Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 1

КРИПТОГРАФІЧНІ ПРОТОКОЛИ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітньо-професійна програма	*Безпека державних інформаційних ресурсів*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна (денна)*
Рік підготовки, семестр	*І рік підготовки, весняний семестр*
Обсяг дисципліни	*4 кредита*
Семестровий контроль/ контрольні заходи	*залік /модульна контрольна робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	Googleclassroom

Київ – 2023

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус вибіркового освітнього компонента циклу професійної підготовки “Криптографічні протоколи” передбачене освітньо-професійною програмою підготовки здобувачів вищої освіти магістр “Безпека державних інформаційних ресурсів” спеціальності 125 – Кібербезпека та захист інформації.

Предмет навчальної дисципліни є застосування криптографічних протоколів для забезпечення послуг інформаційної безпеки.

Метою навчальної дисципліни є посилення та закріплення у курсантів наступних компетентностей: (КЗ1) Здатність застосовувати знання у практичних ситуаціях; (КЗ2) Здатність проводити дослідження на відповідному рівні; (КЗ3) Здатність до абстрактного мислення, аналізу та синтезу; (КЗ5) Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності); (КФ1) Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки; (КФ2) Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки; (КФ3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури; (КФ6) Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (КФ8) Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації; (КФ13) Здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.

Результати навчання, на формування та покращення яких спрямована дисципліна: (РН2) Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; (РН3) Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; (РН6) Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення; (РН13) Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури; (РН20) Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик; (РН22) Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати

достовірність результатів досліджень, аргументувати висновки; (РН26) Проводити аналіз та синтез криптографічних алгоритмів та криптографічних протоколів; розробляти рекомендації впровадження інноваційних проектів, використовуючи базові методи дослідницької діяльності.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішне вирішення завдань навчальної дисципліни базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті вивчення дисципліни “Математичні методи побудови та аналізу симетричних криптосистем”.

Навчальні дисципліни, які забезпечуються цією навчальною дисципліною: виконання магістерської дисертації та військове стажування.

3. Зміст навчальної дисципліни

Семестр 2
Семестровий (кредитний) модуль 1.Криптографічні протоколи.
Розділ 1. Криптографічні протоколи.
Тема 1. Криптографічні ґеш-функції.
Тема 2. Цифровий підпис.
Тема 3. Протоколи автентифікації.
Тема 4. Протоколи управління ключами.
Тема 5. Безпека інформації на прикладному рівні.
Тема 6. Безпека інформації на транспортному рівні.
Тема 7. Безпека інформації на мережному рівні.

4. Навчальні матеріали та ресурси

Основна література:

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Видавництво “Форт”, 2013. – 880 с.

2. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: Монографія. – Харків: Видавництво «Форт», 2015. – 960 с.

3. Лагун А.Е. Криптографічні системи та протоколи: Навчальний посібник – Львів: Видавництво Львівська політехніка, 2013. – 96 с.

4. Тарнавський Ю.А. Технології захисту інформації: підручник: – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

5. Щур Н.О., Покотило О.А. Основи криптології: Навчальний посібник – Житомир: Державний університет Житомирська політехніка, 2021. – 120 с.

Додаткова література:

1. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: Бак, 2003. – 144 с.

2. Корченко В.П. Прикладна криптологія: системи шифрування: підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – Житомир: ДУТ, 2014. – 448 с.

3. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування.

4. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка

5. Behrouz A. Forouzan, Introduction to cryptography and network security — 1st ed. / N.Y. McGraw-Hill, 2008. Vol. 752.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп'ютерний практикум)	СР
Розділ 1. ***Криптографічні протоколи***						
Тема 1	**Криптографічні ґеш-функції**	**23**	**4**	**6**	**0**	**13**
Заняття 1/1	Вступ. 1. Цілі підтримки інформаційної безпеки. 2. Послуги та механізми інформаційної безпеки. 3. Методи реалізації механізмів інформаційної безпеки. Основна література: [1-5].	4	2			2
Заняття 1/2	Цілісність повідомлень. 1. Загальні положення. 2. Криптографічні критерії ґеш-функції. 3. Випадкова модель Oracle. 4. Атаки випадкової моделі Oracle. Основна література: [1-5].	4	2			2
Заняття 1/3	Встановлення дійсності повідомлення. 1. Код виявлення модифікації. 2. Код встановлення дійсності повідомлення. Основна література: [1-5].	5		2		3
Заняття 1/4	Ітеративні ґеш-функції. 1. Ітеративна ґеш-функція. Схема Меркеля-Дамгарда. 2. Підходи до розробки ґеш-функцій. 3. Схеми ґеш-функцій: Рабіна, Девіса-Мейера, Матіса-Мейера-Осеаса, Міагучи-Пренеля. Основна література: [1-5].	5		2		3
Заняття 1/5	Дослідження алгоритму безпечного ґешування SHA-512. 1. Створення дайджест повідомлення SHA-512. 2. Функції розширення слова та стиску в SHA-512. 3. Загальна структура раунду SHA-512. Основна література: [1-5].	5		2		3

Тема 2	**Цифровий підпис**	**22**	**4**	**6**	**0**	**12**
Заняття 2/1	Загальні положення про цифровий підпис. 1. Порівняння звичайного та цифрового підписів. 2. Процес цифрового підпису. 3. Послуги безпеки цифрового підпису. 4. Атаки цифрового підпису. Основна література: [1-5].	4	2			2
Заняття 2/2	Схема цифрового підпису RSA. 1. Загальна ідея цифрового підпису RSA. 2. Підпис RSA дайджесту повідомлення. 3. Атаки на дайджест RSA. Основна література: [1-5].	4	2			2
Заняття 2/3	Дослідження схем цифрових підписів. 1. Цифровий підпис RSA. 2. Цифровий підпис Ель-Гамаля. 3. Цифровий підпис Шнорра. 4. Стандарт цифрового підпису DSS. 5. 0,5 МКР. Основна література: [1-5].	9		4		5
Заняття 2/4	Дослідження схеми цифрового підпису на еліптичних кривих. 1. Загальні положення. 2. Процедура генерації ключів. 3. Процедура підпису та перевірки. 4. ДСТУ 4145-2002. Основна література: [1-5].	5		2		3
Тема 3	**Протоколи автентифікації**	**16**	**4**	**4**	**0**	**8**
Заняття 3/1	Автентифікація об’єкту. 1. Загальні положення. 2. Паролі та атаки на нього. 3. Методи біометрії. Основна література: [1-5].	4	2			2
Заняття 3/2	Автентифікація за допомогою функції “запит-відповід”. 1. Використання шифру з симетричним ключем. 2. Використання функції ключового ґешування. 3. Використання шифру з асиметричним ключем. 4. Використання цифрового підпису. Основна література: [1-5].	4	2			2
Заняття 3/3	Дослідження протоколів з нульовим розголошенням. 1. Протокол Фіата-Шаміра.	8		4		4

	2. Протокол Фейге-Фіата-Шаміра. 3. Протокол Кіскатера-Гілу. Основна література: [1-5].					
Тема 4	**Протоколи управління ключами**	**21**	**4**	**6**	**0**	**11**
Заняття 4/1	Управління ключами з використанням симетричного шифрування. 1. Центр розподілу ключів (KDC). 2. Простий протокол KDC. 3. Протокол Нідхема-Шредера. 4. Протокол Отвея-Ріса. Основна література: [1-5].	4	2			2
Заняття 4/2	Протокол встановлення достовірності Kerberos. 1. Сервери протоколу Kerberos. 2. Дослідження протоколу Kerberos. Основна література: [1-5].	4	2			2
Заняття 4/3	Дослідження методів погодження симетричних ключів. 1. Метод Діффі-Хелмана. 2. Метод “від станції до станції”. Основна література: [1-5].	5		2		3
Заняття 4/4	Управління ключами з використанням асиметричного шифрування. 1. Центр довіри та сертифікації. Сертифікат X.509. 2. Інфраструктура відкритих ключів (PKI). Основна література: [1-5].	8		4		4
Тема 5	**Безпека інформації на прикладному рівні**	**13**	**4**	**2**	**0**	**7**
Заняття 5/1	Протокол PGP. 1. Сценарії протоколу PGP. 2. Кільця ключів. 3. PGP-алгоритми. Основна література: [1-5].	4	2			2
Заняття 5/2	PGP-сертифікати. 1. Довіра та законність. 2. Старт кільця. 3. Таблиці кільця ключів. 4. Модель довіри. Основна література: [1-5].	4	2			2
Заняття 5/3	Розпакування інформації з кілець. 1. Розпакування на боці передавача. 2. Розпакування на боці приймача. Основна література: [1-5].	5		2		3
Тема 6	**Безпека інформації на транспортному рівні**	**9**	**2**	**2**	**0**	**5**

