безпеки є основним в Україні для захисту державних інформаційних систем?
a) ISO 27001
b) ГОСТ 34.003
c) NIST SP 800
d) ДСТУ ISO/IEC 27001:2015
e) RFC 1918

84. Що є основною метою використання систем виявлення та запобігання вторгнень (IDS/IPS)?
a) Збереження резервних копій
b) Шифрування даних
c) Розподіл доступу користувачів
d) Виявлення і запобігання несанкціонованому доступу до системи
e) Захист персональних даних

85. Який із зазначених методів використовується для захисту інформації на рівні мережевої інфраструктури?
a) Шифрування файлів на комп'ютері
b) Віртуальні приватні мережі (VPN)
c) Захист фізичного доступу до серверів
d) Використання цифрових підписів
e) Сканування уразливостей

86. Яке програмне забезпечення використовується для виявлення та знешкодження шкідливих програм у державних інформаційних системах?
a) VPN-клієнти
b) Серверні ОС

c) Антивірусне програмне забезпечення
d) Мережеві протоколи
e) Моніторинг безпеки мереж

87. Який з наведених технічних засобів забезпечує автентифікацію користувачів за допомогою біометричних даних?
a) Міжмережевий екран
b) Сканери відбитків пальців або розпізнавання обличчя
c) Шифрувальні ключі
d) IDS/IPS системи
e) Електронний підпис

88. Який протокол безпеки використовується для захисту переданих через Інтернет даних в Україні?
a) FTP
b) HTTPS (Hypertext Transfer Protocol Secure)
c) POP3
d) HTTP
e) SMTP

89. Який з інструментів захисту забезпечує резервне копіювання даних для відновлення після інцидентів?
a) Міжмережеві екрани
b) Системи контролю доступу
c) Системи резервного копіювання та відновлення даних
d) Антивірусне програмне забезпечення
e) IDS/IPS

90. Який технічний метод забезпечує захист фізичних серверів у державних установах України?
a) Антивірусне ПЗ
b) Захист мережі VPN
c) Системи контролю фізичного доступу (відеоспостереження, картки доступу)
d) Системи шифрування файлів
e) Файрволи

91. Який документ є основою для регулювання процесів інформаційної безпеки на підприємстві?
a) Статут підприємства
b) Бізнес-план
c) Операційний план
d) Політика інформаційної безпеки
e) Договір з постачальниками

92. Який стандарт міжнародно визнаний для впровадження системи управління інформаційною безпекою (СУІБ)?
a) ISO 9001
b) ISO 14001
c) ISO/IEC 27001

d) NIST SP 800-53
e) COBIT

93. Що таке аналіз ризиків в контексті інформаційної безпеки?
a) Виявлення недоліків у програмному забезпеченні
b) Процес встановлення доступів до інформаційних систем
c) Оцінка ймовірності виникнення загроз та їх потенційного впливу на підприємство
d) Тестування систем на вразливості
e) Резервне копіювання даних

94. Який з перелічених заходів є частиною технічної політики інформаційної безпеки на підприємстві?
a) Навчання персоналу
b) Створення політики конфіденційності
c) Визначення правил доступу до файлів
d) Встановлення міжмережевих екранів (файрволів)
e) Оцінка ризиків для бізнесу

95. Який основний принцип управління інцидентами інформаційної безпеки?
a) Шифрування даних
b) Встановлення антивірусного програмного забезпечення
c) Швидке виявлення та реагування на інциденти
d) Оновлення операційних систем
e) Регулярне тестування на вразливості

96. Що є основною метою політики контролю доступу до інформаційних ресурсів на підприємстві?
a) Зниження фінансових витрат
b) Підвищення продуктивності праці
c) Обмеження доступу до критичних ресурсів на основі ролей і прав
d) Встановлення централізованого управління
e) Полегшення процесу автентифікації

