ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій

28 серпня 2024 р., протокол № 8

Голова Вченої ради

_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА
вибіркової навчальної дисципліни загальної підготовки
«Основи кібербезпеки»

факультет інформаційно-комп'ютерних технологій

для здобувачів вищої освіти освітнього ступеня «бакалавр»

Схвалено на засіданні кафедри інженерії програмного забезпечення

28 серпня 2024 р., протокол № 7

Завідувач кафедри

_____ Тетяна ВАКАЛЮК

Розробник: к.т.н., доцент, доцент кафедри інженерії програмного забезпечення Надія ЛОБАНЧИКОВА

Житомир

2024 – 2025 н.р.

Робоча програма вибіркової навчальної дисципліни загальної підготовки «Основи кібербезпеки» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни	
	денна форма навчання	заочна форма навчання
Кількість кредитів 3	Вибіркова	
Модулів – 1	Лекції	
	16 год.	2 год.
Змістових модулів – 3	Практичні	
	_32__ год.	4 год.
Загальна кількість годин – 90	Лабораторні	
	–	–
Тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи – 2,6	Самостійна робота	
	42 год.	84 год.
	Вид контролю: залік	

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями кібербезпеки та захисту інформації в інформаційно-комунікаційних системах, методологічними та законодавчими основами організації, планування та впровадження систем кібербезпеки та захисту інформації в сучасних бізнес-процесах, а також основним аспектам практичної діяльності по їх створенню, забезпеченню функціонування та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завданнями вивчення навчальної дисципліни є:

– оволодіння принципами побудови систем кіберзахисту;

– розуміння головних задач та сервісів кібербезпеки;

– оволодіння загальними теоретичними поняттями та основними нормативно-правовими документами у сфері кібербезпеки;

– отримання знань щодо основних складових інформаційної безпеки;

– отримання знань щодо існуючих моделей загроз та порушника, основних причин порушення безпеки;

– отримання знань щодо класифікації засобів кібербезпеки, організаційних та технічних заходів забезпечення кіберзахисту;

– оволодіння принципами захисту інформації від несанкціонованого доступу, методами аутентифікації, ідентифікації та авторизації користувачів інформаційно-комунікаційних систем, методами контролю доступу в тому числі безпеки доступу до хмарних ресурсів, основи IAM (Identity and Access Management), служби аутентифікації та керування доступом;

– оволодіння теоретичними основами криптографічних та стеганографічних методів захисту інформації, у тому числі захист даних у застосунку, захист даних під час передачі;

– оволодіння методами та засобами здійснення процедури оцінки ефективності систем кіберзахисту;

– оволодіння технологіями реалізації криптографічних алгоритмів захисту інформації;

– оволодіння методами розробки моделі загроз та моделі порушників інформаційної безпеки;

– оволодіння методами та технологіями моніторингу та реагування на інциденти.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати додатково наступні Soft skills:

- *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;
- *уміння виступати привселюдно*: навички, необхідні для виступів на публіці; навички проведення презентації;
- *керування часом:* уміння справлятися із завданнями вчасно;
- *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;
- *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;
- *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

МОДУЛЬ 1

Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі.

Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.

Дефініція основних понять і визначень у сфері кібербезпеки. Основні нормативно-правові документи із захисту інформації.

Тема 2. Загрози безпеці інформаційних систем

Джерела загроз інформаційній безпеці. Системна класифікація і загальний аналіз загроз безпеці інформації. Модель загроз та порушника і кіберпросторі.

Тема 3. Інциденти у сфері високих технологій

Основні поняття та визначення. Класифікація кібернетичних втручань і загроз. Особливості найпоширеніших кібератак

Змістовий модуль 2. НСД та криптографічні методи захисту інформації

Тема 4. Методи та засоби захисту інформації від НСД

Способи та методи НСД в сучасних ІТС. Основні принципи захисту інформації від НСД. Рівні інформаційно-комунікаційної системи. Несанкціонований доступ на різних рівнях інформаційно-комунікаційної системи. Класичні моделі розмежування доступу. Ідентифікація і аутентифікація користувачів.

Тема 5. Криптографічні методи захисту інформації

Історична довідка. Основні поняття криптографії. Загальна класифікація алгоритмів шифрування. Кваліфікований електронний підпис. Реалізація алгоритмів шифрування. Стеганографія.