Заняття 6/1	SSL-архітектура. 1. Алгоритми зміни ключів. 2. Алгоритми шифрування та розшифрування. 3. Алгоритми ґешування та стиску. 4. Генерування криптографічних параметрів. Основна література: [1-5].	4	2			2
Заняття 6/2	Протоколи SSL. 1. Протокол встановлення з'єднання. 2.Протокол зміни параметрів шифрування. 3. Аварійний протокол. 4. Протокол передачі записів. 5. 0,5 МКР. Основна література: [1-5].	5		2		3
Тема 7	**Безпека інформації на мережному рівні**	**8**	**4**	**0**	**0**	**4**
Заняття 7/1	Протокол IPSec. 1. Транспортний режим роботи IPSec. 2. Тунельний режим роботи IPSec. Основна література: [1-5].	4	2			2
Заняття 7/2	Протоколи безпеки IPSec. 1. Протокол AH. 2. Протокол ESP. 3. Послуги, які забезпечує IPSec. Основна література: [1-5].	4	2			2
Разом за розділом 1		**112**	**26**	**26**	**0**	**60**
Залік		**8**		**2**		**6**
Всього годин		**120**	**26**	**28**	**0**	**66**

6. Самостійна робота курсанта

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до семестрової залікової контрольної роботи.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
	Розділ 1. Криптографічні протоколи	
1	Тема1. Криптографічні ґеш-функції. 1. Дослідження ітеративної функції криптографічного ґешуванняWhirlpool (Загальна ідея шифру Whirlpool; Структура раунду шифру Whirlpool; Розширення ключа та аналіз шифру Whirpool). 2. Стандарти функції ґешування (ДСТУ ГОСТ 34.311:2009; ДСТУ 7564:2014). Література: основна [1-5], додаткова [1-5].	13
2	Тема 2. Цифровий підпис.	12

	1. Дослідження схеми цифрового підпису на еліптичних кривих (Загальні положення; Процедура генерації ключів; Процедура підпису та перевірки). 2. Стандарти цифрового підпису (ДЕРЖСТ 34.310-95; ДЕРЖСТ 34.310-2001, ДЕРЖСТ 34.310-2012; ДСТУ 4145-2002). Література: основна [1-5], додаткова [1-5].	
3	Тема 3. Протоколи автентифікації. 1. Методи біометрії. 2. Дослідження протоколів з нульовим розголошенням. (Фіата-Шаміра; Фейге-Фіата-Шаміра; Кіскатера-Гілу). Література: основна [1-5], додаткова [1-5].	8
4	Тема 4. Протоколи управління ключами. 1. Дослідження протоколів управління ключами з використанням симетричного шифрування (протоколи Нідхема-Шредера та Отвея-Ріса). 2. Дослідження методів погодження симетричних ключів (протоколи Діффі-Хелмана). 3. Інфраструктура відкритих ключів (PKI). Література: основна [1-5], додаткова [1-5].	11
5	Тема 5. Безпека інформації на прикладному рівні 1. PGP-пакети та повідомлення (PGP-пакети; PGP-повідомлення). 2. Протокол MIME (Структура протоколу MIME; Заголовки MIME). 3. Протокол S/MIME (Синтаксис криптографічного повідомлення; Управління ключами. Криптографічні алгоритми). 4. Захист електронної пошти (Інсталяція PGP, генерація ключів та їх обмін. Дослідження режимів роботи PGP). Література: основна [1-5], додаткова [1-5].	7
6	Тема 6. Безпека інформації на транспортному рівні 1. Формати повідомлення SSL (Повідомлення передачі записів; Повідомлення зміни параметрів шифрування; Аварійне повідомлення; Повідомлення встановлення з'єднання; Прикладні дані). 2. Протокол TLS (Генерація криптографічної секретності; Аварійний протокол; Протокол встановлення з'єднання; Протокол передачі записів). Література: основна [1-5], додаткова [1-5].	5
7	Тема 7. Безпека інформації на мережному рівні 1. Протокол інтернет-обміну ключами IKE (Компоненти протоколу управління ключами в Інтернеті; Удосконалений протокол управління ключами Діффі-Хелмана; Фази та режими IKE). 2. Режими роботи протоколу IKE (Основний режим; Енергійний режим; Швидкий режим; Протокол ISAKMP). Література: основна [1-5], додаткова [1-5].	4
8	Підготовка до заліку	6
Всього годин		**66**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила поведінки та відвідування навчальних занять передбачають: оволодівати теоретичними знаннями і практичними навичками за обраною спеціальністю; дотримуватися графіка навчального процесу та вимог навчального плану; відвідувати навчальні заняття і виконувати у встановлені терміни усі види завдань, передбачені навчальними планами і програмами; у разі хвороби, несення служби в наряді або у виняткових випадках курсант може бути відсутній на заняттях (з подальшим відпрацюванням пропущеного матеріалу).

