Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра «Комп'ютерних систем, мереж і кібербезпеки» (№ 503)

**ЗАТВЕРДЖУЮ**

Голова НМК
_____ Д.М. Крицький
(підпис) (ініціали та прізвище)
« 31 » серпня 2021 р.

# СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## Методи та технології кібербезпеки критичних інфраструктур

(назва навчальної дисципліни)

**Галузь знань:** 10 Природничі науки, 11 Математика та статистика, 12 Інформаційні технології, 15 Автоматизація та приладобудування, 16 Хімічна та біоінженерія, 17 Електроніка та телекомунікації, 19 Архітектура та будівництво

**Спеціальність:** 101 Екологія, 103 Науки про Землю, 113 Прикладна математика, 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 123 Комп'ютерна інженерія, 124 Системний аналіз, 125 Кібербезпека, 151 Автоматизація та комп'ютерно-інтегровані технології, 152 Метрологія та інформаційно-вимірювальна техніка, 163 Біомедична інженерія, 172 Телекомунікації та радіотехніка, 173 Авіоніка, 193 Геодезія та землеустрій

**Освітня програма:** усі освітні програми за відповідними спеціальностями

**Рівень вищої освіти**: ***другий (магістерський)***

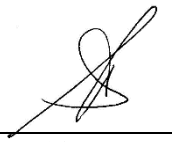
**Силабус введено в дію з 01.09.2021 року**

**Харків – 2021 р.**

Розробник: Брежнєв Є.В., професор, д.т.н., професор 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки (№ 503)

Протокол № 1 від « 30 » серпня 2021 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

Погоджено з представником здобувачів освіти:

_____ _____ _____
(підпис) (ініціали та прізвище)

## 1. Загальна інформація про викладача

Брежнєв Євген Віталійович, д.т.н., професор. З 2017 з року викладає в університеті наступні дисципліни:
Теорія і методи зеленої ІТ-інженерії;
Методи та технології створення критичних ІТ-інфраструктур;
Методи та технології кібербезпеки критичних інфраструктур.

Напрями наукових досліджень: Функціональна та кібербезпека інформаційно-керуючих систем та критичних інфраструктур, Забезпечення якості програмних засобів, Моделювання бізнес процесів, Цифрова трансформація ІТ індустрії

## 2. Опис навчальної дисципліни

**Семестр, в якому викладається дисципліна** – 2 семестр.

**Обсяг дисципліни:**

**4** кредитів ЄКТС (120 годин), у тому числі аудиторних – 48 годин, самостійної роботи здобувачів **–** 73 годин.

**Форми здобуття освіти**

Денна, дистанційна, дуальна.

**Дисципліна** – вибіркова.

**Види навчальної діяльності** – лекції, лабораторні роботи, самостійна робота здобувача.

**Види контролю** – поточний, модульний та підсумковий (семестровий) контроль (іспит).

**Мова викладання** – українська.

**Необхідні обов'язкові попередні дисципліни (пререквізити)** –інженерія програмного забезпечення.

**Необхідні обов'язкові супутні дисципліни (кореквізити)** – технології розроблення та забезпечення функціональної безпеки ІУС; Технології забезпечення кібербезпеки апаратних та програмованих засобів.

## 3. Мета та завдання навчальної дисципліни

**Мета**

Мета вивчення: є отримання магістрами теоретичних знань і навичок з оцінювання ризиків кібербезпеки сучасних КІ та інформаційно-керуючих систем (ІКС), використання інструментальних засобів оцінювання ризиків кібербезпеки.

**Завдання**

Вивчення базових понять теорії ризиків кібербезпеки критичних інфраструктур, а також методів її забезпечення.

Після опанування дисципліни здобувач набуде наступні **компетентності:**

- здатність до усної та письмової комунікації іноземною мовою.
- здатність до участі у проектній діяльності; здатність до адаптації та дії в новій ситуації.
- володіння науковими методами обґрунтування, вибору та аналізу криптографічних механізмів і систем захисту.
- готовність використати сучасні досягнення науки і передових технологій.
- здатність розуміти і аналізувати напрями розвитку розподілених систем і мереж, загальної теорії побудови математичних моделей і їх реалізації, теорії і практики керівництва проектами зі створення захищених розподілених інформаційних ресурсів.
- здатність до самостійної науково-дослідної діяльності (аналіз, співставлення, систематизація, абстрагування, моделювання, перевірка достовірності даних, прийняття рішень та ін.), готовність генерувати та використовувати нові ідеї.
- здатність застосовувати професійно-профільовані знання й практичні навички для розв’язання типових задач зі спеціальності.
- здатність самостійної практичної роботи відповідно до отриманої кваліфікації.