97. Який компонент інформаційної безпеки є відповідальним за забезпечення конфіденційності даних на підприємстві?
a) Відновлення даних
b) Аудит безпеки
c) Шифрування інформації
d) Резервне копіювання
e) Моніторинг мережевого трафіку

98. Що є основним напрямком роботи відділу інформаційної безпеки на підприємстві?
a) Розробка програмного забезпечення
b) Забезпечення захисту інформаційних активів підприємства
c) Підтримка IT-інфраструктури
d) Автоматизація бізнес-процесів
e) Оптимізація фінансових витрат на IT

99. Що таке політика реагування на інциденти інформаційної безпеки?
a) Політика шифрування даних
b) План розвитку IT-систем
c) Набір правил та процедур для виявлення, аналізу і реагування на інциденти інформаційної безпеки
d) Політика створення резервних копій
e) Стратегія управління ризиками

100. Який підхід використовується для управління інформаційною безпекою на підприємстві відповідно до стандарту ISO/IEC 27001?
a) Управління фінансовими ризиками
b) Управління ризиками інформаційної безпеки
c) Управління мережевими інцидентами
d) Розвиток IT-інфраструктури
e) Оптимізація бізнес-процесів

101. Який основний принцип організації внутрішньооб'єктного режиму на підприємствах?
a) Забезпечення доступу всім співробітникам до всіх приміщень
b) Використання виключно електронних замків
c) Обмеження доступу до окремих зон на основі функціональних обов’язків працівників
d) Використання відеоспостереження для кожного приміщення
e) Створення єдиної зони доступу для всіх працівників

102. Що є ключовим елементом фізичного захисту об'єкта?
a) Використання програмного забезпечення для захисту інформації
b) Зберігання даних у хмарних сервісах
c) Огорожа периметра та контроль доступу до об'єкта
d) Регулярне оновлення операційних систем
e) Підтримка резервних копій даних

103. Які засоби є основними для контролю фізичного доступу на об'єкті?
a) Біометричні системи, зони безпеки
b) Оцінка ризиків та антивірусне ПЗ
c) Звичайні ключі та електронні пошти
d) Системи карткового доступу, біометричні сканери, відеоспостереження
e) Автоматизовані робочі місця

104. Який документ визначає порядок організації секретного діловодства на підприємствах?
a) Політика конфіденційності
b) Закон про доступ до публічної інформації
c) Закон про персональні дані
d) Інструкція з організації режиму секретності
e) Регламент IT-безпеки

105. Що є основною метою організації режиму секретності на підприємстві?
a) Захист авторських прав
b) Виконання міжнародних договорів

c) Запобігання кіберзлочинам
d) Захист від розголошення державної або комерційної таємниці
e) Контроль витрат на безпеку

106. Який із зазначених методів є частиною фізичного захисту об'єкта?
a) Використання антивірусного ПЗ
b) Розробка шифрувальних алгоритмів
c) Налаштування мережевих протоколів
d) Охоронна сигналізація та патрулювання території
e) Зберігання інформації в хмарі

107. Яка з перелічених дій є частиною організації внутрішньооб'єктного режиму?
a) Встановлення антивірусного ПЗ на всі комп'ютери
b) Використання електронної пошти для внутрішньої комунікації
c) Контроль відвідувачів та реєстрація їхнього перебування на об'єкті
d) Зберігання резервних копій у віддаленому центрі обробки даних
e) Регулярне проведення навчання з кібербезпеки

108. Хто є відповідальним за організацію режиму секретності на підприємстві?
a) IT-відділ
b) Спеціально призначена посадова особа з режиму секретності
c) Фінансовий директор
d) Керівник відділу кадрів
e) Юридичний відділ

109. Що включає система охорони об'єкта для фізичного захисту інформації?
a) Використання електронної пошти для передачі даних
b) Застосування електронного документообігу
c) Встановлення систем відеоспостереження та сигналізації
d) Автоматизація обробки інформації
e) Резервне копіювання даних на зовнішні носії

