МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра _*програмної інженерії та інформаційних технологій управління*__
(назва)

«**ЗАТВЕРДЖУЮ**»
Голова науково-методичної комісії _____
(назва комісії)

_____ _____
(підпис) (ініціали та прізвище)

«_____»_____20_____ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека інформаційних систем

(назва навчальної дисципліни)

рівень вищої освіти_____*другий (магістерський)*_____
перший (бакалаврський) / другий (магістерський)

галузь знань_____*12 Інформаційні технології*_____
(шифр і назва)

спеціальність ____*126 Інформаційні системи та технології*_____
(шифр і назва)

вид дисципліни ___*професійна підготовка*_____
(загальна підготовка / професійна підготовка)

форма навчання _____*денна*_____
(денна / заочна)

Харків – 2017 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни

Безпека інформаційних систем

(назва дисципліни)

Розробники:

доцент, к.т.н., доц.		*Євсеєв С.П.*
(посада, науковий ступінь та вчене звання)	(підпис)	(ініціали та прізвище)
(посада, науковий ступінь та вчене звання)	(підпис)	(ініціали та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

програмної інженерії та інформаційних технологій управління

(назва кафедри)

Протокол від «31» 2017 року № 1

Завідувач кафедри _____ _____ Годлевський М.Д.

(назва кафедри) (підпис) (ініціали та прізвище)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри	Підпис голови НМК (для дисциплін загальної підготовки та дисциплін професійної підготовки за спеціальністю) або завідувача випускової кафедри (для дисциплін професійної підготовки зі спеціалізації, якщо РПНД розроблена не випусковою кафедрою)

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни "Безпека інформаційних систем" є формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидії несанаційному доступу, кіберзагроз на прикладі послуг безпеки в банківських системах, грамотного застосування механізмів захисту банківської інформації на основі сучасних процедур криптосистем для забезпечення доступності, цілісності, конфіденційності та автентичності банківських транзакцій та даних.

Компетентності:

Загальні компетентності:

- Здатність застосовувати знання у практичних ситуаціях.
- Знання та розуміння предметної області та розуміння професійної діяльності.
- Здатність вчитися і оволодівати сучасними знаннями.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні (фахові) компетентності:

- здатність формування моделі порушника, визначення основних видів атак, моделі ризиків на основі синергетичного підходу, визначення ризиків безпеки інформації, інформаційної безпеки та кібербезпеки.

Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
здатність формування моделі порушника, визначення основних видів атак, моделі ризиків на основі синергетичного підходу, визначення ризиків безпеки інформації, інформаційної безпеки та кібербезпеки	Знання основних положення законодавства в галузі інформаційної та кібербезпеки, положень основних міжнародних та національних стандартів з формування системи управління інформаційною безпекою використовувати механізмів та протоколів ЦКД	визначати основні засади використання технічних систем захисту інформації (ТСЗІ), формувати профіль захисту відповідно до забезпечення послуг безпеки; проводити розрахунки ризику НСД до банківської інформації за допомогою сучасних методик та з використанням	Здатність донесення до фахівців і нефахівців інформації, ідей, проблем, рішень та власного досвіду в галузі професійної діяльності; здатність ефективно формувати комунікаційну стратегію.	Здатність здійснювати захист даних в корпоративних розподілених інформаційних системах, застосовувати системи криптографії в професійній діяльності, вивчати нові технології, методі та прийоми щодо забезпечення захисту інформації;

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
		ПЗ		

Структурно-логічна схема вивчення навчальної дисципліни

Попередні дисципліни:	Наступні дисципліни:
“Технології захисту інформації”	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Загальний обсяг (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари		Контрольні роботи (кількість робіт)	Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
1	**90/ 3**	**32**	**58**	**32**	**16**	**16**		**1**	**З**	

Співвідношення кількості годин аудиторних занять до загального обсягу складає 62 % (%):

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Назви змістових модулів. Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	2	3	4	5
Змістовий модуль 1. Принципи побудови концепції інформаційної безпеки				
	Л ЛР ПЗ СР	4 2 4 10	**Тема 1. Основні положення концепції інформаційна безпека** Механізми захисту ОС. Аналіз основних методології оцінки ризику ІБ	

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Назви змістових модулів. Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
	Л ЛР ПЗ СР Л ПЗ ЛР	4 2 4 10 6 4 4	**Тема 2. Напрямки забезпечення інформаційної безпеки** Можливості захисту файлової системи (EFS). Аналіз можливостей Центру безпеки. **Тема 3. Способи захисту інформації** Засоби аналізу захищеності. Автентифікація користувачів на основі токенів безпеки.	
Змістовий модуль 2. Принципи риск менеджменту. Управління ризиками в сфері інформаційної безпеки				
	Л ПЗ ЛР С Л ЛР СР Л СР Л СР	4 4 4 14 4 4 10 6 14 4 10	**Тема 4. Основі моделі забезпечення ІБ** Підсистема реєстрації. Дослідження стійкості парольного захисту **Тема 5. Менеджмент інцидентів ІБ** SQL-ін’єкції і методи боротьби з ними. Дослідження ефективних методів захисту від експлойтів **Тема 6. Управління ризиками** **Тема 7. Методологія оцінки ризиків**	
Разом (годин)		90		