Очікується, що після опанування дисципліни здобувач будуть досягнуті наступні **результати навчання** і він буде:

- вміти проводити пошук інформації в спеціалізований літературі, використовуючи різноманітні ресурси: журнали, бази даних, on-line ресурси.
- вміти використовувати набуті знання за допомогою аналітичного апарату і логічного мислення, уміти застосовувати їх у наукових дослідженнях.
- вміти застосовувати міри ризику, оцінювати та використовувати їх у наукових дослідженнях.
- вміти використовувати здобуті у наукових дослідженнях навички, необхідні для ефективної педагогічної та викладацької діяльності.

- вміти використовувати набуті навички для організації діяльності і спілкування з керівництвом та колегами.

## 4. Зміст навчальної дисципліни

Модуль 1. Вступ до дисципліни.

Тема 1. Критичні інфраструктури. Основні визначення, класифікація, загрози, вразливості. Основні положення "Зеленої книги з захисту критичної інфраструктури". Смарт грид як нова генерація критичної інформаційної інфраструктури. Основні поняття захисту критичної інформаційної інфраструктури. Основні поняття ризик аналізу.

Тема 2. Ризик менеджмент в контексті кібербезпеки. Локальні та емерджентні ризики. Взаємодія між системами в КІ. Основні моделі кіберінцидентів та атак. Ризик аналіз функціональної безпеки інформаційно-керуючих систем в умовах невизначеності.

Тема 3. Кібер резіліенс КІ та кібертероризм. . Основні властивості систем, що забезпечують різіліенс. Основні показники оцінювання. Функція відновлення. Кібертероризм. Методи та інструментальні засоби оцінювання кібербезпеки. Методи оцінювання ризиків та кібербезпеки ІКС.

Практичні завдання.

Семінар. Огляд інструментальних засобів ризик аналізу інформаційної безпеки ІКС та критичної інфраструктури. Практикум. Використання інструментальних засобів для вирішення задач оцінювання кіберризиків.

Модульний контроль.

Модуль 2. Методи та інструментальні засоби оцінювання кібербезпеки ІКС та КІ.

Тема 4. Нечіткі методи оцінювання кібер безпеки. Поняття нечіткої функції, нечіткої змінної. Функції належності. Нечіткі продукційні системи виводу першого роду. Нечіткі продукційні системи виводу другого роду. Лінгвістичне оцінювання кібер безпеки. Нечітка продукційна система Мамдані-Заде. Нечітка продукційна система Такаги-Сугено-Канга.

Тема 5. Методи оцінювання кібер безпеки та резіліенсу з урахуванням взаємовпливу між системами в КІ. Байесовські мережі довіри та їх застосування для задач оцінювання кібербезпеки. Матричні методи

Модульний контроль.

Модуль 3. Методи та засоби забезпечення кібербезпеки КІ та ІКС.

Тема 6. Основні бізнес-процеси забезпечення кібербезпеки в ІТ компанії. Процесно-орієнтовані методи забезпечення кібербезпеки. Нормативно-правова

база України з питань захисту КІ. Аспект кібербезпеки в законодавчій базі України.

Тема 7. Методи забезпечення інформаційної безпеки підприємства. Забезпечення кібербезпеки критичної інфраструктури на прикладі систем критичного застосування (атомна промисловість, банківські системи, тощо). Нормативно-правова база з питань забезпечення кібер безпеки (NIST, IAEA, ISO). Застосування кібердиверсності для забезпечення безпеки КІ.

Модульний контроль.

## 5. Індивідуальні завдання

Не передбачено навчальним планом

## 6. Методи навчання

Словесні, наочні, практичні.