По прибутті на навчальні заняття курсанти повинні відключати мобільні телефони; входити і виходити з аудиторії тільки з дозволу керівника заняття і тільки у виняткових

випадках; уважно слухати пояснення керівника заняття та відповіді одногрупників; не розмовляти і не займатися сторонніми справами; виконувати всі вказівки керівника навчального заняття, мати на заняттях всі необхідні підручники, зошити, приладдя; підтримувати чистоту і порядок в приміщеннях, дотримуватися морально-етичних правил поведінки і спілкування.

Штрафні та заохочувальні бали.

Сума як штрафних, так і заохочувальних балів не має перевищувати 10 балів:

– за умови гарної підготовки і активної роботи на практичному занятті +1 бал. (одному або двом кращим курсантам на кожному практичному занятті може додаватися як заохочування 1 бал);

– активність на заняттях і систематична робота протягом семестру +1 ... +10;

– участь в олімпіадах, а також ВНО і наукових конференціях, виконання задач з удосконалення методичних і дидактичних матеріалів з дисципліни +1…+10;

– несвоєчасне виконання або невиконання завдання на самопідготовку –1 бал.

– неготовність, пасивність на заняттях і несистематична робота протягом семестру –1…–10.

Дотримання академічної доброчесності курсантами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання. В цьому випадку з курсантів вимагається обов’язково наявність справних відеокамери та мікрофону, які мають бути увімкнені на кожному дистанційному занятті.

Навчальна література освітнього компоненту є відкритою, не містить відомостей з обмеженим доступом і може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Видами контролю якості навчання курсантів є: поточний, календарний та семестровий контроль.

Поточний контроль знань та вмінь курсантів проводиться протягом усіх видів занять. Він реалізується проведенням експрес-контролів, індивідуальним усним або груповим письмовим опитуванням на лекціях та практичних заняттях. В семестрі передбачена модульна контрольна робота. Підсумковий контроль здійснюється у вигляді заліку наприкінці семестру навчання.

Рейтинг курсанта з кредитного модуля складається з балів, що він отримує за:

– виконання 5 експрес-контролів;

– контроль на лекціях та практичних заняттях (дві відповіді);

– виконання модульної контрольної роботи.

Критерії нарахування балів:

Експрес-контролі оцінюються з 10 балів кожна:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації) – 9-10 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 7-9 бали;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 6-7 бали;

– “незадовільно” – відповідь не відповідає вимогам на «задовільно» – 0-5 балів.

Тобто максимум 5 х 10 = 50 балів.

Контроль на лекціях та практичних заняттях (відповіді оцінюються з 10 балів кожна):

– “відмінно” – повна відповідь (не менше 90% потрібної інформації) – 9-10 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 7-9 бали;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 6-7 бали;

– “незадовільно” – відповідь не відповідає вимогам на «задовільно» – 0-5 балів.

Тобто максимум 2 х 10 = 20 балів.

