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

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

ТЕХНОЛОГІЇ ОРГАНІЗАЦІЇ ТА ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

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	*5 кредитів*
Семестровий контроль/ контрольні заходи	*Екзамен, модульна контрольна робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	

Київ 2023

Програма навчальної дисципліни

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

Навчальна дисципліна "*Технології організації та захисту державних інформаційних ресурсів*" передбачена освітньо-професійною програмою підготовки здобувачів вищої освіти *Безпека державних інформаційних ресурсів*, *ступеня вищої освіти магістр.* Відноситься до вибіркових освітніх компонентів.

Метою навчальної дисципліни "Технології організації та захисту державних інформаційних ресурсів" є формування у курсантів системи знань в області організації захисту державних інформаційних ресурсів, виявленню та аналізу шкідливого програмного забезпечення та підсилення наступних компетентностей:

КЗ-1	Здатність застосовувати знання у практичних ситуаціях.
КЗ-2	Здатність проводити дослідження на відповідному рівні.
КЗ-5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ11	Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.

Предметом навчальної дисципліни є системи аналізу шкідливого програмного забезпечення.

Виконання програми навчальної дисципліни "Технології організації та захисту державних інформаційних ресурсів" дозволяє підсилити курсантами наступні результати навчання:

РН2	Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому.
РН21	Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН24	Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.

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

Успішне вирішення завдань навчальної дисципліни "Технології організації та захисту державних інформаційних ресурсів" базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті підготовки за ступенем вищої освіти бакалавр, а також навчальної дисципліни "Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах". Навчальна дисципліна забезпечує "Кібернавчання", "Військове стажування", а також виконання магістерської дисертації.

3. Зміст навчальної дисципліни

Семестровий (кредитний) модуль 1. Технології організації та захисту державних інформаційних ресурсів.

Тема 1. Основи організації кібербезпеки держави.

Тема 2. Організація захисту державних інформаційних ресурсів.

Тема 3. Виявлення та аналіз шкідливого програмного забезпечення.

4. Навчальні матеріали та ресурси

Основна література.

1. Peter Bruce, Andrew Bruce, Peter Gedeck. Practical Statistics for Data Scientists. 2nd Ed., O'Reilly Media, 2020, 350 с.

2. Qian Han, Salvador Mandujano, Sebastian Porst, V.S. Subrahmanian, Sai Deep Tetali, and Yanhai Xiong. THE ANDROID MALWARE HANDBOOK. San Francisco, 2024, 332 с.

3. Dylan Barker, Malware Analysis Techniques. BIRMINGHAM-MUMBAI, 281 с.

4. Рекомендації щодо підвищення рівня кібербезпеки для державних органів всіх рівнів, 2023, 85 с.

Додаткова література.

1. Information technology. Security techniques. Information security management. Measurement: ISO/IEC 27004:2009 / International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2009. – 55 с.

2. Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. Handbook for Computer Security Incident Response Teams (CSIRTs) / – Pittsburgh, 2003. – 223 с.

3. Performance Measurement Guide for Information Security: NIST Special Publication 800-55- rev1. / U.S. Government Printing Office. Washington – 2008. – 80 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчальна дисципліна *"Технології організації та захисту державних інформаційних ресурсів"* вивчається курсантами на 1-ому курсі у весняному семестрі.

Видами навчальних занять є лекції, практичні та самостійна робота.

Лекції є початковими заняттями в темах дисципліни. В них формуються головні завдання теми та викладаються основні напрямки їх вирішення, вивчається конкретизований теоретичний матеріал.

На практичних заняттях курсанти закріплюють та поглиблюють знання, отримані на лекціях, з формуванням у них вмінь виконання окремих завдань з кібербезпеки інформаційних ресурсів, набувають практичних навичок моделюванні окремих елементів системи кібербезпеки державних інформаційних ресурсів, а також проводиться виконання практичного завдання.

Самостійна робота курсантів проводиться без керівництва викладача з метою самостійного закріплення та розширення знань.

В процесі вивчення дисципліни проводиться виховна робота з курсантами. В процесі занять виховується наполегливість у переборенні труднощів, уміння самостійно освоювати нові засоби та методи захисту інформації.

Поточний контроль знань та вмінь курсантів реалізується індивідуальним усним або груповим письмовим опитуванням на практичних заняттях та модульною контрольною роботою.