Змістовий модуль 3. Захист інформації в розподілених інформаційних системах та організація кібербезпеки

Тема 6. Технології віртуалізації

Ключові терміни. Переваги та недоліки. Типи віртуалізації. Платформи віртуалізації.

Тема 7. Шкідливе програмне забезпечення та захист від нього

Шкідливе програмне забезпечення та захист від нього. Організаційно-технічні заходи забезпечення захисту інформації.

Тема 8. Політика безпеки. Оцінка ефективності систем захисту інформації.

Поняття політики безпеки. Види політик безпеки. Організація секретного діловодства. Підходи до оцінки ефективності систем захисту інформації.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	Усього	Лекції	Практичні	Самостійна робота	Усього	Лекції	Практичні	Самостійна робота
Модуль 1								
Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі								
Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.	5	2		3	5			5
Тема 2. Загрози безпеці інформаційних систем	8	2	2	4	8	0,25	1	6,75
Тема 3. Інциденти у сфері високих технологій	7	2	2	3	7	0,25		6,75
Разом за змістовий модуль 1	20	6	4	10	20	0,5	1	18,5
Змістовий модуль 2. Основи криптографічних методів кіберзахисту								
Тема 4. Методи та засоби захисту інформації від НСД	10	2	4	4	10			10
Тема 5. Криптографічні методи захисту інформації	20	2	10	8	20	0,5	1	18,5
Разом за змістовий модуль 2	30	4	14	12	30	0,5	1	28,5
Змістовий модуль 3. Організація захисту інформації								
Тема 6. Технології віртуалізації	6	2	2	2	6	0,25		5,75
Тема 7. Шкідливе програмне забезпечення та захист від нього	14	2	4	8	14	0,25	1	12,75
Тема 8. Політика безпеки. Оцінка ефективності систем захисту інформації	20	2	8	10	20	0,5	1	18,5
Разом за змістовий модуль 3	40	6	14	20	40	1	2	37
ВСЬОГО	90	16	32	42	90	2	4	84

5. Теми практичних робіт

№ З/П	НАЗВА ТЕМИ	КІЛЬКІСТЬ ГОДИН	
		ДЕННА ФОРМА	ЗАОЧНА ФОРМА
1	Обстеження об’єкту інформаційної діяльності та формування звітної документації.	2	1
2	Складання імовірнісного прогнозу та моделі порушника	2	-
3	Захист інформації від несанкціонованого доступу	2	
4	Захисту інформації за допомогою шифру перестановки та заміни	2	1
5	Програмна реалізація шифру перестановки та заміни	2	-
6	Шифрування текстової інформації із використанням криптографічного шифру гамування	2	-
7	Застосування асиметричних криптосистем для захисту інформації	2	-
8	Шифрування та дешифрування інформації за допомогою криптографічної системи з відкритим ключем RSA	2	-
9	Нанесення цифрових водяних знаків у зображення просторовим методом LSB	2	-
10	Налаштування параметрів безпеки операційної системи Windows 10 із застосуванням програми VirtualBox	2	-
11	Політика безпеки	2	-
12	Програмна реалізація дискреційної політики безпеки організації	2	1
13	Створення систем охорони периметру	2	-
14	Фізичний захист інформації в серверних кімнатах	2	-
15	Технічний захист інформації: кімната переговорів	2	-
16	Визначення міцності захисту інформації	2	1
РАЗОМ		32	4

6. Завдання для самостійної роботи

Виконання самостійної роботи студентів проводиться у вигляді проходження безкоштовних онлайн курсів, що розміщені на сторінці освітньої освітнього порталу. Студент обирає курс з нижчезазначеного переліку, проходить їх самостійно та надсилає викладачу сертифікат про проходження. Студент має право проходженням.

Перелік онлайн курсів:

Cisco: Вступ до кібербезпеки;

Udacity: Introduction to Cybersecurity, Інженер з безпеки;

Skillshare: Кібербезпека: перейдіть від нуля до героя

Coursera: Кібербезпека для всіх, Вступ до спеціалізації з кібербезпеки

Зарахування самостійної роботи відбувається викладачем на підставі отриманого сертифікату від студентів. Отримані результати переводяться в бали, виділені для самостійної роботи та заноситься до рейтингу поточного оцінювання студента.

