МОН УКРАЇНИ

НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Проректор з навчальної роботи

Олександр ГРИЩУК

«29» квітня 2022 р.

ПРОГРАМА
АТЕСТАЦІЙНОГО ЕКЗАМЕНУ
за освітньо-професійною програмою
«ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ»

першого (бакалаврського) рівня вищої освіти
за спеціальністю 122 «Комп'ютерні науки»
галузі знань 12 «Інформаційні технології»

Освітня кваліфікація
Бакалавр з комп'ютерних наук

Київ – 2022

Програму атестаційного екзамену для атестації випускників першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Інформаційна безпека в комп'ютеризованих системах» за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» у 2021-2022 навчальному році розроблено кафедрою інформаційно-аналітичної діяльності та інформаційної безпеки.

Розглянуто та схвалено на засіданні кафедри інформаційно-аналітичної діяльності та інформаційної безпеки.

Протокол № 8 від 11 квітня 2022 року.

Розглянуто та схвалено на засіданні Вченої Ради факультету транспортних та інформаційних технологій.

Протокол № 8 від 26 квітня 2022 року.

Розглянуто та схвалено на засіданні Науково-методичної ради Національного транспортного університету.

Протокол № 29 від 29 квітня 2022 року.

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Атестаційний екзамен є формою атестації випускників першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Інформаційна безпека в комп'ютеризованих системах» за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» у 2021-2022 навчальному році. Атестація завершується видачею документа встановленого зразка про присудження здобувачу освітньої кваліфікації «Бакалавр з комп'ютерних наук «Інформаційна безпека в комп'ютеризованих системах»».

Атестаційний екзамен передбачає оцінювання досягнення результатів навчання, визначених освітньо-професійною програмою «Інформаційна безпека в комп'ютеризованих системах» для атестації.

Програма атестаційного екзамену для випускників першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Інформаційна безпека в комп'ютеризованих системах» за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» розроблена кафедрою інформаційно-аналітичної діяльності та інформаційної безпеки на основі цієї освітньо-професійної програми.

Атестаційний екзамен проводиться у письмовій формі з використанням тестових технологій. Процедура проведення атестаційного екзамену може змінюватись у разі несприятливої безпекової ситуації.

Білет атестаційного екзамену містить 14 запитань двох рівнів складності з основних профілюючих дисциплін.

Запитання першого рівня складності (з 1-го по 10-е запитання білета атестаційного екзамену) передбачають вибір студентом відповіді із наведених у білеті 3 варіантів відповіді, з яких тільки один правильний.

Запитання другого рівня складності (з 11-го по 14-е запитання білета атестаційного екзамену) передбачають надання студентом розгорнутої теоретичної відповіді.

Правильний на думку студента варіант відповіді на запитання першого рівня складності студент позначає безпосередньо на бланку білета атестаційного екзамену.

Відповідь на запитання другого рівня складності студент наводить на аркушах для письмової відповіді.

1. ДИСЦИПЛІНА «ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

1. Основні поняття та визначення

Мета, основні завдання та міжпредметні зв'язки навчальної дисципліни. Основні визначення та поняття інформаційної безпеки. Сутність захисту інформації. Завдання у сфері захисту інформації. Поняття та види загроз інформаційній безпеці. Стандарти інформаційної безпеки. Нормативно-правове забезпечення інформаційної безпеки.

2. Електричні і магнітні поля об'єктів

Фізичні поля об'єктів. Електричні і магнітні поля об'єктів та їх характеристики. Електромагнітне поле та електромагнітна хвиля. Діапазони, джерела та використання електромагнітних хвиль.

3. Акустичні поля об'єктів

Акустичні поля об'єктів та їх характеристики. Діапазони, джерела та використання пружних хвиль. Фізичні поля різної природи як носії інформації.

4. Технічні канали витоку інформації

Загальні поняття. Класифікація технічних каналів витоку інформації. Сутність та шляхи утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами. Канал побічних електромагнітних випромінювань ОТЗС. Канал побічних електромагнітних випромінювань ДТЗС. Канал паразитної модуляції сигналів ВЧ генераторів. Канал паразитної ВЧ генерації підсилювачів. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС. Канал побічних електромагнітних наведень на комунікації ДТЗС. Канал ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).

5. Технічні канали витоку мовної інформації

Акустичні канали витоку інформації. Акустовібраційні (віброакустичні) канали витоку інформації. Акустоелектричні канали витоку мовної інформації. Акустооптоелектронні (лазерні акустичні) канали витоку інформації. Канали ВЧ нав'язування (для зняття мовної інформації).

6. Засоби несанкціонованого отримання інформації

Засоби проникнення у приміщення, що захищається. Пристрої прослуховування приміщень. Радіозакладки. Пристрої для прослуховування телефонних ліній.

7. Методи і засоби віддаленого отримання інформації по технічним каналам

Методи і засоби під'єднання. Методи і засоби віддаленого отримання інформації. Системи прихованого відеоспостереження. Акустичний контроль приміщень через засоби телефонного зв'язку. Перехоплення електромагнітних випромінювань.

8. Захист акустичної, електронної та письмової інформації

Методи і засоби виявлення та блокування технічних каналів витоку акустичної інформації. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв.

Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист електронної інформації. Захист письмової інформації від оптичного зняття.

Орієнтовні питання для атестаційного екзамену

Запитання першого рівня складності

1. Що називається інформаційною безпекою?
2. У чому полягає сутність захисту інформації?
3. Які існують види захисту інформації?
4. Яке призначення технічного захисту інформації?
5. Що називається фізичним полем об’єкту?
6. Що є джерелом електричного поля?
7. Які фізичні величини є кількісними характеристиками електричного поля?
8. Що є джерелом магнітного поля?
9. Які фізичні величини є кількісними характеристиками магнітного поля?
10. Що таке електромагнітна хвиля?
11. Що називається акустичним полем?
12. Які частоти коливань відносяться до звукового діапазону частот?
13. Які частоти коливань відносяться до інфразвукового діапазону частот?
14. Які частоти коливань відносяться до ультразвукового діапазону частот?
15. Що таке небезпечний сигнал?
16. Як класифікують сигнали в залежності від природи фізичного поля?
17. Що може бути носієм інформації?
18. Що розуміють під витоком інформації?
19. Що називається технічним каналом витоку інформації?
20. Як класифікують технічні канали витоку інформації?
21. Що відносять до основних технічних засобів і систем?
22. Що відносять до допоміжних технічних засобів і систем?
23. Що називається акустичним каналом витоку інформації?
24. Що називається акустовібраційним каналом витоку інформації?
25. Які пристрої використовуються для прослуховування приміщень?
26. У чому полягає метод високочастотного нав’язування?
27. Які є канали витоку акустичної інформації?
28. Які є канали витоку електронної інформації?
29. Які є канали витоку письмової інформації?
30. Що таке радіозакладка?