110. Який метод захисту використовується для забезпечення фізичної безпеки серверних кімнат на підприємстві?
a) Використання антивірусного ПЗ
b) Шифрування даних
c) Контроль фізичного доступу за допомогою карт або біометричних систем
d) Використання VPN
e) Зберігання даних в зашифрованому вигляді

111. Яка основна роль департаменту інформаційної безпеки на підприємстві?
a) Контроль фінансових потоків
b) Управління бізнес-процесами
c) Забезпечення захисту інформаційних активів і мінімізація ризиків витоку інформації
d) Встановлення обладнання для офісу
e) Розробка програмного забезпечення

112. Яке з наведених завдань є відповідальністю департаменту інформаційної безпеки?

a) Створення маркетингових стратегій
b) Забезпечення технічної підтримки співробітникам
c) Контроль витрат на IT
d) Виявлення і реагування на інциденти інформаційної безпеки
e) Розробка продуктів компанії
)

113. Що є ключовим напрямком роботи з персоналом у сфері інформаційної безпеки?
a) Підвищення заробітної плати
b) Проведення навчання та тренінгів з безпеки для співробітників
c) Оцінка продуктивності працівників
d) Створення резервних копій інформації
e) Встановлення корпоративної пошти

114. Яка основна мета навчання співробітників щодо інформаційної безпеки?
a) Підвищення мотивації до роботи
b) Створення команди для виконання проєктів
c) Формування обізнаності працівників про загрози та їхнє навчання щодо методів захисту
d) Підвищення кваліфікації у сфері маркетингу
e) Організація робочого процесу в IT-відділі

115. Хто несе відповідальність за безпеку даних на рівні користувачів в компанії?
a) Фінансовий директор
b) Кожен співробітник, який працює з корпоративною інформацією
c) Лише директор компанії
d) Лише департамент IT
e) Юридичний відділ

116. Який інструмент допомагає відстежувати дії співробітників з інформацією?
a) Антивірусне програмне забезпечення
b) Шифрування даних
c) Система контролю доступу та аудиту (SIEM-системи)
d) Встановлення міжмережевих екранів
e) Використання VPN

117. Що є одним із ключових компонентів політики безпеки щодо роботи з персоналом?
a) Використання корпоративного транспорту
b) Оптимізація робочих процесів
c) Регламентація прав доступу до інформації на основі посадових обов'язків
d) Впровадження корпоративного стилю
e) Оформлення страхування працівників

118. Що повинно бути зроблено при наймі нового співробітника в контексті інформаційної безпеки?
a) Надання співробітнику доступу до всіх корпоративних ресурсів
b) Оформлення страховки
c) Ознайомлення з політиками інформаційної безпеки та підписання зобов'язання про нерозголошення

d) Призначення співробітника адміністратором системи
e) Встановлення антивірусного ПЗ на його пристрій

119. Як називається процес перевірки співробітників перед наданням доступу до конфіденційної інформації?
a) Аудит безпеки
b) Розслідування інцидентів
c) Фоновий скринінг або перевірка благонадійності (background check)
d) Оцінка персоналу
e) Сертифікація безпеки

120. Що повинна включати процедура звільнення співробітника для забезпечення інформаційної безпеки?
a) Оплата відпускних
b) Відкликання всіх прав доступу та видалення його акаунтів з інформаційних систем
c) Надання рекомендацій для наступного роботодавця
d) Архівування всіх електронних листів
e) Встановлення паролів для нових співробітників

121. Що є основною метою реагування на інциденти інформаційної безпеки?
a) Зниження фінансових витрат
b) Розширення IT-інфраструктури
c) Мінімізація шкоди і відновлення нормальної роботи після інциденту
d) Проведення технічного обслуговування систем
e) Оновлення програмного забезпечення

122. Який перший етап у процесі реагування на інцидент?
a) Відновлення нормальної роботи
b) Аналіз інциденту
c) Виявлення та ідентифікація інциденту
d) Інформування керівництва
e) Видалення шкідливого програмного забезпечення