## 7. Методи контролю

Поточний контроль (теоретичне опитування й розв’язання практичних завдань), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

## 8. Критерії оцінювання та розподіл балів, які отримують здобувачі

| Складові навчальної роботи | Бали за одне заняття (завдання) | Кількість занять (завдань) | Сумарна кількість балів |
|---|---|---|---|
| **Змістовний модуль 1** | | | |
| Робота на лекціях | 0…1 | 7 | 0…7 |
| Виконання і захист лабораторних (практичних) робіт | 4..7 | 2 | 8..14 |
| Модульний контроль | 12…14 | 1 | 12…14 |
| **Змістовний модуль 2** | | | |
| Робота на лекціях | 0…1 | 6 | 0…6 |
| Виконання і захист лабораторних (практичних) робіт | 4...7 | 3 | 12...21 |
| Модульний контроль | 14…16 | 1 | 14…16 |
| **Змістовний модуль 3** | | | |
| Робота на лекціях | 0…1 | 6 | 0…6 |
| Виконання і захист лабораторних (практичних) робіт | 4...7 | - | - |
| Модульний контроль | 14…16 | 1 | 14…16 |
| **Усього за семестр** | | | **60…100** |

Контроль знань при проведенні занять оцінюється за такими шкалами:

1) активність на лекції під час відповідей на питання:

– повна відповідь на питання – 2 бали;

– неповна відповідь – 1 бал;

– відсутність на лекції – 0 балів;

2) виконання і захист лабораторних робіт:

– виконані всі завдання лабораторної роботи, оформлені відповідно до вимог, надано вичерпні правильні відповіді на всі запитання – 4 бали;

– виконані всі завдання лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді на всі запитання – 3 бали;

– виконано 75-99% завдань лабораторної роботи, мають місце незначні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 2 бали;

– виконано 50-74% завдань лабораторної роботи, мають місце значні відхилення від оформлення відповідно до вимог, надано правильні відповіді не на всі запитання – 1 бал;

– студент не допущений до захисту роботи (виконано менше 50% її завдань) або робота не захищена – 0 балів.

На модульний контроль (всього 18 балів) виносяться всі пройдені за контрольований період теми, які включаються у варіанти тестових завдань, що містять по 18 питань. Максимальна кількість балів за кожне тестове питання – 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до заліку. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

**Прийнята шкала оцінювання**

| Сума балів за всі види навчальної діяльності | Оцінка для екзамену, *курсового проекту* (роботи), практики |
|---|---|
| 90-100 | відмінно |
| 75-89 | добре |
| 60-74 | задовільно |
| 01-59 | незадовільно з можливістю повторного складання |

**Критерії оцінювання роботи здобувача протягом семестру**

**Задовільно (60 - 74).** Показати необхідний обсяг знань та вмінь для одержання позитивної оцінки. Захистити не менше 80% від усіх завдань лабораторних занять. Вміти самостійно визначати основні елементи захисту критичної інформаційної інфраструктури та її ризик аналізу. Вміти аналізувати аварій (кібер інциденти) в смарт грід.

**Добре (75 - 89).** Твердо знать мінімум знань, виконати не менше 90% завдань лабораторних занять. Вміти визначати основні властивості систем, що забезпечують різіліенс. Вміти формулювати та визначати показники різіліенсу. Застосовувати методи та інструментальні засоби оцінювання кібербезпеки, а також методи оцінювання ризиків та кібербезпеки ІКС. Вміти проектувати бізнес-процеси забезпечення кібербезпеки в компанії.

**Відмінно (90 - 100)**. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати.

## 9. Політика навчального курсу

Відпрацювання пропущених занять відбувається відповідно до розкладу консультацій, за попереднім погодженням з викладачем. Питання, що

стосуються академічної доброчесності, розглядає викладач або за процедурою, визначеною у Положенні про академічну доброчесність.