Запитання другого рівня складності

1. Фізичні поля об’єктів
2. Характеристики і параметри електричних і магнітних полів об’єктів

3. Електромагнітне поле та електромагнітна хвиля
4. Шкала електромагнітних хвиль
5. Характеристики і параметри акустичних полів об’єктів
6. Діапазони, джерела та використання пружних хвиль
7. Фізичні поля різної природи як носії інформації
8. Поняття технічного каналу витоку інформації
9. Фізичні основи утворення технічних каналів витоку інформації
10. Класифікація технічних каналів витоку інформації
11. Канал побічних електромагнітних випромінювань ОТЗС
12. Канал побічних електромагнітних випромінювань ДТЗС
13. Канал паразитної модуляції сигналів ВЧ генераторів
14. Канал паразитної ВЧ генерації підсилювачів
15. Канал побічних електромагнітних наведень на лінії електроживлення ОТЗС
16. Канал побічних електромагнітних наведень на комунікації ДТЗС
17. Канал ВЧ нав’язування для зняття інформації, що обробляється в ОТЗС
18. Акустичні канали витоку інформації. Акустовібраційні канали витоку інформації
19. Акустооптоелектронні (лазерні акустичні) канали витоку інформації
20. Канали ВЧ нав’язування для зняття мовної інформації
21. Організаційно-технічні заходи щодо технічного захисту інформації
22. Пристрої прослуховування приміщень. Радіозакладки
23. Методи і засоби під’єднання. Методи і засоби віддаленого отримання інформації
24. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації
25. Захист акустичної інформації від зняття радіозакладними пристроями
26. Методи пошуку радіозакладних пристроїв
27. Захист інформації від витоку по технічних каналах, утворених ДТЗС
28. Захист інформації від несанкціонованого запису звукозаписувальними пристроями
29. Захист електронної інформації
30. Захист письмової інформації від оптичного зняття

Список рекомендованої літератури

1. Аль-Амморі А.Н., Іщенко Р.М., Дехтяр М.М. Основи технічного захисту інформації: методичні вказівки до виконання лабораторних робіт для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12

«Інформаційні технології» спеціальності 122 «Комп'ютерні науки» освітньої програми «Інформаційна безпека в комп’ютеризованих системах». – К.: НТУ, 2022. – 37 с.
2. Гайдур Г.І., Кременецька Я.А., Морозова С.В. Фізичні поля як носії інформації: навчальний посібник. – К.: ДУТ, 2019. – 170 с.
3. Дмитриченко М.Ф., Гололобов Ю.П., Зачек І.Р., Габа В.М., Мороз І.Є. Фізика і транспорт: навчальний посібник. – Львів: Українська академія друкарства, 2014. – 328 с.
4. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навчальний посібник. – К.: ІСЗІ НТУУ «КПІ», 2016. – 104 с.
5. Ластівка Г.І., Шпатар П.М. Технічний захист інформації в інформаційних та телекомунікаційних системах: навчальний посібник. – Чернівці: Чернівецький національний університет, 2018. – 252 с.
6. Луценко В.М., Прогонов Д.О. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спец. 125 «Кібербезпека». – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.
7. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Видавництво Національної академії внутрішніх справ, 2012. – 104 с.

2. ДИСЦИПЛІНА «ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ ТА ЗАХИСТ ІНФОРМАЦІЇ»

1. Концепція електронного документообігу як навчальна дисципліна.

Дисципліна «Електронний документообіг та захист інформації»: об’єкт, предмет, мета, структура). Базові поняття дисципліни (документознавство, інформаційна діяльність, документ, інформація). Зв'язок курсу з іншими дисциплінами документознавчого циклу. Значення курсу в підготовці документознавців.

2. Класифікація документів. Діловодство.

Класифікація документів за ознаками: за змістом, за походженням, за терміновістю, за доступністю, за формою, за терміном зберігання, за характером інформаційних зв’язків, за типом носіїв, за назвою.

Документ як базове поняття документознавства. Міжнародне та вітчизняне визначення поняття «документ» у стандартах. Специфіка структури документа. Поняття «реквізит», «формуляр документа». Текст (гіпертекст − в електронних документах) як головна ознака документа. Поняття методу і способу документування.

3. Нормативно-законодавча база України в сфері запровадження електронного документообігу.

Діловодство: основні поняття, задачі, складові частини і види. Адміністративне і соціальне діловодство. Законодавче регулювання діловодства за кордоном та в Україні. Стандарти, закони та інструкції.

4. Електронний офіс та його основні функції

Етапи розвитку концепції електронного офісу. Основні функціїї електронного офісу. Основні види інформаційних обмінів в організації. Організація роботи з документами. Типова схема підприємства. Інформаційна модель організації

5. Поняття електронного документа та електронного документообігу

Обов’язкові ознаки документа. Статус електронного документа. Система автоматизації документообігу (система електронного документообігу)

6. Мета впровадження та функціонування системи електронного документообігу в органах державної влади.

Робота в середовищі сучасних систем електронного документообігу Інформаційний ринок як сфера інформаційної діяльності документознавця. Загальна характеристика, суб’єкти інформаційного ринку.

7. Критерії для впровадження електронного документообігу в організації.

За типом організації. Масштаби організації. Річний обсяг документообігу на підприємстві. Стиль управління і корпоративна культура організації. Проблеми, що виникають при впровадженні систем електронного документообігу.

8. Поняття та визначення кваліфікованого електронного підпису

Визначення основних понять Статті 1 Закону України «Про електронний цифровий підпис»: електронний підпис, електронний цифровий підпис, кваліфікований електронний підпис, засіб кваліфікованого електронного

підпису, особистий ключ, відкритий ключ , засвідчення чинності відкритого ключа, сертифікат відкритого ключа, посилений сертифікат відкритого ключа, акредитація, компрометація особистого ключа, блокування сертифіката ключа, підписувач, послуги кваліфікованого електронного підпису, надійний засіб кваліфікованого електронного підпису.

Власноручний підпис та кваліфікований електронний підпис

9. Захищеність та правовий статус кваліфікованого електронного підпису.

Електронна печатка. Використання кваліфікованого електронного підпису. Відмінності накладання кваліфікованого електронного підпису на електронний документ від підписання документа на папері.

10. Сертифікат відкритого ключа.

Суб'єкти інфраструктури відкритого ключа. Центр сертифікації ключів та акредитований центр сертифікації ключів.

11. Мета і головні завдання інтегрованої системи електронного документообігу.

Основні властивості інтегрованої системи електронного документообігу та очікувані результати від її впровадження. Вимоги до сучасних систем електронного документообігу. АСКОД.

12. Захист інформації

Основні властивості інформації. Основні визначення та поняття інформаційної безпеки. Державні органи забезпечення інформаційної безпеки. Сутність захисту інформації. Мета захисту інформації в системах е-урядування. Завдання у сфері захисту інформації.

13. Поняття та види загроз інформаційній безпеці.

Чинники, що актуалізують загрозу кібербезпеці. Класифікація загроз інформаційній безпеці. Стандарти інформаційної безпеки («Європейські критерії»). Канали витоку інформації. Програмно-технічний рівень протидії загрозам інформаційній безпеці.

Запитання першого рівня складності

1. Високотехнологічний підхід до керування документаційними процесами в органах державної влади
2. Визначення поняття «документознавство»
3. Визначення поняття «діловодство»
4. Поняття «реквізит»
5. Поняття «формуляр документа»
6. Поняття «гіпертекст»
7. Яким нормативним документом регулюється документообіг?
8. Автор електронного документа
9. Суб'єкти електронного документообігу
10. На що спрямоване державне регулювання у сфері електронного документообігу
11. Ким визначається порядок електронного документообігу?