123. Хто зазвичай відповідає за організацію реагування на інциденти в організації?
a) Відділ маркетингу
b) Команда реагування на інциденти (Incident Response Team, IRT)
c) Відділ продажів
d) Відділ кадрів
e) Всі працівники організації

124. Яка ключова дія повинна бути виконана після виявлення інциденту?
a) Відновлення даних
b) Зміна паролів
c) Інформування зацікавлених сторін та відповідальних осіб
d) Оновлення антивірусного ПЗ
e) Встановлення нового обладнання

125. Що включає процес ескалації інциденту?

a) Створення резервних копій даних
b) Передача інциденту на вищий рівень управління або фахівцям, якщо він не може бути вирішений на початковому рівні
c) Повідомлення поліції
d) Оцінка збитків
e) Закриття інциденту

126. Яка з наведених фаз є останньою у процесі реагування на інцидент?
a) Виявлення інциденту
b) Постінцидентний аналіз і звітність
c) Ескалація інциденту
d) Очищення систем від загроз
e) Оцінка збитків

127. Що таке постінцидентний аналіз?
a) Створення плану захисту
b) Розробка нових систем безпеки
c) Оцінка причин інциденту, наслідків і якості реагування для уникнення подібних ситуацій у майбутньому
d) Архівування даних
e) Оцінка фінансових витрат

128. Яка основна мета плану реагування на інциденти?
a) Зниження витрат на IT-обладнання
b) Автоматизація бізнес-процесів
c) Контроль доступу до інформаційних систем
d) Забезпечення оперативного і ефективного реагування на інциденти з мінімізацією шкоди
e) Підвищення продуктивності співробітників

129. Який з наведених документів описує порядок дій при виникненні інцидентів?
a) Політика конфіденційності
b) План розвитку IT-інфраструктури
c) План реагування на інциденти (Incident Response Plan)
d) Бізнес-план компанії
e) Посадова інструкція IT-спеціаліста

130. Що є важливим елементом у забезпеченні успішного реагування на інциденти?
a) Наявність резервних копій даних
b) Встановлення нових серверів
c) Наявність заздалегідь розроблених планів реагування і спеціально навченої команди
d) Встановлення додаткового антивірусного ПЗ
e) Використання хмарних сервісів для зберігання даних

131. Яка основна мета аудиту інформаційної безпеки на підприємстві?
a) Підвищення продуктивності праці
b) Оцінка фінансових витрат
c) Виявлення вразливостей і оцінка рівня захисту інформаційних активів
d) Розробка нових продуктів
e) Оптимізація бізнес-процесів

132. Яка з наведених діяльностей не є частиною процесу аудиту інформаційної безпеки?
a) Оцінка ризиків
b) Проведення маркетингових досліджень
c) Аналіз політик і процедур безпеки
d) Інтерв'ювання працівників
e) Перевірка фізичного доступу до приміщень

133. Який стандарт є основним для проведення аудиту інформаційної безпеки?
a) ISO 9001
b) ISO 14001
c) ISO/IEC 27001
d) NIST SP 800-53
e) COBIT

134. Що таке "внутрішній аудит" в контексті інформаційної безпеки?
a) Аудит, що проводиться зовнішніми експертами
b) Аудит, що проводиться співробітниками підприємства для оцінки власних процесів безпеки
c) Аудит, що стосується тільки фінансів
d) Аудит, що не має значення для безпеки
e) Аудит, що проводиться тільки один раз на рік

135. Який із зазначених етапів є першим у процесі аудиту інформаційної безпеки?
a) Аналіз результатів
b) Планування аудиту
c) Проведення інтерв'ю
d) Визначення політик безпеки
e) Підготовка звіту