Виконання модульної контрольної роботи оцінюються з 30 балів:

– “відмінно” – повна відповідь (не менше 90% потрібної інформації) – 27-30 балів;

– “добре” – достатньо повна відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 23-26 бали;

– “задовільно” – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 18-22 бали;

– “незадовільно” – відповідь не відповідає вимогам на «задовільно» – 0 балів.

Тобто максимум 30 балів.

$$RD = 50 + 20 + 30 = 100.$$

Залікова контрольна робота оцінюється з 100 балів. Контрольне завдання складається з трьох питань з переліку, що наданий у цьому документі.

Кожне завдання оцінюється: два теоретичних питання – по 30 балів кожне, практичне – 40 балів за такими критеріями:

– “відмінно”, повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд;

– “добре”, достатньо повна відповідь (не менше 75% потрібної інформації, або незначні неточності), що виконана згідно з вимогами до рівня «умінь»;

– “задовільно”, неповна відповідь (не менше 65% потрібної інформації та деякі помилки), що виконана згідно з вимогами до «стереотипного» рівня;

– “достатньо”, неповна відповідь (не менше 60% потрібної інформації та деякі помилки);

– “незадовільно” - незадовільна відповідь – 0 балів.

Календарний контроль: провадиться відповідно до Графіка-календаря освітнього процесу в ІСЗЗІ КПІ ім. Ігоря Сікорськогона навчальний рік як моніторинг поточного стану виконання вимог силабусу. Умовою атестації є отримання не менше 50% від кількості балів, яку курсант може отримати на час проведення атестації.

Умовою допуску до заліку є: виконання усіх видів робіт та завдань, що передбачені робочим навчальним планом на семестр з цього кредитного модуля.

Сума рейтингових балів, отриманих курсантом протягом семестру, переводиться до підсумкової оцінки згідно з таблицею.

Курсант, який у семестрі отримав $\boldsymbol{RD < 60}$ виконує залікову контрольну роботу. У цьому разі сума балів за виконання залікової контрольної роботи переводиться до підсумкової оцінки згідно з таблицею.

Курсант, який у семестрі отримав $RD \geq 60$ балів, може взяти участь у заліковій контрольній роботі з метою підвищення оцінки. У цьому разі бали, отримані ним на заліковій контрольній роботі, є остаточними.

Таблиця переведення рейтингових балів до оцінок

Кількість балів	*Оцінка*
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше 60	Незадовільно

9. Додаткова інформація з дисципліни (освітнього компонента)

Теоретичні питання, які виносяться на залікову контрольну роботу

1. Дайджест повідомлення. Схема перевірки цілісності повідомлення. Критерії криптографічної ґеш-функції.
2. Випадкова модель Oracle.
3. Аналіз (складність) атак випадкової моделі Oracle.
4. Код виявлення модифікації повідомлення (MDC).
5. Код встановлення дійсності повідомлення (MAC).
6. Вкладений MAC (HMAC, CMAC).
7. Ітеративна ґеш-функція. Схема Меркеля-Дамгарда.
8. Схеми ґеш-функцій (Рабіна, Девіса-Мейера, Матіса-Мейера-Осеасе, Міагучи-Пренеля).
9. Алгоритм безпечного ґешування SHA-512 (загальна схема, формат повідомлення).
10. Функції розширення та стиску в SHA-512.
11. Структура раунду в SHA-512.
12. Ітеративна функція ґешуванняWhirlpool (загальна схема, формат повідомлення).
13. Цифровий підпис (порівняння, загальна схема, атаки, підробки).
14. Послуги безпеки цифрового підпису.
15. Цифровий підпис RSA (загальна схема, генерація ключів, підписання та перевірка підпису, атаки).
16. Цифровий підпис RSA дайджесту повідомлення (загальна схема, генерація ключів, підписання та перевірка підпису, атаки).
17. Цифровий підпис Ель-Гамаля (загальна схема, генерація ключів, підписання та перевірка підпису, атаки).
18. Цифровий підпис Шнорра (загальна схема, генерація ключів, підписання та перевірка підпису, атаки).
19. Цифровий підпис DSS (загальна схема, генерація ключів, підписання та перевірка підпису, атаки).
20. Цифровий підпис на еліптичних кривих (загальна схема, генерація ключів, підписання та перевірка підпису).
21. Порівняльний аналіз стандартів цифрового підпису (ДЕРЖСТ 34.310-95, ДЕРЖСТ 34.310-2001, ДЕРЖСТ 34.310-2012, ДСТУ 4145-2002).