12. Якщо автор і адресат у письмовій формі попередньо не домовилися про дату і час, то датою і часом відправлення е-документа вважаються
13. Чим підтверджуються факт одержання документа?
14. У разі ненадходження до автора підтвердження про факт одержання е-документа, то вважається, що е- документ ?
15. Чим перевіряється цілісність електронного документа?
16. Інформаційний ринок
17. Інформаційна модель організації
18. Засіб кваліфікованого електронного підпису
19. Особистий електронний ключ
20. Відкритий електронний ключ
21. Компрометація особистого ключа
22. Блокування сертифіката ключа
23. Послуги кваліфікованого електронного підпису
24. Електронна печатка
25. Електронна позначка часу
26. Центр сертифікації ключів
27. Акредитований центр сертифікації ключів
28. Базові властивості інформації
29. Канали витоку інформації
30. Державні органи забезпечення інформаційної безпеки

Запитання другого рівня складності

1. Класифікація документів. Діловодство
2. Нормативно-законодавча база Уряїни в сфері запровадження електронного документообігу.
3. Електронний офіс та його основні функції
4. Основні види інформаційних обмінів в організації
5. Організація роботи з документами
6. Типова схема підприємства.
7. Інформаційна модель організації
8. Обов’язкові реквізити електронного документа.
9. Статус електронного документа
10. Система автоматизації документообігу (система електронного документообігу)
11. Мета впровадження електронного документообігу
12. Критерії для впровадження електронного документообігу в організації
13. Поняття та визначення кваліфікованого електронного підпису
14. Поняття та визначення електронної печатки
15. Поняття та визначення електронної позначки часу
16. Сертифікат відкритого ключа.
17. Суб’єкти інфраструктури відкритого ключа
18. Мета і головні завдання інтегрованої системи електронного документообігу

19. Основні властивості інтегрованої системи електронного документообігу
20. Очікувані результати від впровадження інтегрованої системи електронного документообігу
21. Основні визначення та поняття інформаційної безпеки
22. Сутність захисту інформації.
23. Завдання у сфері захисту інформації е-урядування
24. Поняття та види загроз інформаційній безпеці у е-урядуванні
25. Стандарти інформаційної безпеки («Європейські критерії»)
26. Канали витоку інформації
27. Програмно-технічний рівень протидії загрозам інформаційній безпеці
28. СЕДО АСКОД. Призначення.
29. Класифікація загроз інформаційній безпеці
30. Чинники, що актуалізують загрозу кібербезпеці

Список рекомендованої літератури

1. Гайдур Г.І., Кременецька Я.А., Морозова С.В. Фізичні поля як носії інформації: навчальний посібник. – К.: ДУТ, 2019. – 170 с.
2. Гречко А.В. Основи електронного документообігу: навчальний посібник. – К.: КНТЕУ, 2006. – 156 с.
3. Кукарін О.Б. Електронний документообіг та захист інформації: навчальний посібник. – К.: НАДУ, 2015. – 84 с.
4. Матвієнко О.В., Цивін М.Н. Основи організації електронного документообігу: навчальний посібник. – К.: Центр учбової літератури, 2008. – 112 с.
5. Сагдеев К.М., Петренко В.И., Чипига А.Ф. Физические основы защиты информации: учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 394 с.
6. Семенченко А.І., Дрешпак В.М., Хошаба О.М. Електронне урядування та електронна демократія: навчальний посібник у 15 ч. Частина 13: Захист інформації в системах електронного урядування. – К.: ФОП Москаленко О.М., 2017. – 72 с.
7. Хорошко В.О., Криворучко О.В., Браіловський М.М., Козюра В.Д., Десятко А.М. Захист систем електронних комунікацій: навчальний посібник. – К.: КНТЕУ, 2019. – 164 с.
8. Палеха Ю. І. Загальне діловодство: теорія та практика керування документацією із загальних питань:Навчальний посібник – вид. 4-те (виправлене і доповнене) - К. :Видавництво Ліра-К – 2014. - 624 с. – (Серія посібників з культури діловодства). Доступ до електронного ресурсу:

Інформаційні ресурси

1. Електронний ресурс Державного університету телекомунікацій: https://dut.edu.ua/uploads/l_1582_99961501.pdf

3. ДИСЦИПЛІНА «ОСНОВИ КРИПТОЛОГІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

1. Базові поняття криптографії.

Основні поняття та визначення. Наука про шифрування. Роль криптології у захисті даних.

2. Історія кодування та шифрування.

Історія криптології. Основні поняття криптології та теорії секретних систем. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та ін. Багатоалфавітні системи шифрування: Енігма, Бьюфорта, Віженера. Їх роль у сучасній криптографії.

3. Шифри простої та складної заміни.

Основи шифрування. Шифри однозначної заміни. Шифр Цезаря. Атбаш. Лозунговий шифр. Полібіанський квадрат. Тюремний шифр. Шифрувальна система Трисемуса. Шифр масонів. Криптоаналіз шифрів однозначної заміни.

4. Поліграмні шифри.

Біграмний шифр Порти. Шифр Playfair. Шифр Хілла. Криптоаналіз поліграмних шифрів.

5. Омофонічні шифри.

Система омофонів. Книжкові шифри. Варіантні шифри. Криптоаналіз омофонічних шифрів.

6. Поліалфавітні шифри.

Диск Альберті. Таблиця Трисемуса. Система шифрування Віженера. Роторні машини. Принцип дії роторної машини «Енігма». Шифри Тіні. Криптоаналіз поліалфавітних шифрів.

7. Нерегулярні шифри.

Принцип дії нерегулярних шифрів. Суміщені шифри. Криптоаналіз шифрів нерегулярної заміни.

8. Прості шифри перестановки. Криптоаналіз шифрів перестановки.

Компоненти криптосистеми та їх функціональні характеристики. Перестановка та підстановка. Прості шифри. Криптоаналітичні атаки та метод підрахунку частот для моно та багатоалфавітних криптосистем.

9. Шифри одинарної перестановки.

Шифри простої одинарної перестановки. Шифр блокової одинарної перестановки. Шифри маршрутної та табличної маршрутної перестановки. Шифр вертикальної перестановки. Шифр перехрестя. Шифр з використанням трикутників і трапецій. Шифри на основі гратів і таблиць. Магічні квадрати.

10. Шифри множинної перестановки.

Основи шифрування. Шифри подвійної перестановки. Криптоаналіз шифрів множинної перестановки.

11. Шифри гамування.

Основи шифрування. Генерація гами. Шифрування з використанням синхронних та самосинхронізованих потокових шифрів.

12. Квантове шифрування.

Основні поняття квантової фізики. Основи квантового шифрування. Шифрування на основі лінійних поляризаторів на приймаючій стороні. Шифрування з використанням поляризаційної роздільної призми на приймаючій стороні.

13. Використання кодів.

Прапорові коди та семафорна азбука. Телеграфна азбука. SMS-повідомлення.

14. Симетричні алгоритми.

Блочні та поточні шифри. Принципи побудови, функціонування та криптоаналізу симетричних блокових алгоритмів шифрування DES (Digital Encryption Standard), ГОСТ 28147-89, AES.

15. Розподіл ключів.

Криптографія з відкритим ключем та цифрові конверти. Використання довіреної третьої сторони. Алгоритм RSA. Алгоритм на основі задачі про укладку ранця. Алгоритм Діффі (DH). Алгоритм еліптичних кривих. Порівняння алгоритмів. Ймовірнісне шифрування. Алгоритм шифрування Ель-Гамаля.

16. Цифровий підпис.

Алгоритми цифрового підпису. Порівняння алгоритмів.

17. Нормативно-правове регулювання у галузі КЗІ.

Державне регулювання господарських відносин у сфері криптографічного захисту інформації в Україні. Правове регулювання ЕЦП в Україні та світі. Державний контроль та право суспільства на криптографію. Міжнародні стандарти в сфері КЗІ. Стандартизація в сфері КЗІ в Україні.