136. Яка з наведених інформаційних систем є важливою для збору даних під час аудиту?
a) Системи управління проектами
b) Системи бухгалтерського обліку
c) Системи моніторингу безпеки (SIEM-системи)
d) Системи для електронної пошти
e) Системи управління кадрами

137. Який документ зазвичай підготовлюється в результаті аудиту інформаційної безпеки?
a) Бізнес-план
b) Політика конфіденційності
c) Звіт про результати аудиту
d) Регламент використання IT-ресурсів
e) Інструкція з безпеки

138. Яка з наведених дій є важливою для вдосконалення системи інформаційної безпеки після аудиту?

a) Зміна співробітників
b) Підвищення заробітної плати
c) Впровадження рекомендованих заходів безпеки на основі висновків аудиту
d) Розширення IT-інфраструктури
e) Проведення маркетингових кампаній

139. Який метод може бути використаний для перевірки ефективності заходів безпеки на підприємстві?
a) Тестування на проникнення (penetration testing)
b) Оцінка фінансових показників
c) Моніторинг продажів
d) Опитування клієнтів
e) Порівняння з конкурентами

140. Який з аспектів є найважливішим для успішного проведення аудиту інформаційної безпеки?
a) Використання дорогих технологій
b) Підтримка з боку керівництва та співробітників підприємства
c) Часті зміни в політиках
d) Відсутність зовнішніх експертів
e) Наявність великої команди аудиторів

141. Яка з наведених послуг є основною у сфері інформаційної безпеки?
a) Розробка програмного забезпечення
b) Маркетингові дослідження
c) Оцінка ризиків і впровадження заходів безпеки
d) Продаж апаратного забезпечення
e) Організація корпоративних заходів

142. Який з методів захисту є ключовим у наданні послуг інформаційної безпеки?
a) Соціальна інженерія
b) Веб-дизайн
c) Шифрування даних
d) SEO-оптимізація
e) Продаж реклами

143. Яка з наведених послуг передбачає регулярний моніторинг безпеки інформаційних систем?
a) Управління інцидентами безпеки
b) Консультаційні послуги
c) Технічна підтримка
d) Розробка веб-сайтів
e) Проведення семінарів

144. Що таке penetration testing у контексті інформаційної безпеки?
a) Перевірка фінансової звітності
b) Метод тестування системи на вразливості шляхом імітації атак
c) Процес резервного копіювання

d) Аудит маркетингових кампаній
e) Оцінка продуктивності персоналу

145. Яка послуга забезпечує навчання співробітників підприємства з питань інформаційної безпеки?
a) Технічна підтримка
b) Проведення тренінгів і семінарів
c) Розробка програмного забезпечення
d) Системна інтеграція
e) Продаж апаратного забезпечення

146. Яка з наведених послуг є частиною комплексного підходу до інформаційної безпеки?
a) Лише тестування програмного забезпечення
b) Оцінка фінансових ризиків
c) Впровадження політик безпеки, моніторинг та управління інцидентами
d) Розробка веб-додатків
e) Рекламні кампанії

147. Що є основним результатом надання послуг у сфері інформаційної безпеки?
a) Підвищення витрат на IT
b) Зменшення ризиків витоку інформації та забезпечення конфіденційності даних
c) Збільшення кількості співробітників
d) Підвищення продажів компанії
e) Підготовка нових продуктів

148. Яка послуга передбачає проведення аудитів для визначення відповідності стандартам безпеки?
a) Маркетингова стратегія
b) Аудит інформаційної безпеки
c) Веб-дизайн
d) Технічна підтримка
e) Розробка корпоративного стилю

149. Що таке "Managed Security Services" (MSS)?
a) Послуги з обслуговування комп'ютерних мереж
b) Аутсорсинг функцій безпеки інформаційних систем
c) Виробництво апаратного забезпечення
d) Послуги з розробки програмного забезпечення
e) Проведення маркетингових кампаній