Підсумковий контроль здійснюється у вигляді екзамену.

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу	Кількість годин				
	Всього	у тому числі			
		Лекції	Практ. (семін.)	Лаборант. (комп.пр.)	СРК
Розділ 1. Технології організації та захисту державних інформаційних ресурсів					

Тема 1.	**Основи організації кібербезпеки держави**	**15**	**6**		**4**	**5**
Заняття 1/1	Забезпечення кібербезпеки – проблематики сучасності. 1. Мета дисципліни, РСО. 2. Нормативно-правові засади забезпечення кібербезпеки. 3. Методологія забезпечення кібербезпеки. Основна література: [1-2].	**3**	2			1
Заняття 1/2	Законодавство України у сфері кібербезпеки. 1. Особливості “Стратегії національної безпеки України” у контексті кібербезпеки. 2. Завдання суб’єктів Національної системи кібербезпеки. Основна література: [1-2].	**3**	2			1
Заняття 1/3	Узагальнена модель кіберзахисту. 1. Типова модель функціонування кібернетичної системи, як системи управління. 2. Ознаки та класифікація кіберзагроз. 3. Кібернетичні дії, як специфічний вид протиборства. 4. Базова модель Національної системи кібербезпеки. Основна література: [1-2].	**3**	2			1
Заняття 1/4	Правове регулювання політики безпеки в інформаційному та кібер- просторах України відповідно до міжнародних стандартів. 1. Огляд основних завдань з кібербезпеки країн Євросоюзу. 2. Огляд основних завдань з кібербезпеки США. 3. Огляд основних завдань з кібербезпеки інших країн. 4. Особливості застосування ISO/IEC 27032:2012 “Інформаційні технології. Методи забезпечення безпеки. Настанови по кібербезпеці.” 5. Безпеки Індустріальних Керівних Систем на основні NIST Special Publication 800-82. Основна література: [1-2].	**3**			2	1
Заняття 1/5	Мережева безпека та найпоширеніші типи кібератак. 1. Різновиди атак. 2.Атаки на стек протоколів TCP/IP. 3. Огляд кращих практик побудови безпечної мережевої архітектури. 4. Пристрої мережевої безпеки. Основна література: [1-4].	**3**			2	1
Тема 2.	**Організація захисту державних інформаційних ресурсів**	**30**	**10**	**22**		**16**

Заняття 2/1	Аналіз правового аспекту забезпечення кібербезпеки об’єкту критичної інфраструктури в Україні. 1. Поняття терміну “критична інфраструктура”. 2. Сектори, об'єкти, системи та ресурси, що можуть бути віднесені до критичної інфраструктури. 3. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури 4. Основні загрози критичній інфраструктурі. Основна література: [3-4].	**3**	2			1
Заняття 2/2	Особливості побудови та функціонування об’єкта критичної інформаційної інфраструктури ОКІ. 1. Процес впровадження кібербезпеки. 2. Визначення об’єкта інформаційної інфраструктури ОКІ 3. Побудова мережевої інфраструктури ОКІІ умовного ОКІ. Основна література: [3-4].	**3**		2		1
Заняття 2/3	Розроблення комунікаційних і технологічних систем умовного об’єкту критичної інфраструктури. 1. Архітектура ОКІІ умовного ОКІ. 2. Фізична інфраструктура мережі. 3. Інтегровані рішення щодо організації системи захисту мережі. 4. Розроблення рекомендацій, щодо забезпечення кібербезпеки умовного об’єкту критичної інфраструктури. Основна література: [3-4].	**3**		2		1
Заняття 2/4	Управління інформаційною безпекою. 1. Взаємодія концептів безпеки. 2. Система управління інформаційною безпекою: функції та принципи. 3. Фази планування СУІБ. 4. Види та категорії заходів безпеки (controls). Основна література: [3-4].	**3**	2			1
Заняття 2/5	Управління інформаційною безпекою. 1. Сімейство стандартів ISO 27000. 2. ISACA COBIT: оцінка на основі процесів. 3. Особливості HIPAA та PCI DSS. Основна література: [3-4].	**3**		2		1
Заняття 2/6	Оцінка критичної інформаційної інфраструктури. 1. Визначення критичних активів. 2. NERC CIP Standards. 3. NIST Cybersecurity Framework. Основна література: [3-4].	**3**		2		1