18. Основні напрямки розвитку сучасної криптографії.

Шифрування на еліптичних кривих. Методи диференціального криптоаналізу. Квантова криптографія.

Орієнтовні питання для фахового випускного випробування

Питання першого рівня складності

1. Що розуміють під поняттям “криптологія”?
2. Що являли собою перші методи шифрування перестановки та заміни?
3. Як охарактеризувати одноалфавітні системи шифрування Віженера, Плейфера, тощо?
4. Як охарактеризувати багатоалфавітні системи шифрування Енігма, Бьюфорта, Віженера?
5. Яку роль відіграють одно-, та багато алфавітні системи шифрування у сучасній криптографії?
6. Основи шифрування. У чому полягає суть шифрів однозначної простої заміни (цезаря, атбаш, лозунговий, полібіанський квадрат)?
7. Основи шифрування. У чому полягає суть шифрів складної заміни (тюремний шифр, шифрувальна система Трисемуса, шифр масонів)?

8. У чому полягає суть криптоаналізу шифрів однозначної та складної заміни?
9. Що таке поліграмні шифри?
10. У чому полягає суть поліграмних шифрів (біграмний шифр Порти, шифр Playfair, шифр Хілла)?
11. У чому полягає суть криптоаналізу поліграмних шифрів?
12. Що таке омонімічні шифри та система омофонів?
13. У чому полягає суть омонімічних шифрів (книжкові шифри, варіантні шифри)?
14. У чому полягає суть криптоаналізу омонімічних шифрів?
15. Що таке поліалфавітні шифри?
16. У чому полягає суть поліалфавітних шифрів (диск Альберті, таблиця Трисемуса, система шифрування Віженера, шифри Тіні)?
17. Що являють собою роторні машини для шифрування?
18. У чому полягає принцип дії роторної машини «Енігма»?
19. У чому полягає суть криптоаналізу поліалфавітних шифрів?
20. Що являють собою нерегулярні шифри?
21. У чому полягає принцип дії нерегулярних шифрів?
22. Що являють собою суміщені шифри?
23. У чому полягає суть криптоаналізу шифрів нерегулярної заміни?
24. Що являють собою прості шифри перестановки?
25. Що являють собою компоненти криптосистеми та їх функціональні характеристики?
26. У чому полягає процес перестановки та підстановки у простих шифрах?
27. Що слід розуміти під криптоаналітичними атаками та методом підрахунку частот для моно та багатоалфавітних криптосистем?
28. Що являють собою шифри одинарної перестановки?
29. Що являють собою шифри множинної перестановки?
30. Що являють собою шифри гамування?

Питання другого рівня складності

1. Шифри простої та блокової одинарної перестановки... Шифри на основі гратів і таблиць. Магічні квадрати.
2. Шифри маршрутної та табличної маршрутної перестановки.
3. Шифр вертикальної перестановки.
4. Шифр перехрестя.
5. Шифр з використанням трикутників і трапецій.
6. Шифри на основі гратів і таблиць. Магічні квадрати.
7. Шифри множинної (подвійної) перестановки.
8. Криптоаналіз шифрів множинної перестановки.
9. Генерація гами.
10. Шифрування з використанням синхронних та самосинхронізованих потокових шифрів.

11. Використання кодів. Прапорові коди та семафорна азбука.
12. Використання кодів. Телеграфна азбука.
13. Використання кодів. SMS-повідомлення.
14. Симетричні алгоритми. Блочні та поточні шифри.
15. Принципи побудови, функціонування та криптоаналізу симетричних блокових алгоритмів шифрування DES (Digital Encryption Standard), ГОСТ 28147-89, AES.
16. Розподіл ключів. Криптографія з відкритим ключем та цифрові конверти.
17. Використання довіреної третьої сторони. Ймовірнісне шифрування.
18. Алгоритм на основі задачі про укладку ранця.
19. Алгоритм Діффі (DH). Алгоритм еліптичних кривих. Алгоритм RSA. Порівняння алгоритмів.
20. Алгоритм шифрування Ель-Гамаля.
21. Цифровий підпис. Алгоритми цифрового підпису. Порівняння алгоритмів.
22. Державне регулювання господарських відносин у сфері криптографічного захисту інформації в Україні.
23. Правове регулювання електронних цифрових підписів в Україні та світі.
24. Державний контроль та право суспільства на криптографію.
25. Міжнародні стандарти в сфері КЗІ.
26. Стандартизація в сфері КЗІ в Україні.
27. Основні напрямки розвитку сучасної криптографії.
28. Шифрування на еліптичних кривих.
29. Методи диференціального криптоаналізу.
30. Квантова криптографія.

Список рекомендованої літератури

1. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К.: ООО Полиграф-Консалдинг, 2005. – 209 с.

2. Вербіцкий О. В. Вступ до криптології. ВНТА. Львів. 1998. – 247 с.

3. Ємець В.А. Сучасна криптографія. Основні поняття. : навч. посіб. / В. А. Ємець, А.М. Мельник, Р.В. Попович. – Львів: «БАК», 2003. – 144 с.

4. Корнієнко Т.А. Алгоритми та процеси симетричного блокового шифрування. : навч. посіб. / Т. А. Корнієнко, А.М. Мельник, В.М. Мельник. – Львів: «БАК», 2003. – 168 с.

5. Журнал «Захист інформації», м. Київ.

6. https://infocity.kiev.ua – Центр комп'ютерної безпеки, м. Київ.
http://www.naiau.kiev.ua – сайт Національної академії внутрішніх справ.

4. ДИСЦИПЛІНА «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

1. Основні поняття інформаційної безпеки

Поняття інформаційної безпеки. Об'єкт захисту інформації. Основні складові інформаційної безпеки. Управління інформаційною безпекою. Важливість і складність проблеми інформаційної безпеки.

2. Загрози інформаційній безпеці в інформаційних системах

Основні визначення і критерії класифікації загроз. Основні загрози доступності. Основні загрози цілісності. Основні загрози конфіденціальності. Шкідницькі програми.

3. Оціночні стандарти в інформаційній безпеці

Роль стандартів ІБ. «Помаранчева книга» як оціночний стандарт. Міжнародний стандарт ISO/IEC 15408. Критерії оцінки безпеки інформаційних систем.

4. Стандарти управління інформаційною безпекою

BS 77899 та ISO/IEC 17799. Їх основні положення. Міжнародний стандарт ISO/IEC 27001:2005 «Системи управління інформаційною безпекою. Вимоги.». Сертифікація СУІБ на відповідність ISO 27001.

5. Створення СУІБ на підприємстві

Етапи створення системи управління ІБ. Категорування активів компанії. Оцінка захищеності інформаційної системи компанії. Оцінка інформаційних ризиків.

6. Методика оцінки ризиків інформаційної безпеки компанії

Управління ризиками. Основні поняття. Метод оцінки ризиків на основі моделі загроз і вразливостей.

7. Метод оцінки ризиків інформаційної безпеки компанії Digital Security

Метод оцінки ризиків на основі моделі інформаційних потоків. Опис архітектури ІС. Розрахунок ризиків по загрозі конфіденційності.

8. Методики і технології управління ризиками

Якісні методики управління ризиками. Кількісні методики управління ризиками. Метод CRAMM.

9. Розробка корпоративної методики аналізу ризиків

Постановка задачі. Методи оцінювання інформаційних ризиків. Табличні методи оцінки ризиків. Методика аналізу ризиків Microsorf.