150. Який аспект є ключовим для вибору постачальника послуг інформаційної безпеки?
a) Вартість послуг
b) Досвід та репутація компанії у сфері інформаційної безпеки
c) Розмір компанії
d) Наявність фізичних офісів
e) Кількість співробітників
b)

151. Яка основна мета страхування у сфері інформаційної безпеки?
a) Зниження витрат на IT
b) Захист від фінансових втрат унаслідок інцидентів інформаційної безпеки
c) Підвищення продажів
d) Зменшення витрат на персонал
e) Підвищення продуктивності праці

152. Який вид страхування покриває ризики, пов'язані з витоком конфіденційних даних?
a) Страхування кіберризиків
b) Страхування життя
c) Страхування майна
d) Страхування відповідальності
e) Страхування здоров'я

153. Який з наведених факторів може вплинути на вартість страхування кіберризиків?
a) Розмір компанії
b) Географічне положення
c) Наявність заходів безпеки та системи управління ризиками
d) Кількість працівників
e) Тип продукції

154. Яка з наведених послуг може бути включена в поліс страхування кіберризиків?
a) Оцінка фінансових показників
b) Технічна допомога при реагуванні на інциденти
c) Розробка маркетингових стратегій
d) Консультації з питань податків
e) Продаж програмного забезпечення

155. Який документ регламентує умови страхування в сфері кібербезпеки?
a) Страховий поліс
b) Контракт на обслуговування
c) Політика конфіденційності
d) Бізнес-план
e) Технічна документація

156. Який з наведених ризиків є найбільш поширеним у страхуванні кіберризиків?
a) Ризик падіння акцій
b) Ризик природних катастроф
c) Ризик витоку даних через хакерські атаки
d) Ризик невиконання контракту
e) Ризик інфляції

157. Які дані зазвичай потрібні для оцінки ризиків при страхуванні інформаційної безпеки?
a) Вартість нерухомості
b) Дохід компанії

c) Історія інцидентів інформаційної безпеки та поточні заходи безпеки
d) Кількість працівників
e) Географічне положення

158. Який з наведених аспектів не є об'єктом страхування в сфері інформаційної безпеки?
a) Витрати на відновлення систем
b) Погіршення репутації компанії
c) Витрати на юридичні послуги
d) Витрати на консультації з безпеки
e) Витрати на відшкодування збитків третім особам

159. Яка з наведених дій є важливою для зменшення ризиків при страхуванні кіберризиків?
a) Впровадження комплексних заходів безпеки
b) Зниження кількості працівників
c) Зменшення обсягу даних
d) Використання тільки безкоштовного програмного забезпечення
e) Залучення зовнішніх консультантів

160. Як страхування може допомогти підприємству після інциденту інформаційної безпеки?
a) Витрати на рекламу
b) Відшкодування витрат на відновлення та реагування на інцидент
c) Збільшення кількості співробітників
d) Підвищення заробітної плати
e) Організація тренінгів для співробітників

161. Яка основна мета стандарту ISO/IEC 27001?
a) Регулювання фінансових звітів
b) Визначення стандартів якості продукції
c) Встановлення вимог до системи управління інформаційною безпекою (ISMS)
d) Оцінка екологічного впливу
e) Розробка нових технологій

162. Яка структура стандарту ISO/IEC 27001?
a) Включає лише технічні вимоги
b) Містить вимоги, рекомендації та інструкції щодо впровадження ISMS
c) Охоплює тільки фізичну безпеку
d) Зосереджується на фінансових питаннях
e) Не має чіткої структури

163. Що таке ISMS в контексті ISO/IEC 27001?
a) Інформаційна система управління
b) Система управління інформаційною безпекою
c) Інформаційні системи та методи захисту
d) Інформаційна служба медичних служб
e) Інститут систем управління

164. Який етап є першим у процесі впровадження стандарту ISO/IEC 27001?
a) Проведення аудиту
b) Оцінка ризиків
c) Підготовка звіту
d) Визначення політики безпеки
e) Розробка плану дій