Критерії переводу балів за результати виконання самостійної роботи з національної шкали в бали ECTS

Відповідність балів національної і кредитно-модульної шкали за виконання самостійної роботи:

Оцінка виконаної студентом самостійної роботи за національною шкалою	Бали ECTS	Оцінка ECTS
5	13,5...15	A
4	12,3...13,4	B
	11,1…12,2	C
3	9,6...11,0	D
	9,0...9,5	E
2	5,3…8,9	F
	<5,1	FX

7. Індивідуальні завдання

Виконання індивідуального завдання (ІЗ) є важливою частиною дисципліни «Основи кібербезпеки» та представляє собою самостійне дослідження студента, який оформив індивідуальний графік навчання, або навчається на заочній формі та є альтернативним варіантом виконання практичних (лабораторних) робіт з дисципліни.

Мета виконання ІЗ є закріплення, узагальнення та поглиблення знань, одержаних студентами під час вивчення дисципліни та їх застосування при самосійній роботі, активізація творчих здібностей студентів, розвиток навичок роботи з нормативно-технічною літературою, прийняття самостійних рішень, набуття практичних навичок роботи щодо захисту інформації програмними та криптографічними засобами.

ІЗ повинно бути результатом самостійних досліджень студента, які:

– сприяють розвитку ініціативності студентів у їх виробничій і дослідницькій діяльності;

– поглиблюють, систематизують та закріплюють теоретичні знання та практичні навички, отримані під час навчання;

– перевіряють уміння студента самостійно освоювати та використовувати сучасні інформаційні технології;

– розвивають у студента навички ведення самостійного науково-практичного пошуку, оволодіння методикою дослідження й експериментування в ході вирішення проблем і питань, поставлених до виконання;

– сприяють набуттю вміння аналізувати отримані результати досліджень, формулювати висновки та положення.

За всі відомості, що викладені в ІЗ, порядок використання в ході підготовки фактичного матеріалу та іншої інформації, пропозиції, технології, обґрунтованість і вірогідність висновків та положень, що захищаються, несе відповідальність безпосередньо автор.

Викладач надає студенту допомогу у виборі теми роботи, проводить консультації з проблемних питань, що виникають у процесі виконання ІЗ, надає допомогу в пошуку методичної та технічної документації, науково-технічної літератури.

8. Методи навчання

На лекційних заняттях: розповідь, пояснення, демонстрація, бесіда, дискусія. На лабораторних роботах: пояснення, дослідження, розв`язування ситуаційних задач, виконання індивідуального варіанту завдання. Самостійна робота студента: реферати, повідомлення, науково-пошукові, дослідницькі проекти, виконання онлайн курсів.

За джерелами знань використовуються такі методи навчання: словесні – розповідь, пояснення, лекція, інструктаж; наочні – демонстрація, ілюстрація; практичні – лабораторна робота, практична робота, вправи. За характером логіки пізнання використовуються такі методи: аналітичний, синтетичний, аналітико-синтетичний, індуктивний, дедуктивний. За рівнем самостійної розумової діяльності використовуються методи: проблемний, частково-пошуковий, дослідницький.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль в тому числі у вигляді комп'ютерних тестів, виконання лабораторних робіт.

Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль, комп'ютерне тестування, виконання практичного завдання. Оцінюється вхідний, проміжний, кінцевий рівень знань студента.

Підсумковий контроль проводиться у вигляді комп'ютерних тестів.

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань поточного контролю	100	100
Підсумкова семестрова оцінка	**100**	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	85	-
Виконання та захист індивідуальних самостійних завдань	15	-
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**): 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт (наводиться перелік видів робіт)	до 10 до 10	- -
Разом за виконання завдань поточного контролю	**100**	**-**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти[1]	Кількість балів за семестр	
	денна форма	заочна форма
Відповіді (виступи) на заняттях, у т.ч. дискусії	6	-
Виконання та демонстрація практичних завдань	33	-
Виконання поточних тестових завдань	46	-
Разом за виконання завдань під час навчальних занять	**85**	**-**

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$Р_{НЗ} = (Р_{В_{100}} \times ВК_{В} + Р_{УД_{100}} \times ВК_{УД} + Р_{ТЗ_{100}} \times ВК_{ТЗ} + Р_{ЗК_{100}} \times ВК_{ЗК}) \times К_{НЗ}, \quad (1)$$