10. Сучасні методи і засоби аналізу і управління ризиками інформаційних систем компаній

Обгрунтування необхідності інвестицій в інформаційну безпеку компанії. Методика FRAP. Методика OCTAVE (октейв). Методика RiskWatch (риск ветч).

Тема 11. Правові міри забезпечення інформаційної безпеки.

Основні напрями забезпечення інформаційної безпеки. Законодавчо-правова база забезпечення інформаційної безпеки на підприємстві. Форми правового захисту інформації на підприємстві. Інші документи підприємства, в яких відображаються питання забезпечення інформаційної безпеки.

Тема 12. Організаційні міри забезпечення безпеки комп'ютерних інформаційних систем.

Загальні положення організаційного захисту. Особливості організаційного захисту комп'ютерних інформаційних систем і мереж. Служба безпеки підприємства.

Орієнтовні питання для фахового випускного випробування

Питання першого рівня складності

1. Що розуміють під поняттям інформаційної безпеки?
2. Що являє собою об'єкт захисту інформації?
3. Як охарактеризувати основні складові інформаційної безпеки?
4. Як визначити поняття «управління інформаційною безпекою»?
5. Охарактеризувати важливість і складність проблеми інформаційної безпеки.
6. Які основні визначення і критерії класифікації загроз?
7. Які існують основні загрози доступності?
8. Які існують основні загрози цілісності?
9. Які існують основні загрози конфіденціальності?
10. Які існують шкідницькі програми?
11. У чому полягає роль оціночних стандартів в інформаційній безпеці?
12. Що таке «Помаранчева книга» як оціночний стандарт?
13. Основне призначення Міжнародного стандарту ISO/IEC 15408.
14. Якими є критерії оцінки безпеки інформаційних систем?
15. Що являють собою стандарти управління інформаційною безпекою BS 77899 та ISO/IEC 17799, їх основні положення?
16. У чому полягає суть міжнародного стандарту ISO/IEC 27001:2005 «Системи управління інформаційною безпекою», його вимоги?
17. Що являють собою сертифікація СУІБ на відповідність ISO 27001?
18. Які існують етапи створення системи управління ІБ на підприємстві?
19. У чому полягає суть категорування активів компанії?
20. Що являє собою оцінка захищеності інформаційної системи компанії?
21. У чому полягає оцінка інформаційних ризиків?
22. Що являють собою методики оцінки ризиків інформаційної безпеки компанії?
23. У чому полягає суть управління ризиками, його основні поняття?
24. Що являє собою метод оцінки ризиків на основі моделі загроз і вразливостей?
25. Що являє собою метод оцінки ризиків інформаційної безпеки компанії Digital Security?
26. У чому полягає метод оцінки ризиків на основі моделі інформаційних потоків?
27. Що слід розуміти під описом архітектури ІС?
28. Що являє собою розрахунок ризиків по загрозі конфіденційності?

29. Які існують методики і технології управління ризиками?
30. Що являють якісні і кількісні методики управління ризиками?

Питання другого рівня складності

1. Розробка корпоративної методики аналізу ризиків, постановка задачі.
2. Класифікація методів оцінювання інформаційних ризиків.
3. Табличні методи оцінки ризиків.
4. Методика аналізу ризиків Microsorf.
5. Сучасні методи і засоби аналізу і управління ризиками інформаційних систем компаній.
6. Обгрунтування необхідності інвестицій в інформаційну безпеку компанії.
7. Методика FRAP. Методика OCTAVE. Методика RiskWatch (риск ветч).
8. Правові міри забезпечення інформаційної безпеки.
9. Основні напрями забезпечення інформаційної безпеки.
10. Законодавчо-правова база забезпечення інформаційної безпеки на підприємстві.
11. Форми правового захисту інформації на підприємстві.
12. Документи підприємства, в яких відображаються питання забезпечення інформаційної безпеки.
13. Організаційні міри забезпечення безпеки комп'ютерних інформаційних систем.
14. Загальні положення організаційного захисту.
15. Особливості організаційного захисту комп'ютерних інформаційних систем і мереж. Служба безпеки підприємства.
16. Порівняльний аналіз міжнародних стандартів та української нормативної бази в частині управління інцидентами ІБ.
17. Концепція національної безпеки України. Загрози національній безпеці України в інформаційній сфері.
18. Характеристики захищеності інформаційних ресурсів. Модель CIA.
19. Загрози безпеці державних інформаційних ресурсів. Типові уразливості інформаційних та комунікаційних систем, причини їх появи. Класифікація атак на державні ресурси.
20. Поняття та категоризація державних інформаційних ресурсів. Принципи та рівні захисту державних інформаційних ресурсів інформаційно-комунікаційних систем.
21. Комплексні системи захисту інформації. Етапи побудови. Види випробувань та вимоги до проведення випробувань комплексних систем захисту інформації (державних інформаційних ресурсів).
22. Критерії оцінки рівня інформаційної безпеки за національними та міжнародними стандартами. Нормативні документи з оцінювання захищеності інформаційних ресурсів.
23. Системи менеджменту інформаційної безпеки. Аудит систем менеджменту інформаційної безпеки.

24. Стандарти серії 27К. Основні принципи та завдання. Основні положення та структура стандарту ISO/IEC 27001:2005. Додаток А стандарту ISO/IEC 27001:2005. Реалізація вимог стандарту.
25. Класифікація ризиків інформаційної безпеки. Основні методи оцінки та аналізу інформаційних ризиків. Ризик-менеджмент стандарт NIST 800-30 та ISO 27002.
26. Соціотехнічна безпека. Основні алгоритми соціотехнічних атак на державні інформаційні ресурси та рекомендації щодо захисту від них.
27. Основи планування безперервності роботи державних інформаційно-комунікаційних систем відповідно до ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Розробка та тестування плану BCP.
28. Поняття та класифікація інцидентів інформаційної безпеки відповідно до міжнародних стандартів та рекомендацій (ISO 18044:2004, ISO/IEC 27002:2005, MOD, ITU-T E.409 тощо).
29. Система управління інцидентами інформаційної безпеки: фази життєвого циклу відповідно до моделі PDCA. Архітектура та функції типової системи управління інцидентами інформаційної безпеки.
30. Особливості організації та функціонування команд (груп) CERT/CSIRT. Організаційні структури та управлінські механізми. Документаційне забезпечення. Діяльність CERT/CSIRT в органах державної влади.

Список рекомендованої літератури

1. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдін // Підручник. — К. : НАУ, 2011. — 620 с.

2. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. — Житомир : ЖВІ НАУ, 2010. — 280 с.

3. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. — К. : «МК-Пресс», 2005. — 432 с.

4. Ліпкан В.А. Національна безпека України / В.А. Ліпкан // Навчальний посібник. — К. : Кондор, 2008. — 552 с.

5. Охорона державних секретів незалежної України. / В.П. Ворожко, Й.У. Мастяниця, Л.Є. Шиманський, О.В. Олійник — К. : Інститут законодавства Верховної Ради України, 2010. — 128 с.

6. Система охорони державної таємниці як складова національної безпеки України [Ворожко В.П., Шлапаченко В.М., Пашков А.С., Макаренко В.В. та ін.]. — К. : НА СБУ, 2008. — 364 с.

7. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник — К. : Вид-во DIRECTLINE, 2009. — 714 с.