165. Який документ є ключовим для впровадження стандарту ISO/IEC 27001?
a) Політика управління інформаційною безпекою
b) Бізнес-план
c) Контракт з постачальниками
d) Регламент використання ресурсів
e) Звіт про фінансові результати

166. Яка з наведених категорій ризиків не розглядається в стандарті ISO/IEC 27001?
a) Фізичні ризики
b) Технічні ризики
c) Політичні ризики
d) Людські ризики
e) Процесні ризики

167. Яка з наведених дій є частиною моніторингу в рамках ISO/IEC 27001?
a) Проведення регулярних внутрішніх аудитів
b) Зменшення витрат на IT
c) Впровадження нових продуктів
d) Збільшення кількості працівників
e) Проведення маркетингових кампаній

168. Який термін визначає аудити, що проводяться для оцінки відповідності ISO/IEC 27001?
a) Внутрішній аудит
b) Зовнішній аудит
c) Операційний аудит
d) Фінансовий аудит
e) Технічний аудит

169. Яка з наведених практик є важливою для підтримання сертифікації за ISO/IEC 27001?
a) Проведення одного аудиту на рік
b) Постійне вдосконалення системи управління інформаційною безпекою
c) Впровадження нових технологій без перевірки
d) Обмеження доступу до інформаційних ресурсів
e) Використання старих систем безпеки

170. Яка з наведених переваг пов'язана з сертифікацією за стандартом ISO/IEC 27001?
a) Підвищення фінансової звітності
b) Покращення довіри клієнтів до підприємства

c) Зменшення кількості працівників
d) Збільшення витрат на IT
e) Відсутність потреби в нових технологіях

171. Яка основна мета переліку захисних заходів у стандарті ISO/IEC 27001?
a) Оцінка фінансових ризиків
b) Створення маркетингової стратегії
c) Забезпечення конфіденційності, цілісності та доступності інформаційних активів
d) Оптимізація бізнес-процесів
e) Управління людськими ресурсами

172. Який з наведених заходів стосується фізичного захисту інформаційних активів?
a) Контроль фізичного доступу до приміщень і обладнання
b) Шифрування даних
c) Тестування на проникнення
d) Оцінка ризиків
e) Захист електронної пошти

173. Яка мета застосування заходу з управління доступом до інформації?
a) Забезпечення швидкого доступу до мережі
b) Обмеження доступу до інформаційних активів тільки для авторизованих користувачів
c) Моніторинг фінансових транзакцій
d) Розробка політики конфіденційності
e) Оптимізація використання апаратних ресурсів

174. Який захід захищає інформацію під час її передачі між системами або мережами?
a) Контроль фізичного доступу
b) Аудит інформаційної безпеки
c) Шифрування даних
d) Впровадження політик безпеки
e) Створення резервних копій

175. Яка мета заходів з управління інцидентами інформаційної безпеки?
a) Відстеження продуктивності працівників
b) Оцінка конкурентних ринків
c) Швидке виявлення, аналіз і реагування на інциденти безпеки
d) Збільшення продажів
e) Зниження вартості IT-ресурсів

176. Який з наведених заходів є важливим для забезпечення безпеки при залученні зовнішніх постачальників?
a) Зниження витрат на IT
b) Управління ризиками постачальників і контроль доступу до інформаційних ресурсів
c) Оптимізація бізнес-процесів
d) Встановлення програмного забезпечення
e) Проведення маркетингових досліджень

177. Яка мета заходів з управління безпекою мобільних пристроїв та віддаленого доступу?
a) Оптимізація продуктивності мережі
b) Забезпечення захисту інформації при використанні мобільних пристроїв і віддаленому доступі до систем
c) Зменшення витрат на мобільні пристрої
d) Підвищення швидкості доступу до даних
e) Створення резервних копій даних