Заняття 2/7	Управління ризиками та оцінка інформаційної безпеки. 1. Загальна концепція управління ризиками інформаційної безпеки. 2. Методи аналізу та управління ризиком. 3. Модель зрілості. Основна література: [3-4].	**3**	2			1
Заняття 2/8	Аудит інформаційної безпеки. Етапи підготовки та проведення. 1. Експертний аудит інформаційної безпеки. 2. Аудит на відповідність стандартам. 3. Інструментальний аналіз захищеності. Основна література: [3-4].	**3**		2		1
Заняття 2/9	Аудит інформаційної безпеки. Етапи завершення та звітності. 1. Розробка плану заходів щодо усунення слабких місць і недоліків у забезпеченні безпеки. 2. Звіт за результатами аудиту. Основна література: [3-4].	**3**		2		1
Заняття 2/10	Збір та обмін інформації про кіберзагрози. 1. Моделі ISAC. 2. Таксономія кіберінцидентів. 3. Обмін даними про кіберінциденти 4. Індикатори компрометації атаки. Основна література: [3-4].	**3**	2			1
Заняття 2/11	Стандарти обміну даними. 1. Structured Threat Information eXpression. 2. MISP. Основна література: [3-4].	**3**		2		1
Заняття 2/12	Типи тестування безпеки. 1. Принципи та ключові елементи тестування безпеки. 2. Етапи тестування безпеки. Основна література: [3-4].	**3**		2		1
Заняття 2/13	Методології та стандарти тестування. 1. Open Source Security Testing Methodology Manual (OSSTMM). 2. OWASP Testing Guide. 3. NIST Special Publication 800-115. 4. Penetration Testing Execution Standard (PTES). 5. Information Systems Security Assessment Framework (ISSAF). 6. PCI DSS Penetration Testing Guide. 7. Penetration Testing. Основна література: [3-4].	**3**	2			1

Заняття 2/14	Тестування безпеки додатків. 1. SAST. 2. DAST. 3. IAST 4. RASP. Основна література: [3-4].	**3**		2		1
Заняття 2/15	Тестування на проникнення. 1. Етапи тестування на проникнення. 2. Типи тестування на проникнення. 3. Інструменти тестування на проникнення. 4. Контрольна робота № 2. Основна література: [3-4].	**3**		2		1
Заняття 2/16	Ландшафт загроз та структура кібератак. 1. Ландшафт загроз. 2. Структура кібератак. 3. Модульна контрольна робота (частина 1). Основна література: [3-4].	**3**		2		1
Тема 3.	**Виявлення та аналіз шкідливого програмного забезпечення**	**57**	**10**	**28**		**19**
Заняття 3/1	Методи і засоби захисту програмного забезпечення. 1. Методи захисту комп'ютерних мереж. 2. Захист мобільного програмного забезпечення. 3. Захист електронної пошти. 4. Принципи створення та використання систем розпізнавання атак та систем розпізнавання вразливостей. Основна література: [1-4].	**3**	2			1
Заняття 3/2	Збір доказів шляхом клонування та перевірка їх застосовності для аналізу. 1. Збір доказів шляхом холодного клонування жорсткого диску. 2. Перевірка отриманих даних. Основна література: [1-4].	**3**		2		1
Заняття 3/3	Збір доказів з працюючої системи та перевірка їх застосовності для аналізу. 1. Збір живих даних з працюючої системи. 2. Перевірка отриманих даних. Основна література: [1-4].	**3**		2		1
Заняття 3/4	Методи та засоби захисту від шкідливого програмного забезпечення. 1. Методи і засоби захисту програмного забезпечення. 2. Типова архітектура системи захисту програмного забезпечення. 3. Критерії оцінки ефективності систем захисту від шкідливого програмного забезпечення. Основна література: [1-4].	**3**	2			1