8. Основи інформаційної безпеки / За ред. проф. В.О. Хорошка / В.О Хорошко, В.С. Чередніченко, М.Є. Шелест. — К. : ДУІКТ, 2008. — 186 с.

9. Смірнов О.А. Основи захисту інформації: навчальний посібник / О.А. Смірнов, Л.Г. Віхрова, С.І. Осадчій, Є.В. Мелешко, В.Ю. Ковтун. — Кіровоград : РВЛ КНТУ, 2011. — 322 с.

10. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. — К. : НАУ, 2005. — 336 с.

11. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. — К. : «МК-Пресс», 2005. — 288 с.

12. Новиков О.М. Безпека інформаційно-комунікаційних систем / О.М. Новиков, М.В. Грайворонський // Підручник. — К. : Вид-во BHV, 2009. — 608 с.

13. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування / І.Д. Горбенко, Ю.І. Горбенко. — Х. : Видавництво «Форт», 2012 — 870 с.

14. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія / І.Д. Горбенко, Ю.І. Горбенко. — Х.: Видавництво «Форт», 2010. — 608 с.

15. Математичні основи криптографії: навчальний посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. — Д.: Національний гірничий університет, 2004. — 391 с.

16. Математичні основи криптоаналізу: навчальний посібник / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. — Д.: Національний гірничий університет, 2010. — 465 с.

17. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. — К. : «МК-Пресс», 2006. — 288 с.

18. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. — Одеса : ОНАЗ ім. О.С. Попова, 2009. — 208 с.

19. Пошаговое руководство по созданию CSIRT (Европейское Агентство по Сетевой и Информационной Безопасности (ENISA) в рамках программы WP-2006), 2006. — 86 с.

20. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. — К. : Арий, 2008. — Том 1. Несанкционированное получение информации. — 464 с.

21. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. — К. : Арий, 2008. — Том 2. Информационная безопасность. — 344 с.

22. Telecommunications Networks – Current Status and Future Trends / [O. Korchenko, P. Vorobiyenko, M. Lutskiy, Ye. Vasiliu, S. Gnatyuk et al.]; edited by J.H. Ortiz. — Rijeka : InTech, 2012. — 446 p.

24. Й.С. Завадський, Менеджмент: «Management», 2-е. вид., К.,Українсько-фінський інститут менеджменту і бізнесу, 1998.

25. Г. Я. Гольдштейн, Основы менеджмента: Конспект лекций. Таганрог: ТРТУ, 1997, Издание второе дополненное.

26. А.А. Дмитриев: «ISO/IEC 27001 – путь к информационной безопасности. Особенности внедрения на отечественных предприятиях», «Das Management» №1, 2009, с. 36-39;

27. «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

28. «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общие сведения и словарь» ISO/IEC 27000:2014, ИСО (Международная организация по стандартизации) и МЭК (Междунар. Электротехн. комиссия), 2014, с. 41.

29. В.О. Лебединець, С.М. Коваленко, Н.О. Тахтаулова, «Імплементація циклу Демінга-Шухарта (PDCA) при регламентації процесів системи управління якістю фармацевтичного підприємства», Управління правління, економіка та забезпечення якості в фармації, № 1(21), с. 11-17, 2012.

32. О.О. Цвілій, Безпека інформаційних технологій: сучасний стан стандартів ISO27K системи управління інформаційною безпекою, *Телекомунікаційні та інформаційні технології*., №2, с. 73-79, 2014.

33. А.А. Дмитриев: «ISO/IEC 27001 – путь к информационной безопасности. Особенности внедрения на отечественных предприятиях», «Das Management» №1, 2009, с. 36-39.

34. «Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, p. 34.

35. «Information technology. Security techniques. Information security management systems implementation guidance», ISO/IEC 27003:2017, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2017, p. 45.

36. «IT-Grundschutz Methodology – Community Draft», BSIStandard 200-2, Federal Office for Information Security (BSI), 2017, p.131.

37. «Системи забезпечення інформаційної безпеки. Огляд», Компанія «Валтек», 2018. [Online]. Available: https://valtek.com.ua/ua/system- integration/ security-control-system/ integrated-security systems /information-security-system-review [Accessed: 26- Dec-2018].

38. «Методи захисту системи управління інформаційною безпекою», Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT), ДСТУ ISO/IEC 27001:2015, Національний стандарт України, ДП «УкрНДНЦ», 2016, с. 28.

39. О.І. Гарасимчук, Ю. М. Костів, Оцінка ефективності систем захисту інформації, Вісник КНУ імені Михайла Остроградського. Випуск 2 (67), 2011, с. 16-20.

5. ДИСЦИПЛІНА «ПРОГРАМНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

1. Проблеми теорії захисту інформації у сучасних ІС.

Складність створення систем захисту інформації. Поняття захисту інформації в ІТС та її роботи з організації. Поняття теорії захисту інформації та її періоди розвитку. Особливості теорії захисту інформації. Формальні та неформальні підходи до розгляду питань теорії захисту інформації. Напрямки розвитку теорії захисту інформації.

2. Характеристика загроз безпеки інформації.

Основні поняття, визначення і критерії класифікації загроз безпеки КС. Основні загрози доступності. Поняття випадкових та навмисних загроз. Загроза розкриття і їх протидія. Основні загрози цілісності. Основні загрози конфіденціальності. Шкідницькі програми. Загроза порушення цілісності і їх протидія. Загроза відмови в обслуговуванні.

3. Несанкціонований доступ. Порушники безпеки.

Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності. Напрями повсякденної діяльності в ІТС для підтримки її працездатності. Послуги забезпечення доступності в ІТС. Спосіб несанкціонованого доступу та цілі зловмисника. Поняття комп'ютерного піратства та категорії порушників безпеки. Поняття моделі порушника безпеки.

4. Шляхи забезпечення безпеки інформації.

Концепція захисту інформації. Стратегія та архітектура захисту інформації. Види забезпечення безпеки інформації. Концепція захисту інформації. Стратегія захисту інформації та ієрархічний підхід до забезпечення безпеки інформації. Етапи розробки концепції захисту інформації.

5. Політика безпеки інформації.

Поняття політики захисту інформації. Етапи реалізації систем захисту. Правові та організаційно-адміністративні заходи протидії комп'ютерним злочинам. Інженерно-технічні заходи протидії комп'ютерним злочинам. Комплекс задач при розробці політики безпеки. Правила забезпечення політики безпеки інформації. Перший етап проектування та реалізації системи захисту. Ймовірні загрози у комп'ютерних мережах. Заходи визначення політики безпеки. Другий етап проектування та реалізації системи захисту – реалізація політики безпеки. Третій етап проектування та реалізації системи захисту – підтримка політики безпеки.

6. Моделі політики безпеки.

Дискреційна політика безпеки, переваги та недоліки. Мандатна політика безпеки, переваги та недоліки. Рольова політика безпеки. Політика безпеки – монітор безпеки.

7. Криптографічні методи захисту інформації.

Основні положення та визначення, поняття криптографії. Характеристика алгоритмів шифрування. Що забезпечує використання криптографії. Засоби виявлення несанкціонованих змін у переданих повідомленнях. Поняття

криптографічного захисту. Вимоги до криптографічних систем захисту інформації. Поняття симетричного шифрування. Поняття несиметричного шифрування. Поняття потокових та блокових алгоритмів шифрування. Найпопулярніші алгоритми шифрування та їх характеристики. Особливості симетричних криптоалгоритмів. Особливості несиметричних криптоалгоритмів. Методи захисту інформації у операційних системах. Загальна схема алгоритму шифрування DES. 8. Опис алгоритму шифрування DES. Опис алгоритму операції розгортання ключа у DES. Переваги та недоліки алгоритму шифрування DES. Опис алгоритму шифрування RSA.

