СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	Забезпечення безперервності бізнесу
Мова викладання	українська
Викладач (-і)	М.Є. Шелест професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор
Профайл викладача (-ів)	0000-0001-7110-4876
Контакти викладача	mishel3141@gmail.com

1. Анотація курсу -

З розвитком ІТ-можливостей у сучасному світі на перший план виступає автоматизація управління, технологічних, виробничих та інших процесів. Тож інформаційні системи займають провідну роль у бізнес-системі, при цьому взаємозв'язок ІТ та бізнес-процесів настільки щільний, що життєздатність підприємств повністю залежить від надійності технологій, що підтримують найважливіші бізнес-процеси.

Управління безперервністю бізнесу в даний час є одним з найбільш актуальних напрямків, що динамічно розвиваєтсья стратегічного та оперативного управління сучасними підприємствами.

У даному курсі, висвітлюються питанням криптографічного захисту інформації, зокрема:

° Кризи підприємства і завдання антикризового управління. Макрокризи і державне регулювання;

° Технологія антикризового управління;

° Стандарти забезпечення безперервності бізнесу;

° Control Objectives for Information and related Technology.

Змістовий модуль 1. Кризи підприємства і завдання антикризового управління. Макрокризи і державне регулювання.

Тема 1. Антикризове управління підприємства.

Загальні поняття про кризу та кризові явища. Причини виникнення кризи. Симптоми і розпізнавання криз. Мета і завдання антикризового управління. Фази циклу і їх прояв. Макросередовище і державне втручання. Загальне поняття системи і її види. Соціально-економічні системи і середовище. Взаємодія і розвиток соціально-економічних систем. Склад і зміст системи управління. Поняття стійкості і її види. Можливість криз та антикризове управління. Функціональний менеджмент. Антикризовий менеджмент і стійкість фірми. Концептуальна модель безупинного стратегічного планування

Тема 2. Технологія антикризового управління.

Створення антикризової команди (робочої групи) і вироблення дій. Аналіз і прогнозування розвитку кризової ситуації. Система прийняття рішень в умовах кризи. Забезпечення, реалізація антикризових заходів й

аналіз наслідків. Модель менеджера антикризового управління. Дії менеджера в кризовій ситуації. Рольова поведінка менеджера

Змістовий модуль 2. Стандарти забезпечення безперервності бізнесу.

Тема 3. Аналіз стандартів в області BCM.

BS25999. Управління програмою BCM. Моніторинг ефективності програми УББ. Аналіз вимог до програми BCM. Оцінка впливу на бізнес. Оцінка існуючих загроз. Оцінка ресурсів необхідних для BCM. Визначення стратегії BCM.

AS/NZS 5050 (HB 292:2006).

Тема 4. Control Objectives for Information and related Technology.

Ресурси IT у CobiT описані п'ятьма складовими. Критерії оцінки інформації. Показники досягнення результатів.

ISO/IEC 27002:2005. Аспекти управління безперервністю бізнесу. Місто та роль процесу інформаційної безпеки. Безперервність бізнесу та оцінка ризиків. Розробка та впровадження плану безперервності бізнесу (ПББ). Структура ПББ. Підтримка та супровід ПББ.

2. Мета та цілі курсу

Мета дисципліни «Забезпечення безперервності бізнесу» є навчання студентів забезпечувати надійність функціонування бізнес-процесів в умовах впливу негативних чинників кризових ситуацій.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації/

КФ 2. Здатність розробляти, впроваджувати і супроводжувати програмні, програмно-апаратні та технічні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах (автоматизованих систем та їх додатків) та у інфраструктурі організації в цілому.

КФ 4. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

Завданнями вивчення навчальної дисципліни є:

- навчити організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- отримати практичні навички використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності
- сформувати відповідні компетентності щоб аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих

задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

- набути вмінь впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

- отримати відповідні компетентності щоб забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

- ознайомити з принципами використання их програмно-апаратних та технічних комплексів захисту інформаційних ресурсів;

- навчити вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки та задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

- отримати необхідні навички для забезпечення належного функціонування системи моніторингу інформаційних ресурсів і процесів в ІТС;

3. Результати навчання –

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

2 - організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

3 - використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

4 - аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

7- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

8- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі,

сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

9 - використовувати програмні, програмно-апаратні та технічні комплекси захисту інформаційних ресурсів;

10 - вирішувати задачі управління процесами відновлення штатного функціонування ІТС з використанням процедур резервування згідно встановленої політики безпеки;

12 - розробляти, впроваджувати та супроводжувати процеси належного функціонування системи моніторингу інформаційних ресурсів і бізнес процесів в інфраструктурі організації.