Заняття 3/5	Основи аналізу артефактів. 1. Налаштування та використання Spamtrap. 2. Підготовка файлів для використання. Основна література: [1-4].	**3**		2		1
Заняття 3/6	Обробка та зберігання артефактів. 1. Будівництво сховища для артефактів. 2. Аналіз отриманих результатів. Основна література: [1-4].	**3**		2		1
Заняття 3/7	Аналіз локальних інцидентів. 1. Збір доказів. 2. Отримання інформації з пам'яті. 3. Отримання образу диска. Основна література: [1-4].	**3**		2		1
Заняття 3/8	Обробка та розслідування інциденту. 1. Реагування та розслідування інциденту на місцевому рівні. 2. Реагування на мережеві інциденти. Основна література: [1-4].	**3**	2			1
Заняття 3/9	Аналіз пам'яті при розслідуванні інцидентів. 1. Перевірка файлу дампу пам'яті. 2. Сканування пам'яті правилами Yara. 3. Аналіз списку процесів. 4. Аналіз мережевих артефактів. 5. Підсумки аналізу пам'яті. Основна література: [1-4].	**3**		2		1
Заняття 3/10	Аналіз дисків при розслідуванні інцидентів. 1. Монтування розділу Windows і створення часової шкали. 2. Антивірусна перевірка. 3. Аналіз файлової системи. 4. Аналіз журналів програми. Основна література: [1-4].	**3**		2		1
Заняття 3/11	Аналіз дисків при розслідуванні інцидентів. 1. Декомпіляція виконуваного файлу Python. 2. Аналіз попередньої вибірки. 3. Аналіз системних журналів. Основна література: [1-4].	**3**		2		1
Заняття 3/12	Методи аналізу змісту спаму. 1. Надсилання спам-повідомлень. 2. Перевірка спаму в базі даних. Основна література: [1-4].	**3**	2			1
Заняття 3/13	Мережевий аналіз інцидентів. 1. Пошук слідів шкідливої активності на робочій станцією Microsoft Windows. 2. Співставлення слідів з попередньою інформацією. 3. Підготовка рекомендації до подальших дії. Основна література: [1-4].	**3**		2		1

Заняття 3/14	Виявлення ознак шахрайської HTTP-сесії. 1. Пошук відмінностей між нормальною та шахрайською HTTP-сесією. 2. Визначення характеристик шахрайського сеансу. Основна література: [1-4].	**3**		2		1
Заняття 3/15	Поглиблений аналіз артефактів. 1. Отримання зображень з пам'яті 2. Пошук та отримання шкідливого програмного забезпечення з образів пам'яті. Основна література: [1-4].	**3**		2		1
Заняття 3/16	Вступ до пакувальників та захисників. 1. Розпакування запакованого зразка UPX. 2.Розпакування UPX за допомогою ESP. 3. Розпакування зразка Dyre. 4. Відстеження дочірніх процесів трояна Tinba. Основна література: [1-4].	**3**	2			1
Заняття 3/17	Поглиблений аналіз артефактів. 1. Базовий аналіз пам'яті Linux. 2. Обхід мережевих екранів. Основна література: [1-4].	**3**		2		1
Заняття 3/18	Поглиблений аналіз артефактів. 1. Отримання зображень з пам'яті. 2. Базовий аналіз образів Windows. Основна література: [1-4].	**3**		2		1
Заняття 3/19	Дослідження перспективних методів та засобів забезпечення захисту державних інформаційних ресурсів. 1. Проактивне виявлення інцидентів. 2. Автоматизація обробки інцидентів. 3. Модульна контрольна робота (частина 2). Основна література: [1-4].	**3**		2		1
Разом за розділом 1		**120**	**26**	**50**	**4**	**40**
Екзамен		30				30
Всього годин		**150**	**26**	**50**	**4**	**70**

6. Самостійна робота здобувачів

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до екзамену.

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
Тема 1. Основи організації кібербезпеки держави.		
1.	Завдання суб'єктів Національної системи кібербезпеки. Базова модель Національної системи кібербезпеки. Огляд основних завдань з кібербезпеки країн США. Огляд основних завдань з кібербезпеки інших країн.	5