8. Методи і засоби захисту інформації в операційних системах.

Засоби захисту інформації. Загальний критерій безпеки системи. Поняття безпеки програмного забезпечення. Контрольно-іспитовий метод аналізу безпеки ПЗ. Логіко-аналітичний метод аналізу безпеки ПЗ. Формальна постановка задачі аналізу безпеки ПЗ за допомогою контрольно-іспитових методів. Схема аналізу безпеки програм контрольно-іспитовими методами. Формальна постановка задачі аналізу безпеки ПЗ за допомогою логіко-аналітичних методів. Схема аналізу безпеки програм логіко-аналітичними методами.

9. Об`єктно-концептуальна модель обчислювальної системи та руйнуюче програмне забезпечення.

Поняття спадкування та включення у об’єктно-орієнтованому аналізі. Поняття нелегітимних відносин руйнуючого программного забезпечення. Основні підкласи, що належать до класу руйнуючого програмного забезпечення.

10. Модель взаємодії об'єктів обчислювальної системи з погляду безпеки.

Означення геш-функції. Означення стійкості за першим та другим прообразом. Означення односторонньої геш-функції. Умови стійкості геш-функція до колізій. Поняття безключової геш-функції. Поняття ключової геш-функції.

Тема 11. Електроний цифровий підпис.

Поняття електронного цифрового підпису. Властивості електронного цифрового підпису. Вимоги до електронного цифрового підпису. Класифікація електронних цифрових підписів. Опис алгоритмів генерації та верифікації ЕЦП. Опис схеми ЕЦП з додаванням та відновленням повідомлення. Поняття симетричної та асиметричної схеми ЕЦП.

Тема 12. Керування ключами.

Використання RSA для цифрового підпису. Поняття керуванням ключами. Мета керування ключами. Основні стани криптографічного ключа у життєвому циклі. Перехідні стани криптографічного ключа у життєвому циклі. Функції керування ключами підтримки життєвого циклу. Етапи та процеси життєвого циклу керування ключами.

Орієнтовні питання для фахового випускного випробування

Питання першого рівня складності

1. Вкажіть у чому складність створення систем захисту інформації.
2. Опишіть поняття захисту інформації в ІТС та її роботи з організації.
3. Опишіть поняття теорії захисту інформації та її періоди розвитку.
4. Наведіть особливості теорії захисту інформації.
5. Вкажіть у чому полягають формальні та неформальні підходи до розгляду питань теорії захисту інформації.
6. Вкажіть, які є напрямки розвитку теорії захисту інформації.
7. Вкажіть, що собою представляє загроза безпеки КС.
8. Вкажіть, які загрози безпеки КС відносять до випадкових.
9. Вкажіть, які загрози безпеки КС відносять до навмисних.
10. Вкажіть, що собою представляє загроза розкриття і їх протидія.
11. Вкажіть, що собою представляє загроза порушення цілісності і їх протидія.
12. Вкажіть, що собою представляє загроза відмови в обслуговуванні.
13. Вкажіть напрями повсякденної діяльності в ІТС для підтримки її працездатності.
14. Вкажіть якими послугами забезпечується доступність в ІТС.
15. Вкажіть, що собою представляє спосіб несанкціонованого доступу та які мети переслідує зловмисник.
16. Вкажіть, що таке комп'ютерне піратство та категорії порушників безпеки.
17. Вкажіть, що визначає модель порушника безпеки.
18. Опишіть концепцію захисту інформації.
19. Опишіть стратегію захисту інформації та ієрархічний підхід до забезпечення безпеки інформації.
20. Опишіть етапи розробки концепції захисту інформації.
21. Вкажіть поняття політики захисту інформації.
22. Охарактеризуйте правові та організаційно-адміністративні заходи протидії комп'ютерним злочинам.
23. Охарактеризуйте інженерно-технічні заходи протидії комп'ютерним злочинам.
24. Вкажіть комплекс задач при розробці політики безпеки.
25. Вкажіть правила забезпечення політики безпеки інформації.
26. Опишіть перший етап проектування та реалізації системи захисту.
27. Вкажіть, які ймовірні загрози виділяють у комп'ютерних мережах.
28. Вкажіть, яким заходам повинна визначатися політика безпеки.
29. Опишіть другий етап проектування та реалізації системи захисту – реалізація політики безпеки.
30. Опишіть третій етап проектування та реалізації системи захисту – підтримка політики безпеки.
31. Опишіть дискреційну політику безпеки.
32. Опишіть переваги та недоліки дискреційної політики безпеки.

33. Опишіть мандатну політику безпеки.
34. Опишіть переваги та недоліки мандатної політики безпеки.
35. Опишіть рольову політику безпеки.
36. Опишіть політику безпеки - монітор безпеки.
37. Вкажіть, що собою представляє криптографія.
38. Вкажіть для забезпечення чого можна використовувати криптографію.
39. Вкажіть, що застосовують для виявлення несанкціонованих змін у переданих повідомленнях.
40. Вкажіть, що собою представляє криптографічний захист.
41. Вкажіть, які вимоги ставляться перед криптографічними системами захисту інформації.
42. Опишіть поняття симетричного шифрування.

Питання другого рівня складності

1. Опишіть поняття несиметричного шифрування.
2. Розкрийте поняття потокових та блокових алгоритмів шифрування.
3. Охарактеризуйте найпопулярніші алгоритми шифрування.
4. Опишіть особливості симетричних криптоалгоритмів.
5. Опишіть особливості несиметричних криптоалгоритмів.
6. Вкажіть, які методи захисту інформації у операційних системах.
7. Зобразіть загальну схему алгоритму шифрування DES.
8. Опишіть алгоритм шифрування DES.
9. Опишіть алгоритм операції розгортання ключа у DES.
10. Вкажіть на переваги та недоліки алгоритму шифрування DES.
11. Опишіть алгоритм шифрування RSA.
12. Наведіть означення спадкування та включення у об’єктно-орієнтованому аналізі.
13. Опишіть поняття нелегітимних відносин руйнуючого программного забезпечення.
14. Опишіть основні підкласи, що відносяться до класу руйнуючого програмного забезпечення.
15. Сформулюйте загальний критерій безпеки системи.
16. Опишіть поняття безпеки програмного забезпечення.
17. Опишіть контрольно-іспитовий метод аналізу безпеки ПЗ.
18. Опишіть логіко-аналітичний метод аналізу безпеки ПЗ.
19. Опишіть формальну постановку задачі аналізу безпеки ПЗ за допомогою контрольно-іспитових методів.
20. Наведіть схему аналізу безпеки програм контрольно-іспитовими методами.
21. Опишіть формальну постановку задачі аналізу безпеки ПЗ за допомогою логіко-аналітичних методів.
22. Наведіть схему аналізу безпеки програм логіко-аналітичними методами.
23. Наведіть означення геш-функції.
24. Дайте означення стійкості за першим та другим прообразом.
25. Дайте означення односторонньої геш-функції.

