СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Ступінь освіти	магістр
Галузь знань	12 Інформаційні технології
Тривалість викладання	3, 4 чверть
Заняття:	Весняний семестр
лекції:	2 години
лабораторні заняття:	1 години
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=2063

Кафедра, що викладає: Кафедра безпеки інформації та телекомунікацій

Інформація про викладачів:

Корченко Анна Олександрівна	професор, д.т.н.
Персональна сторінка	http://bit.nmu.org.ua/ua/pro_kaf/prepods/Korchenko.php
E-mail:	**korchenko.a.o@nmu.one**

Тимофєєв Дмитро Сергійович	старший викладач
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/timofeev.php
E-mail:	**tymofieiev.d.s@nmu.one**

1. Анотація до курсу

Аудит ІБ, як правило, використовується для об'єктивної оцінки рівня забезпечення безпеки об’єктів інформаційної діяльності (ОІД). Проведення аудиту слугує для того, щоб виробити ефективні заходи забезпечення ІБ в компаніях, організаціях, установах. За допомогою аудиту ІБ здійснюється збір і аналіз

інформації стосовно ОІД, який перевіряється. Проводиться він з метою кількісної, а також якісної оцінки рівня захищеності ОІД від ймовірних атак з боку зловмисників. Аудит дозволяє також привести раніше створену систему безпеки у відповідність до оновлених вимог, упорядкувати і систематизувати існуючі заходи, спрямовані на забезпечення захисту ОІД.

Саме проведення аудиту може надати об'єктивну оцінку захищеності будь-якого виду підприємства або установи, а також попередити реалізацію потенційних загроз.

2. Мета та завдання курсу

Мета дисципліни – Систематизовано засвоїти сукупність відомостей щодо основних понять, принципів, методів та засобів організації і проведення аудиту інформаційної безпеки, а також оцінки та моніторингу процесів інформаційної безпеки відповідно до вимог найбільш поширених міжнародних стандартів. Навчитись використовувати в практичній діяльності рекомендації щодо впровадження стандартів інформаційної безпеки в установах, організаціях, відомствах.

Завдання курсу:

вивчення дисципліни має прищепити студентам системний підхід до використання методів та засобів проведення аудиту, знання та практичні навички з використання сучасних міжнародних стандартів та програмних рішень, що використовуються в діяльності аудиторів інформаційної та кібербезпеки.

3. Результати навчання

Уміння та навички аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій у сфері інформаційної та кібербезпеки

Уміння та навички обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з аудиту з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та кібербезпеки.

4. Структура курсу

ЛЕКЦІЇ 80 годин

1 Нормативне забезпечення перевірки та оцінки діяльності з управління ІБ

1.1. ДСТУ ISO / IEC 27004 Оцінка функціонування СУІБ

1.2. ДСТУ ISO / IEC 27006-2008 -Вимоги до органів, що здійснюють аудит і сертифікацію СУІБ

1.3. IS0 / IEC 27007 і IS0 /IEC 27008 - Керівництва з аудиту СУІБ і засобів управління ІБ, реалізованих в СУІБ

1.4. ДСТУ ISO/IEC 19011:2012 «Настанови щодо здійснення аудитів систем управління»

2. Процеси перевірки системи управління ІБ

2.1. Види перевірок СУІБ

2.2. Моніторинг ІБ

2.3. Самооцінка ІБ

2.4. Внутрішній аудит ІБ

2.4.1. Цілі і завдання внутрішніх аудитів ІБ

2.4.2. Організаційні принципи внутрішнього аудиту ІБ

2.4.3. Принципи забезпечення ефективності внутрішнього аудиту ІБ

2.4.4. Підрозділ внутрішнього аудиту що контролює питання ІБ в організації

2.5. Зовнішній аудит ІБ

2.5.1. Принципи проведення зовнішнього аудиту ІБ

2.5.2. Управління програмою зовнішнього аудиту ІБ

2.5.3. Етапи проведення зовнішнього аудиту ІБ

2.5.4. Компетентність аудиторів ІБ

2.5.5. Взаємини представників аудиторської групи і організацій, що перевіряються

2.6. Аналіз СУІБ з боку вищого керівництва організації

2.7. Інструментальні засоби перевірки ІБ

3. Оцінка діяльності з управління ІБ

3.1. Оцінка ефективності та результативності діяльності з управління ІБ

3.2. Вимірювання, міра вимірювання, показник і метрика

3.2.1. Метрики безпеки

3.2.2. Вимірювання, пов'язані з ІБ

3.3. Зрілість процесів СУІБ

4 Аудит кібербезпеки об’єктів

4.1 Практика провідних міжнародних організацій у галузі аудита кібербезпеки

4.2.Основні стандарти та рекомендації

ПРАКТИЧНІ ЗАНЯТТЯ 40 годин

1. Дослідження реальних об’єктів інформаційної діяльності
2. Розробка програми аудиту інформаційної безпеки
3. Розробка засобів збору інформації на об’єктах
4. Оцінка ризиків інформаційної безпеки в процесі аудиту

РАЗОМ 120 годин

5. Технічне обладнання та/або програмне забезпечення.

Технічні засоби навчання: мультимедійні та комп’ютерні пристрої.

Програмні засоби дистанційної освіти: MS Office 365, MS Teams, дистанційна платформа Moodle.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 - 89	добре
60 - 73	задовільно
0 - 59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
55	40	30	5	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

55 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

10 балів – Достатня зрозумілість відповіді

7 бали – Добра зрозумілість відповіді

4 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". https://cutt.ly/IBesJEc

.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов’язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об’єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

7.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освіти буде запропоновано анонімно заповнити електронні анкети (Microsoft Forms Office 365), які буде розіслано на ваші університетські поштові скриньки. Заповнення анкет є важливою складовою вашої навчальної активності, що дозволить оцінити

дієвість застосованих методів викладання та врахувати ваші пропозиції стосовно покращення змісту навчальної дисципліни. За участь у анкетуванні здобувач вищої освіти отримує 5 балів.

8 . Рекомендовані джерела інформації

1. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.
2. Аудит інформаційної безпеки: навчальний посібник / автори: Бабенко Т.В., Бігдан А.М., Тимофєєв Д.С., Мирутенко Л.В., Кручінін О.В. – К.: КНУ, 2022. – 310 с.
3. Усач Б. Ф. Організація і методика аудиту: підручник / Б. Ф. Усач, З. О. Душко, М. М. Колос. – К.: Знання, 2006. – 295 с.
4. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
5. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)
6. ДСТУ ISO/IEC 19011:2012 «Настанови щодо здійснення аудитів систем управління».
7. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».
8. ДСТУ ISO/IEC 27006:2008 «Інформаційні технології. Методи і засоби забезпечення безпеки. Вимоги до органів, які забезпечують аудит і сертифікацію систем менеджменту ІБ».
9. NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4.
10. ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
11. Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
12. CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
13. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).