## 10. Методичне забезпечення та інформаційні ресурси

https://drive.google.com/drive/u/0/folders/1_as3aHZokjrK7h3hnYFd2wR7MCrANkdi

1. The MathWorks. [online]. Fuzzy Logic Toolbox. Available: http://www.mathworks.com/products/fuzzylogic/ [Dec 16, 2005]
2. [Электронный ресурс]: режим доступа ttps://www.cyberriskanalytics.com/
3. [Электронный ресурс]: режим доступа: https://www.riskwatch.com/
4. [Электронный ресурс]: режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html
5. [Электронный ресурс]: режим доступа: http://www.security-risk-analysis.com/introcob.htm
6. [Электронный ресурс]: режим доступа: http://www.amenaza.com/index.php

## 11. Рекомендована література

**Базова**


1. V. Kharchenko, V. Sklyar, E. Brezhniev, 2013, Safety of information and control systems. Models, techniques and technologies – Palmarium Academic Publishing, pp. 528.
2. R. Bloomfield, K. Netkachova, R. Stroud, 2013, “Security-Informed Safety: If It’s Not Secure, It’s Not Safe”, Software Engineering for Resilient Systems Lecture Notes in Computer Science, Volume 8166, Springer Berlin Heidelberg, pp. 17-32.
3. Yastrebenetsky, M., Kharchenko, V., 2014, “Nuclear power plant instrumentation and control systems for safety and security”, IGI Global, pp. 470.
4. M. Yastrebenetsky, V. Kharchenko (Edits), “*Nuclear Power Plant Instrumentation and Control Systems for Safety and Security*”, A volume in the Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series, Hershey, Pennsylvania, United States of America, IGI Global, 2014, 470 p.
5. Huffmire, C. Irvine, T.D. Nguyen, “*Handbook of FPGA Design Security*”, Springer, 2010, 177 p.
6. V. Kharchenko, A. Kovalenko, V. Sklyar, O. Siora, “Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements

Context", Proceedings of the International Conference on Information and Digital Technologies (IDT 2015), Žilina, Slovakia, July 7-9, 2015, pp. 117-123.

7. Momoh, J. A, "Fundamentals of analysis and computation for the Smart Grid," Power and Energy Society General Meeting, 2010 IEEE , vol., no., pp.1-5, 25-29 July 2010.

8. Arnold, G. W, "Challenges and Opportunities in Smart Grid: A Position Article," Proceedings of the IEEE, vol.99, no.6, pp.922-927, June 2011.

9. ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary (IDT).

10. NIST SP800-30 Risk Management Guide for Information Technology Systems Text]. – National Institute of Standards and Technology 2002 – 95 p.

11. Byres, E. J., Franz, M. and Miller, D., "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", International Infrastructure Survivability Workshop (IISW '04), IEEE, Lisbon, Portugal, December 4, 2004.

12. Scambray, J. and McClure, S., "Hacking Exposed Windows 2000: Network Security Secrets and Solutions," McGraw_Hill, 2001.

13. B. Utne, P. Hokstad, G. Kjolle, J. Vatn, I.A. Tendel, D. Bertelsen, H. Fridheim, J. Rustrum, Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS approach.

14. U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Washington, DC, 2013.

15. R. Belohlavek, V. Vychodil, Attribute implications in a fuzzy setting, in: B. Ganter, L. Kwuida (Eds.), Lecture Notes in Artificial Intelligence, vol. 3874, Springer-Verlag, Heidelberg, 2015.

**Допоміжна**

1. Rinaldi, J.Peerenboom Identifying, Understanding, and Analyzing Critical Infrastructure Dependencies /IEEE Control Systems Magazine, Vol. 21 - Dec. 2001 - pp. 11-25.

2. Singer, D. 1990. A fuzzy set approach to fault tree and reliability analysis. FuzzySets and Systems, 34, 2: 145-55.

3. Wayne C. Turner, Steve Doty Energy management handbook, Sixth edition, Fairmont Press, Inc, 2006, 389 p.

4. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1991. Fuzzy variables as a basis for a theory of fuzzy reliability in the possibility context. Fuzzy Sets and Systems, 42, 2: 145-172.

5. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1991. Posbist reliability behavior of typical systems with two types of failures. Fuzzy Sets and Systems, 43, 1:17-32.

6. Cai, K.Y., Wen, C.Y., and Zhang, M.L. 1993. Fuzzy states as a basis for a theory of fuzzy reliability. Microelectronic Reliability, 33, 1: 2253-2263.

7. MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, 24 Nov. 1980.

8. Pederson, P., Dudenhoeffer, D., Hartley, S. & Perman, M. 2006. Critical Infrastructre Interdependency modelling: A survey of U.S and international research. Report prepared by the Idaho National Laboratory.