	Атаки на стек протоколів TCP/IP. Основна література: [1-4]. Додаткова література: [1-3].	
Тема 2. Організація захисту державних інформаційних ресурсів.		
2.	Побудова мережевої інфраструктури ОКІІ умовного ОКІ. Інтегровані рішення щодо організації системи захисту мережі Фази планування СУІБ. Особливості HIPAA та PCI DSS. Методи аналізу та процес управління ризиком. Structured Threat Information eXpression PCI DSS Penetration Testing Guide Структура кібератак. Основна література: [1-4]. Додаткова література: [1-3].	16
Тема 3. Виявлення та аналіз шкідливого програмного забезпечення.		
3.	Захист електронної пошти. Критерії оцінки ефективності систем захисту від шкідливого програмного забезпечення. Отримання образу диска Реагування на мережеві інциденти. Аналіз мережевих артефактів. Аналіз системних журналів. Співставлення слідів з попередньою інформацією. Визначення характеристик шахрайського сеансу. Відстеження дочірніх процесів трояна Tinba. Базовий аналіз образів Windows. Автоматизація обробки інцидентів. Основна література: [1-4]. Додаткова література: [1-3].	19
4.	Підготовка до екзамену.	30
Всього годин		**70**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає систему вимог, які викладач ставить перед курсантами:

Правила поведінки та відвідування навчальних занять передбачають: оволодівати теоретичними знаннями і практичними навичками за обраною спеціальністю; дотримуватися графіка навчального процесу та вимог індивідуального навчального плану; відвідувати навчальні заняття і виконувати у встановлені терміни усі види завдань, передбачені цим силабусом; у разі хвороби, несення служби в наряді або у виняткових випадках курсант може бути відсутнім

на заняттях (з подальшим відпрацюванням пропущеного матеріалу самостійно або на консультаціях).

По прибутті на навчальні заняття курсанти повинні відключати мобільні телефони; входити і виходити з аудиторії тільки з дозволу керівника заняття; уважно слухати пояснення керівника заняття та відповіді одногрупників; не розмовляти і не займатися сторонніми справами; виконувати всі вказівки керівника навчального заняття; підтримувати чистоту і порядок в приміщеннях, дотримуватися морально-етичних правил поведінки і спілкування.

Дотримання академічної доброчесності здобувачами освіти 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 навчальної 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. При проведення письмових контрольних заходів вимагається верифікація курсанта (фото з документом). Навчальна література навчальної дисципліни зазначена в розділі 4, 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 здобувачів є: поточний, календарний та семестровий контроль.

Оцінювання результатів навчання курсантів здійснюється у відповідності до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського.

Рейтинг з дисципліни складається з двох складових: стартової ($R_c = 60$ – призначена для оцінювання заходів поточного контролю впродовж семестру) та екзаменаційної ($R_e = 40$ – призначена для оцінювання на екзамені).

Рейтинг курсанта з освітнього компонента складається з балів, які він отримує за:

1) 15 виконаних та захищених практичних завдань, кожне з яких оцінюється у 2 бали;

2) модульну контрольну роботу (заняття № 2/16, 3/19), розділена на 2 частини роботи кожна з яких оцінюється максимум в 5 балів;

3) 5 експрес-контролів (заняття № 2/5, 2/8, 2/16, 3/2, 3/5, 3/14), кожне з яких оцінюється у 3 бали;

4) 2 доповіді на семінарі (заняття № 1/4, 1/5), кожна з яких оцінюється у 2 бали;

5) ведення конспекту лекції – 1 бал;

6) штрафні та заохочувальні бали (максимальна кількість рейтингових балів – не більше 6).

Система рейтингових (вагових) балів і критерії оцінювання

1. Виконання практичних завдань

Ваговий бал – 2. Максимальна кількість балів за всі завдання: 2б × 15 = 30 балів:

правильно і повністю виконані всі завдання, захист без запізнень – 2 б.

частково виконані завдання або наявні незначні помилки – 1,5 б.

завдання виконані з помилками або із запізненням – 1 б.

завдання не виконані – 0 б.

2. Модульна контрольна робота

Ваговий бал – 5. Максимальна кількість балів за всі частини модульної контрольної роботи: 5б × 2 = 10 балів.

правильно і повністю виконані всі завдання – 5 б.

частково виконані завдання або наявні незначні помилки – 4 б.

завдання виконані з помилками – 3 б.

завдання не виконані – 0 б.

3. Експрес-контролі.

Ваговий бал – 3. Максимальна кількість балів: 3б × 5 = 15 балів.

правильно і повністю надано відповіді на питання – 3 б.

частково надані відповіді або наявні незначні помилки – 2 б.