26. Вкажіть, коли геш-функція стійка до колізій.
27. Вкажіть, що собою представляють безключові геш-функції.
28. Вкажіть, що собою представляють ключові геш-функції.
29. Розкрийте поняття електронного цифрового підпису.
30. Наведіть властивості електронного цифрового підпису.
31. Сформулюйте вимоги до електронного цифрового підпису.
32. Опишіть, як класифікуються електронні цифрові підписи.
33. Опишіть алгоритми генерації та верифікації ЕЦП.
34. Опишіть схеми ЕЦП з додаванням та відновленням повідомлення.
35. Розкрийте поняття симетричної та асиметричної схеми ЕЦП.
36. Вкажіть, як використовується RSA для цифрового підпису.
37. Вкажіть, що розуміють під керуванням ключами.
38. Вкажіть, яка мета керування ключами.
39. Вкажіть основні стани криптографічного ключа у життєвому циклі.
40. Вкажіть перехідні стани криптографічного ключа у життєвому циклі.
41. Вкажіть, якими функціями керування ключами підтримується його життєвий цикл.
42. Вкажіть, які етапи та процеси містить життєвий цикл керування ключами.

Список рекомендованої літератури

1. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. – Львів : Видавництво Львівської політехніки, 2015. –256 с.

2. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.

3. Лагун А. Е. Криптографічні системи та протоколи: нав. посібник / А. Е. Лагун. – Львів : Видавництво Львівської політехніки, 2013. – 96 с.

4. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: Монографія / І.Д. Горбенко, Ю.І. Горбенко. — Х.: Видавництво «Форт», 2010. — 608 с.

5. Математичні основи криптографії: навчальний посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. — Д.: Національний гірничий університет, 2004. — 391 с.

6. Математичні основи криптоаналізу: навчальний посібник / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. — Д.: Національний гірничий університет, 2010. — 465 с.

7. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.

8. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Олександр ГРИЩУК
«29» квітня 2022 р.

КРИТЕРІЇ
оцінювання досягнення результатів навчання
на атестаційному екзамені за освітньо-професійною програмою
«Інформаційна безпека в комп'ютеризованих системах»
першого (бакалаврського) рівня вищої освіти
за спеціальністю 122 «Комп'ютерні науки»
галузі знань 12 «Інформаційні технології»

Структура оцінки атестаційного екзамену

Оцінка ***атестаційного екзамену*** (за шкалою від 0 до 100 балів) складається із суми балів, виставлених атестаційною комісією в результаті перевірки письмової роботи, виконаної студентом під час атестаційного екзамену, за відповіді студента на кожне з 14 запитань білета атестаційного екзамену.

Порядок оцінювання досягнення результатів навчання

Оцінку атестаційного екзамену визначають у такому порядку:

1) виставляють бали за відповіді на кожне запитання білета атестаційного екзамену виходячи із наведених нижче критеріїв оцінювання відповідей;

2) обчислюють оцінку атестаційного екзамену за формулою:

$$O = \sum_{i=1}^{14} Б_i,$$

де $Б_i$ – кількість балів за відповідь на і-е запитання.

Відповіді у чернетці не перевіряють та до уваги не беруть.

Критерії оцінювання відповідей на запитання

Відповідь на кожне запитання першого рівня складності (запитання з 1-го по 10-е, які передбачають вибір студентом відповіді із наведених у білеті 3 варіантів відповіді, із яких тільки один правильний) може бути оцінена у 2 бали (якщо вибрано правильну відповідь) або 0 балів (якщо вибрано неправильну відповідь із запропонованих у білеті варіантів відповіді, або вибрано більше одного варіанта відповіді, або відповідь не надано).

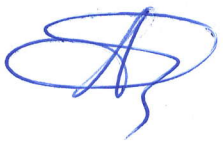
Відповідь на кожне запитання другого рівня складності (запитання з 11-го по 14-е, які передбачають надання студентом розгорнутої теоретичної відповіді) може бути оцінена балами від 0 до 20.

Відповідь на запитання другого рівня складності оцінюють виходячи із наведених у таблиці характеристик відповіді.

Кількість балів	Характеристика відповіді
16–20	Повна, наведена у логічно правильній послідовності відповідь, яка свідчить про всебічні, систематизовані та глибокі знання матеріалу навчальної дисципліни; демонструє здатність студента вільно оперувати здобутими знаннями: диференціювати та інтегрувати їх, відтворювати та аналізувати отриману інформацію, робити обґрунтовані висновки та узагальнення, виявляти й відстоювати власну позицію, переконливо висловлювати думку та чітко формулювати відповідь. Як правило, таку оцінку отримує студент, який відповів на запитання не менше ніж на 90 %. Відповідь оцінюють у 20 балів тільки за умови надання вичерпної відповіді на запитання.
11–15	Досить повна, без суттєвих неточностей, наведена у логічно правильній послідовності відповідь, яка свідчить про ґрунтовні та систематизовані знання матеріалу навчальної дисципліни; демонструє здатність студента впевнено оперувати здобутими знаннями: відтворювати та аналізувати отриману інформацію, пояснювати основні закономірності, робити висновки, чітко висловлювати думку та формулювати відповідь. Як правило, таку оцінку отримує студент, який відповів на запитання на 70–90 %.
6–10	Не зовсім повна, із неточностями та окремими незначними помилками, наведена в основному у правильній послідовності відповідь, яка свідчить про задовільні знання матеріалу навчальної дисципліни, демонструє здатність студента відтворювати основний матеріал навчальної дисципліни відповідно до поставленого запитання. Як правило, таку оцінку отримує студент, який відповів на запитання на 50–70 %.
1–5	Фрагментарна, із суттєвими неточностями та принциповими помилками відповідь, яка свідчить про неповноту знань основного матеріалу навчальної дисципліни, демонструє наявність у студента утруднень при відтворенні інформації відповідно до поставленого запитання. Як правило, таку оцінку отримує студент, який відповів на запитання менше ніж на 50 %.

0	Відповідь не надано або надана відповідь не відповідає поставленому запитанню.

Оцінка атестаційного екзамену від 0 до 59 балів вважається незадовільною.

Завідувач кафедри
інформаційно-аналітичної
діяльності та інформаційної безпеки
д-р техн. наук, професор  Алі АЛЬ-АММОРІ

ДОДАТОК А
ФОРМА БІЛЕТА АТЕСТАЦІЙНОГО ЕКЗАМЕНУ

НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

АТЕСТАЦІЙНИЙ ЕКЗАМЕН

Освітня програма ***«Інформаційна безпека в комп'ютеризованих системах»***

спеціальності ***122 «Комп'ютерні науки»***

Перший (бакалаврський) рівень вищої освіти

ЗАТВЕРДЖУЮ

Проректор
з навчальної роботи

Завідувач
кафедри інформаційно-аналітичної діяльності та інформаційної безпеки

Білет № ___

Запитання І рівня складності

Запитання та варіанти відповідей	**Позначення студентом вибраної відповіді**
1. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
2. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
3. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
4. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
5. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	

6. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
7. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
8. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
9. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	
10. Текст запитання	
а) варіант відповіді	
б) варіант відповіді	
в) варіант відповіді	

Запитання ІІ рівня складності

11. Текст запитання

12. Текст запитання

13. Текст запитання

14. Текст запитання

Розглянуто та схвалено на засіданні кафедри інформаційно-аналітичної діяльності та інформаційної безпеки.

Протокол № 8 від 11 квітня 2022 року.

Розглянуто та схвалено на засіданні Вченої Ради факультету транспортних та інформаційних технологій.

Протокол № 8 від 26 квітня 2022 року.

Розглянуто та схвалено на засіданні Науково-методичної ради Національного транспортного університету.

Протокол № 29 від 29 квітня 2022 року.