178. Яка з наведених заходів належить до управління активами в ISO/IEC 27001?
a) Контроль фізичного доступу
b) Ідентифікація та класифікація інформаційних активів
c) Моніторинг фінансових показників
d) Залучення нових співробітників
e) Встановлення оновлень програмного забезпечення

179. Який захід забезпечує безперервність бізнесу в умовах порушень інформаційної безпеки?
a) Оцінка ризиків
b) Управління доступом
c) Підготовка планів з безперервності діяльності (BCP) і відновлення після катастроф (DRP)
d) Зниження витрат на IT
e) Проведення тренінгів з безпеки

180. Яка з наведених цілей стосується управління людськими ресурсами в контексті інформаційної безпеки?
a) Підвищення продуктивності праці
b) Проведення інтерв'ю
c) Забезпечення, щоб працівники розуміли свої обов’язки щодо захисту інформації
d) Зменшення витрат на навчання
e) Впровадження автоматизованих систем управління

7. Список рекомендованих для опрацювання джерел

Основна

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с. URL:

2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик.

3. Закон України «Про інформацію» URL: https://zakon.rada.gov.ua/laws/show/2657-12

4. Закон України Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР від 05.07.1994 р., URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

5. Полторак В.П. Інформаційна безпека та захист даних в комп’ютерних

технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». – Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.

6. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.

7. Букет Д.А. Управління інформаційною безпекою за допомогою комплексної системи захисту. (2022) URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2617

8. Управління інформаційною безпекою: навчально-методичний посібник./ А. І. Поворознюк, О.А. Поворознюк – Харків: НТУ «ХПІ», 2021. – 135 с.

9. Поворознюк О.А. Багатокритеріальна оцінка альтернатив при проєктуванні двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації / А.І. Поворознюк, О.А. Поворознюк, Г.Є. Філатова // Системи управління, навігації та зв'язку, 2021 – вип. 2(64) – С.92-95.

10. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 346 с

Додаткова

1. Susukailo, V., Opirsky, I., Yaremko, O. (2021). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. У Lecture Notes in Electrical Engineering (с. 257–271). Springer International Publishing. URL: https://doi.org/10.1007/978-3-030-92435-5_15

2. Kurii, Y. Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21-32.

3. (2022) ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html

4. (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/82875.html

5. (2013) ISO/IEC 27001: Information Technology — Security Techniques — Information Security Management Systems — Requirements. URL: https://www.iso.org/standard/54534.html

6. (2013) ISO/IEC 27002: Information Technology — Security Techniques — Code of Practice for Information Security Controls. URL: https://www.iso.org/standard/54533.html

7. 2020 ISO Survey of Management System Standards reveals 17% increase in certifications. URL: https://www.quality.org/article/2020-iso-survey-management-system-

standards-reveals-17- increase-certifications

8. MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. URL: https://msecb.com/wp-content/uploads/2023/01/MSECB-Transition-Policy-on-MS-Certification-to-ISOIEC27001.pdf?utm_source=sendinblue&utm_campaign=Clients%20ISOIEC%20270012022%20Transition% 20Policy&utm_medium=email

9. Global Cybersecurity Outlook 2022. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2022

10. ISO/IEC 27001: What's new in IT security? URL: https://www.iso.org/contents/news/2022/10/new-iso-iec27001.html

11. What Are The ISO 27001 Changes In 2022. URL: https://bestpractice.biz/what-are-the-iso-27001-changes-in2022/

12. ISO 27001 2013 vs. 2022 revision – What has changed? URL: https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/

13. ISO/IEC 27001 - What are the main changes in 2022? URL: https://pecb.com/article/isoiec-27001---what-arethe-main-changes-in-2022

14. ISO 27001: Аналіз змін та особливості відповідності новій версії стандарту. URL: file:///C:/Users/user/Downloads/Admin,+004.pdf

15. IT-безпека та інформаційна безпека – у чому різниця? URL: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/it-bezpeka-ta-informacijna-bezpeka-%E2%80%93-u-chomu-riznicya