відповіді містять помилки – 1 б.

завдання не виконані – 0 б.

4. Доповіді на семінарах.

Ваговий бал – 2. Максимальна кількість балів: 2б × 2 = 4 балів.

доповідач розкриває тему повністю та приймає активну участь в обговоренні теми семінару – 2 б.

доповідач розкриває тему неповністю або не приймає участі в обговоренні теми семінару – 1 б.

доповідь не підготовлена – 0 б.

5. Ведення конспекту лекції

Ваговий бал – 1. Максимальна кількість балів: 1б × 1 = 1 бал.

конспект повний (в т.ч. питання, що виносяться на самопідготовку) – 1.

конспект не повний або відсутній – 0.

6. Штрафні та заохочувальні бали за:

невчасно здані практичні завдання, пасивність на заняттях та несистематична самостійна робота протягом семестру -1… -6.

активність на заняттях та систематична самостійна робота протягом семестру, участь на олімпіадах та наукових конференціях +1…+ 6.

Календарна атестація курсантів проводиться за окремим розпорядженням КПІ ім. Ігоря Сікорського за результатами поточного рейтингу курсанта на час атестації. Якщо значення цього рейтингу не менше 50 % від максимально можливого на час атестації, курсант вважається атестованим.

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів складає R_c = 30+10+15+4+1 = 60 балів. Рейтингова оцінка з кредитного модуля формується як сума балів поточної успішності навчання – стартового рейтингу R_c та екзаменаційних балів R_e. Максимальна сума балів стартового рейтингу R_c складає 60. Необхідною умовою допуску до екзамену є те, що попередня рейтингова оцінка з кредитного модуля має бути не менше $0{,}6 \cdot R_c$ (36 балів), а також здані завдання всіх практичних занять і написані всі контрольні роботи.

Екзаменаційний білет містить 3 завдання: 2 теоретичних і 1 практичне.

Теоретичні питання з екзаменаційного білета оцінюються в 15 балів кожне, відповідно до системи оцінювання:

повна відповідь (не менше 90% потрібної інформації) – 15 балів;

достатньо повна відповідь (не менше 75% потрібної інформації або незначні неточності) – 12-14 балів;

неповна відповідь (не менше 60% потрібної інформації та деякі помилки) – 9-11 балів;

незадовільна відповідь – 0 балів.

Практичне завдання оцінюється у 10 балів:

повне безпомилкове розв'язування завдання – 10 балів;

достатньо повне розв'язування завдання – 8-9 балів;

завдання виконане з певними недоліками – 6-7 балів;

завдання не виконано – 0 балів.

Сума стартових балів та балів за екзаменаційну роботу переводиться до екзаменаційної оцінки згідно з таблицею:

Бали R=$R_c + R_e$	Оцінка
95-100	відмінно
85-94	дуже добре
75-84	добре
65-74	задовільно
60-64	достатньо
Менше 60	незадовільно
$R_c < 36$	не допущено

Заохочувальні та штрафні бали застосовуються вибірково та мають на меті підвищення мотивації курсантів до активної, відповідальної, системної роботи на заняттях протягом семестру.

9. Додаткова інформація з навчальної дисципліни

Питання, що виносяться на екзамен цілком відповідають тим, що були зазначені в змісті дисципліни.

Для практичної реалізації знань і умінь, отриманих під вивчення курсу "Технології організації та захисту державних інформаційних ресурсів" використовується програмним середовищем та системи віртуалізації, що потребує спеціальної ліцензії.

Приклад питань, що виносяться на семестровий контроль (екзамен):

1. Узагальнена модель кібернетичної системи.
2. Державна система захисту критичної інфраструктури.
3. Класифікація та джерела кіберзагроз.
4. Поняття віддаленої атаки на відмову в обслуговуванні, механізм дії, класифікація.
5. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури.
6. Основні загрози критичній інфраструктурі.
7. Фази планування СУІБ.
8. Особливості HIPAA та PCI DSS.
9. Загальна концепція управління ризиками інформаційної безпеки.
10. Типова архітектура системи захисту програмного забезпечення.
11. Реагування та розслідування інциденту на місцевому рівні.
12. Реагування на мережеві інциденти.
13. Створити правило Yara та провести сканування пам’яті.