У результаті вивчення навчальної дисципліни студент повинен:

Знати:

– сутність та задачі забезпечення безперервності бізнесу;

– основні стратегії, інструкції та порядок дій для мінімізації загроз та зменшення шкоди в умовах впливу негативних чинників кризових ситуацій.

Вміти:

– забезпечувати безпеку працівників та відвідувачів офісних будівель.

– мінімізувати загрози або зменшити шкоду, яку можуть завдати загрози.

– продовжувати головні функцій компанії.

– створювати та впроваджувати документовані плани та інструкції для забезпечення швидкого та ефективного виконання стратегій відновлення.

4. Обсяг курсу. Зазначте загальку кількість кредитів, кількість занять та годин самостійної роботи

Вид заняття	Загальна к-сть годин
лекції	16
практичні	14
самостійна робота (контрольна робота)	60

5. Пререквізити. Вивчення дисципліни «Забезпечення безперервності бізнесу» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів «Вища математика», «Спеціальні глави математики», «Основи програмування», «Основи криптографічного захисту інформації».

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• практичні заняття : 20% семестрової оцінки;

• домашні завдання: 20% семестрової оцінки;

•КР: 20% семестрової оцінки;

• залік: 40% семестрової оцінки.

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки лабораторних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положення про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності балів).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням.

8. Рекомендована література

Базова

1. О.В.Вербіцький. Вступ до криптології. Видавництво НТЛ., Львів, 2008, с.248.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина, - М.: Радио и связь, 2007. -328 с.
3. Баричев С.Г., Серов Р.Е. Основы современной криптографии. – М.: Радио и связь, 2015. – 152 с.
4. Молдовян А.А., Молдовян В.А., Советов В.Я. Криптография. – Серия "Учебники для вузов. Специальная литература". – Спб.: Издательство "Лань", 2006. – 224 с.
5. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
6. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: Корнійчук, 2011. – 152 с.
7. А.О.Антонюк. Основи захисту інформації в автоматизованих системах. – К.: КМ Академія, 2006. – 244 с.
8. А.Ю.Щеглов. Защита компьютерной информации от несанкционированного доступа. НиТ:Санкт-Петербург, 2004.

9. Hoffstein J. An Introduction to Mathematical Cryptography / J. Hoffstein, J. Pipher, J. Silverman. - Springer Science+Business Media, LLC, 2008. – 524 p.
10. Jeffrey H. An Introduction to Mathematical Cryptography / H. Jeffrey, P. Jill, H. Joseph. – Berlin: Springer, 2008. – 540 p.
11. Ян С. Криптоанализ RSA / С. Ян. — Ижевск: РХД. 2011. — 312 с.
12. Srivastava A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem / A. Srivastava, A. Mathur // International Journal of Scientific and Research Publications. – 2013. – Vol. 3 (6). – P. 1-4.
13. Hayder R.H. H-Rabim Cryptosystem / R.H. Hayder // Journal of Mathematics and Statistics. - 2014. – Vol. 10 (3). – P. 304-308.
14. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: ТВП. – 2001. – 254с.

Допоміжна

Домарев В.В.. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. 688 с.
Казарин О.В. Теория и практика защиты программ. М.: МГУЛ, 2003. 450 с.
Фергюсон Нильс, Шнайер Брюс. Практическая криптография / Н.Н. Селина (пер.с англ.). - М.; СПб.; К. : Диалектика, 2015. - 421с.
Харин Юрий Семенович, Берник Василий Иванович, Матвеев Геннадий Васильевич, Агиевич Сергей Валерьевич. Математические и компьютерные основы криптологии : Учеб. пособие для студ. мат. и инж.-техн. спец. вузов - Минск : ООО "Новое знание", 2013. - 382с.

Інформаційні ресурси

Новітні теоретичні та практичні дані та матеріали? що стосуються теорії та практики захисту інформації рекомендується відслідковувати засобом звертання до наступних сайтів.

1. http://www.rsasecurity.com
2. http://www.nist.gov
3. http://www.eprint.iacr.org
4. http://www.citeseer.ist.psu.edu
5. http://www.ansi.org
6. http://www.cryptography.org
7. http://www.iso.org
8. http://www.linuxiso.org
9. http://www.cryptography.com
10. http://www.springerlink.com
11. http://www.cacr.math.uwaterloo.ca
12. http://www.financialcryptography.com
13. http://www.austinlinks.com
14. http://world.std.com/~franl/crypto.html
15. http://www.cryptonessie.org
16. http://www.cryptography.ru

17. http://www.osti.gov/eprints
18. http://www.intel.com
19. http://www.msdn.com
20. http://www.ph4s.ru/book_kripto.html