де $Р_{НЗ}$ – кількість набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр;

$Р_{В_{100}}$, $Р_{УД_{100}}$, $Р_{ТЗ_{100}}$, $Р_{ЗК_{100}}$ – кількість набраних здобувачем вищої освіти балів за семестр відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання поточних тестових завдань, за виконання та захист завдань, кейсів (кожний окремо вид робіт на навчальних заняттях оцінюється за 100-бальною шкалою);

$ВК_В$, $ВК_{УД}$, $ВК_{ТЗ}$, $ВК_{ЗК}$ – вагові коефіцієнти відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання поточних тестових завдань, за виконання та захист завдань, кейсів. Значення вагових коефіцієнтів становить:
$ВК_В = 20 \div 80 = 0,25$;
$ВК_{УД} = 10 \div 80 = 0,125$;
$ВК_{ТЗ} = 30 \div 80 = 0,375$;
$ВК_{ЗК} = 20 \div 80 = 0,25$;

$К_{НЗ}$ – коригувальний коефіцієнт. Значення коригувального коефіцієнту становить $К_{НЗ} = 80 \div 100 = 0,8$.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35–49 балів, він отримує право за власною заявою опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 34 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою вивчення навчального матеріалу дисципліни понад обсяги, встановлені навчальним планом освітньої програми, визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1.	Авторизація	Authorization
2.	Авторське право	Copyright / author’s right
3.	Академічна доброчесність	Academic integrity
4.	Аутентифікація	Authentication
5.	Впровадження	Implementation
6.	Гіпотеза	Hypothesis
7.	Доступність	Accessibility
8.	Евристично-орієнтований	Heuristics-based
9.	Експеримент	Experiment
10.	Ефект	Effect
11.	Ідентифікація	Identification
12.	Інформація	Information
13.	Кібербезпека	Cybersecurity

№ з/п	Термін державною мовою	Відповідник англійською мовою
14.	Конфіденційність	Confidentiality
15.	Метод дослідження	Research method
16.	Моделювання	Modelling
17.	Наука	Science
18.	Орієнтований на поведінку	Behavior-based
19.	Посвідчення особи	Know Your Customer (KYC)
20.	Приватний ключ	Private key
21.	Публічний ключ	Public key
22.	Сигнатурно-орієнтований	Signature-based
23.	Транзакція	Transaction
24.	Хеш	Hesh
25.	Хеш-дерево, дерево Меркла	Merkle tree
26.	Цілісність	Integrity
27.	Шифрування	Encryption

12. Рекомендована література

Основна література

1. ДСТУ ISO/IEC 27001:2023. Інформаціна безпека, кібербезпека та захист конфіденційності. Системи керування безпекою. Вимоги.
2. НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
4. Дудикевич, В. Б. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.
5. Інформаційна безпека та гібридні загрози: навчальний посібник. Укл. Мухін В.Є., Завгородній В.В., Завгородня Г.А. Київ : ТОВ «ТРОПЕА», 2024. 104 с. DOI: https://doi.org/10.32703/978-617-8268-36-7.
6. Oleksandr O. Nonik, Nadiia M. Lobanchykova, Tetiana A. Vakaliuk, Viacheslav V. Osadchyi and Oleksandr V. Farrakhov. Approaches to solving proxy performance problems for HTTP and SOCKS5 protocols for the case of multi-port passwordless access. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems. Kyiv, Ukraine, February 28, 2024. Edited by Volodymyr Sokolov, Vasyl Ustimenko, Tamara Radivilova, Mariya Nazarkevych. CEUR Workshop Proceedings, 2024. Vol. 3654. Pp. 189–200. – Режим доступу: https://ceur-ws.org/Vol-3654/paper16.pdf

7. Lobanchykova N. M., Vakaliuk T. A., Osadchyi V. V., Medvediev M. G., Pilkevych I. A. Study of Cyber Security Approaches in Organizing Digital Voting. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, February 28, 2023. Edited by Volodymyr Sokolov, Tamara Radivilova, Vasyl Ustimenko, Mariya Nazarkevych. CEUR Workshop Proceedings, Vol-3421, 2023. Pp. 198-205. – Режим доступу: https://ceur-ws.org/Vol-3421/short5.pdf

