СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Ступінь освіти	магістр
Освітня програма	Кібербезпека
Тривалість викладання	3, 4 чверть
Заняття:	Весняний семестр
лекції:	2 години
лабораторні заняття:	1 година
Мова викладання	українська

Кафедра, що викладає: Кафедра безпеки інформації та телекомунікацій

Викладач:

Тимофєєв Дмитро Сергійович

Старший викладач кафедри безпеки інформації та телекомунікацій

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

Превентивно і реактивно планувати, управляти заходами безпеки професійної діяльності, приймати рішення у складних та непередбачуваних ситуаціях, лідерські якості на посаді керівника.

Співпрацювати в міжнародному контексті та в глобальному інформаційному середовищі за фахом.

Використовувати управлінсько-організаційні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.

Проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.

Використовувати математичні, технічні та правові методи забезпечення інформаційної та кібернетичної безпеки.

4. Структура курсу

ЛЕКЦІЇ

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

1. Дослідження реальних об’єктів інформаційної діяльності
2. Розробка програми аудиту інформаційної безпеки
3. Розробка засобів збору інформації на об’єктах
4. Програмне моделювання процесу управління ризиками інформаційної безпеки в процесі АІБ

5. Система оцінювання та вимоги

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

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно

75-89	добре
60-74	задовільно
0-59	незадовільно

5.2. 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		
66	30	20	4	**100**

Теоретична частина оцінюється за результатами здачі контрольної тестової роботи, яка містить 20 запитань, з яких 17 – прості тести (1 правильна відповідь), 4 задачі.

5.3. Критерії оцінювання підсумкової роботи

24 тестових завдань з чотирма варіантами відповідей, **1** правильна відповідь оцінюється у **2 бали (разом 48 балів)**. Опитування за тестом проводиться з використанням технології Microsoft Forms Office 365.

4 завдання на відповідність наводяться також у системі Microsoft Forms Office 365. Відповідь записується у вигляді пар відповідностей (термін-визначення, робота-етапи, тощо). Правильно розв’язане завдання оцінюється в 3 бали (**разом 12 балів** за 4 завдання), причому:

- **3 бали** – відповідність еталону;
- **2 бали** – одна невідповідність;
- **1 бал** – більше однієї невідповідності, але є правильні відповіді;
- **0 балів –** розв’язання відсутнє або всі відповіді невірні.

Несвоєчасно вислана відповідь враховується такою, що не здана.

5.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує 5 запитань з переліку контрольних запитань. Кількість вірних відповідей визначають кількість отриманих балів. Максимальна кількість балів за захист 4 практичних робіт – **40 балів** = 4 роботи*2 бали*5 питань.

6. Політика курсу

6.1. 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". http://www.nmu.org.ua/ua/content/activity/us_documents/System_of_prevention_and_detection_of_plagiarism.pdf.

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.

6.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

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

6.3. 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).

6.4 Політика щодо оскарження оцінювання

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

6.5. 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.

6.6. Бонуси

Наприкінці вивчення курсу та перед початком сесії здобувача вищої освітим 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 «Основи вітроенергетики». За участь у анкетуванні здобувач вищої освіти отримує **4 бали**.

7. Рекомендовані джерела інформації

Базові

1. Грайворонський М.В.,. Новіков О.М Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
2. 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.
3. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2012. -166 с.: ил. - Серия «Вопросы управления информационной безопасностью. Выпуск 5»

4. Тимофєєв Д.С. Методичні рекомендації до самостійної роботи студентів з дисципліни «Аудит інформаційної безпеки»/ Д.С. Тимофєєв [та ін.]; Нац. гірн. ун-т, каф. безпеки інформації та телекомунікацій. – Д. : НГУ, 2017. – 60 с.
5. Усач Б. Ф. Організація і методика аудиту: підручник / Б. Ф. Усач, З. О. Душко, М. М. Колос. – К.: Знання, 2006. – 295 с.

Додаткові

1. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
2. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT)
3. ДСТУ ISO/IEC 19011:2012 «Настанови щодо здійснення аудитів систем управління».
4. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».
5. ДСТУ ISO/IEC 27006:2008 «Інформаційні технології. Методи і засоби забезпечення безпеки. Вимоги до органів, які забезпечують аудит і сертифікацію систем менеджменту ІБ».
6. 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.
7. 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
8. Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
9. CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
10. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).