22. Автентифікація об’єктів (визначення, відмінності, категорії перевірки).
23. Схеми автентифікації об’єктів з фіксованим паролем.
24. Схеми автентифікації об’єктів з одноразовим паролем.
25. Біометричні методи автентифікації.
26. Використання шифру з симетричним ключем для автентифікації об’єкту за допомогою функції “запит-відповідь”.
27. Використання функції ключового ґешування для автентифікації об’єкту за допомогою функції “запит-відповідь”.
28. Використання шифру з асиметричним ключем для автентифікації об’єкту за допомогою функції “запит-відповідь”.
29. Використання функції цифрового підпису для автентифікації об’єкту за допомогою функції “запит-відповідь”.
30. Протокол автентифікації з нульовим розголошенням Фіата-Шаміра.
31. Протокол автентифікації з нульовим розголошенням Фейге-Фіата-Шаміра.
32. Протокол автентифікації з нульовим розголошенням Кіскатера-Гілу.
33. Центр розподілу ключів (KDC).
34. Простий протокол KDC.
35. Протокол Нідхема-Шредера.
36. Протокол Отвея-Ріїса.
37. Протокол встановлення достовірності Kerberos.
38. Протокол погодження симетричних ключів Діффі-Хелмана.
39. Протокол погодження симетричних ключів «від станції до станції».
40. Методи розподілу відкритих ключів.
41. Сертифікат X.509.
42. Інфраструктура відкритих ключів (структура, режими роботи, моделі довіри).
43. Схема забезпечення автентифікації в протоколі PGP.
44. Схема забезпечення конфіденційності в протоколі PGP.
45. Схема забезпечення автентифікації та конфіденційності в протоколі PGP.
46. Модель довіри в PGP (довіра поручителя, довіра сертифікату, законність ключів).
47. Формат таблиць відкритого та закритого кілець.
48. Процес створення цифрового підпису та шифрування повідомлення в PGP (розпакування кілець передавача).
49. Процес розшифрування повідомлення та автентифікації в PGP (розпакування кілець приймача).
50. Алгоритми зміни ключів протоколу SSL.
51. Набори шифрів протоколу SSL. Сеанси та з’єднання.
52. Алгоритм генерації криптографічних параметрів протоколу SSL.
53. Протокол встановлення з’єднання протоколу SSL.
54. Протокол зміни параметрів шифрування протоколу SSL.
55. Транспортний режим роботи протоколу IPSec.
56. Тунельний режим роботи протоколу IPSec.
57. Протокол AH.
58. Протокол ESP.
59. Послуги забезпечення безпеки трафіку протоколу IPSec (SAD). Алгоритм обробки пакету на боці передавача.
60. Політика безпеки протоколу IPSec (SPD). Алгоритм обробки пакету на боці приймача.
61. Протокол створення ключа OAKLEY протоколу IKE.
62. Фази та режими роботи протоколу IKE. Методи автентифікації сторін.
63. Основний режим роботи протоколу IKE.
64. Енергійний режим роботи протоколу IKE.
65. Швидкий режим роботи протоколу IKE.

Практичні питання, які виносяться на модульну контрольну роботу

1. Для SHA-512 обчислити та представити в шістнадцятирічній формі значення поля довжини вихідного повідомлення, якщо довжина повідомлення становить ……

2. Для SHA-512 обчислити значення довжини поля заповнення, якщо довжина повідомлення становить …

3. Для SHA-512 обчислити та представити в шістнадцятирічній формі результат операції $\text{RotShift}_{x\text{-}y\text{-}z}$ (XXXX).

4. Для SHA-512 обчислити значення мажоритарної або умовної функції в шістнадцятирічній формі (значення буферів додаються).

5. Використовуючи схему цифрового підпису RSA підписати повідомлення та перевірити підпис.

6. Для заданого графа визначити: ключі яких користувачів є законними (незаконними) для користувача А? Пояснити чому?

7. Виконати стиснення або розтиснення повідомлення.

8. Використовуючи метод кодування Radix64 або “обмежений друкований рядок”закодувати повідомлення.