8. Lobanchykova N., Kredentsar S., Pilkevych I., Medvediev M. Information technology for mobile perimeter security systems creation. Journal of Physics: Conference Series. 2021. Vol. 1840 (1). Art. no. 012022. DOI: 10.1088/1742-6596/1840/1/012022. Режим доступу: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103522219&doi=10.1088%2f1742-6596%2f1840%2f1%2f012022&partnerID=40&md5=8d5fda39b672fb3bf33a951aa8f94578

9. Lobanchykova, N., Pilkevych, I., Korchenko, O. Analysis of attacks on components of IoT systems and cybersecurity technologies. Joint Proceedings of the Workshops on Quantum Information Technologies and Edge Computing (QuaInT+doors 2021), Zhytomyr, Ukraine, April 11, 2021. Edited by Serhiy O. Semerikov. (CEUR-WS.org). pp. 83-96.

10. Lobanchykova N., Kredentsar S., Pilkevych I., Medvediev M. Information technology for mobile perimeter security systems creation. Journal of Physics: Conference Series, Volume 1840, 012051, XII International Conference on Mathematics, Science and Technology Education (ICon-MaSTEd 2020) 15-17 October 2020, Kryvyi Rih, Ukraine. pp.1-9.

11. Законодавство України: https://zakon.rada.gov.ua/

12. Вакалюк Т. А., Фант М. О., Єфремов Ю.М., Лобанчикова Н.М., Жиляєв Є. В. Огляд алгоритмів виявлення аномалій в роботі комп'ютерних систем. Вісник Кременчуцького національного університету імені Михайла Остроградського, № 6 (149), 2024. С. 94-101. – Режим доступу: https://doi.org/10.32782/1995-0519.2024.6.11.

13. Лобанчикова Н.М. Модель побудови мобільної систем охорони периметру території .Сучасний захист інформації, 2020.Вип №1(41). С.42 – 48.

14. Digitalization of economics : inter-disciplinary and inter-branch approach : manual. Zhytomyr : Publishing House "Book-Druk", 2023. 540 p.

15. Методичні рекомендації до виконання лабораторних робіт. з навчальної дисципліни «Основи кібербезпеки» для студентів освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека»ю Частина 2. (автори: Н.М. Лобанчикова, О.В. Пірог), 2021. 36 с. Електронне видання (Протокол НМР №6 від 21.01.2021 р.). – Режим доступу: https://learn.ztu.edu.ua/course/view.php?id=1994

16. Методичні рекомендації до виконання лабораторних робіт. з навчальної дисципліни «Основи кібербезпеки» для студентів освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека». Частина 1 (автори: Н.М. Лобанчикова, О.В. Пірог), 2021. 56 с. Електронне видання (Протокол НМР №6 від 21.01.2021 р.). – Режим доступу: https://learn.ztu.edu.ua/course/view.php?id=1994

17. Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. – Тернопіль 2023. – 88 с.

Допоміжна література

18. Лобанчикова Н.М. Захист інформації в АСУ: навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

19. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation crite¬ria for IT security – Part 1: Introduction and general model.

20. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation crite¬ria for IT security – Part 2: Security functional requirements.

21. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation crite¬ria for IT security – Part 3: Security assurance requirements.

22. Інформаційні технології. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:1995): ДСТУ 3918–1999. – [Чинний від 2000–01–01]. – К.: Держстандарт України, 2000. – 50 с. – (Національний стандарт України).

12. Інформаційні ресурси в Інтернеті

23. Макс Бонк. Розуміння різних типів технік виявлення антивірусів – від сигнатурних до поведікових аналізаторів. MEDIACOM: світ новин. 08 квітня 2024. URL: https://mediacom.com.ua/rozuminnya-riznix-tipiv-texnik-viyavlennya-antivirusiv/

24. Сайт бібліотеки Державного університету «Житомирська політехніка». URL: http://lib.ztu.edu.ua.

25. Освітній портал Державного університету «Житомирська політехніка». URL: http://learn.ztu.edu.ua.

26. globalEDGE / Michigan State University. URL: https://globaledge.msu.edu.

27. Сайт Національної бібліотеки України ім. Вернадського. URL: http://www.nbuv.gov.ua.

28. Сервіс Google Академія. URL: https://scholar.google.com.ua.

29. Наукометрична база Scopus. URL: https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=searchbasic#basic.