САМОСТІЙНА РОБОТА

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацьовування лекційного матеріалу	15
2	Підготовка до практичних(лабораторних, семінарських) занять	15
3	Самостійне вивчення тем та питань, які не викладаються на лекційних заняттях	15
4	Виконання індивідуального завдання:	10

5	Інші види самостійної роботи	3
	Разом	**58**

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Розрахункова робота

(вид індивідуального завдання)

Модуль 1. Принципи побудови концепції інформаційної безпеки

Тема 1. Основні положення концепції інформаційна безпека

1. Основні функції ІБ
2. Основні принципи побудови концепції ІБ
3. Основні категорії ІБ
4. Класифікація загроз ІБ
5. Нормативна складова концепції ІБ

Тема 2. Напрямки забезпечення інформаційної безпеки

1. Правова складова ІБ
2. Основи організаційного захисту
3. Основи інженерно-технічного захисту
4. Фізичний захист
5. Модель ІБ

Тема 3. Способи захисту інформації

1. Основні канали НСД до інформації
2. Основні принципи побудови захисту
3. Напрями захисту за допомогою ТСЗІ
4. Методи криптографічного захисту
5. Нормативна складова політики безпеки

Література: основна [1 – 4]; додаткова [5 – 10].

Модуль 2. Принципи риск менеджменту. Управління ризиками в сфері інформаційної безпеки

Тема 4. Основі моделі забезпечення ІБ

1. Основні підходи до математичних моделей ІБ
2. Загальна характеристика моделей дискреційного доступу.
3. Моделі поширення прав доступу
4. Загальна характеристика політики мандатної доступу
5. Загальна характеристика тематичного розмежування доступу

Тема 5. Менеджмент інцидентів інформаційної безпеки

1. модель PDCA опису життєвого циклу
2. Основні етапі ефективного менеджменту інцидентів ІБ
3. Основні поняття, принципи та етапи інцидент-менеджменту
4. Концепція побудови ефективної системи менеджменту інцидентів ІБ
5. Структура та функціональні особливості компонентів типової системи менеджменту інцидентів ІБ

Тема 6. Управління ризиками

1. Модель безпеки з повним перекриттям
2. Основні принципи побудови концепції ІБ
3. Основні вимоги міжнародного стандарту ISO 15408
4. Методика визначення потенціалу нападу при оцінці стійкості функцій безпеки
5. Профіль захисту ІБ

Тема 7. Методологія оцінки ризиками

1. Основні принципи методології оцінки
2. Основні принципи побудови концепції ІБ
3. Методики побудови систем захисту інформації, що включають етап аналізу ризиків
4. Методика “Facilitated Risk Analysis Process (FRAP)”

Методика оцінка серйозності мережевої атаки, яка використовується SANS / GIAC

Література: основна [1 – 4]; додаткова [5 – 10].

МЕТОДИ НАВЧАННЯ

При викладанні навчальної дисципліни для активізації навчального процесу передбачено застосування сучасних навчальних технологій, таких, як: проблемні лекції; робота в малих групах; семінари-дискусії; кейс-метод; ділові ігри.

Проблемні лекції спрямовані на розвиток логічного мислення студентів. Коло питань теми лекції обмежується двома-трьома ключовими моментами, увага студентів концентрується на матеріалі, що не знайшов широкого відображення в підручниках, використовується досвід закордонних навчальних закладів з роздаванням студентам під час лекцій друкованого матеріалу та виділенням головних висновків з питань, що розглядаються. При викладанні лекційного матеріалу студентам пропонуються питання для самостійного розмірковування. При цьому лектор задає запитання, які спонукають студента шукати розв'язання проблемної ситуації. Така система примушує студентів сконцентруватися і почати активно мислити в пошуках правильної відповіді.

На початку проведення проблемної лекції необхідно чітко сформулювати проблему, яку необхідно вирішити студентам. При викладанні лекційного матеріалу слід уникати прямої відповіді на поставлені запитання, а висвітлювати лекційний матеріал таким чином, щоб отриману інформацію студент міг використовувати при розв'язанні проблеми.

Міні-лекції передбачають викладення навчального матеріалу за короткий проміжок часу й характеризуються значною ємністю, складністю логічних побудов, образів, доказів та узагальнень. Міні-лекції проводяться, як правило, як частина заняття-дослідження. На початку проведення міні-лекції за вказаними темами лектор акцентує увагу студентів на необхідності представити викладений лекційний матеріал у так званому структурно-логічному вигляді. На розгляд виносяться питання, які зафіксовані у плані лекцій, але викладаються вони стисло. Лекційне заняття, проведене у такий спосіб, пробуджує у студента активність та увагу при сприйнятті матеріалу, а також спрямовує його на використання системного підходу при відтворенні інформації, яку він одержав від викладача. Проблемні лекції та міні-лекції доцільно поєднувати з такою формою активізації навчального процесу, як робота в малих групах.

Робота в малих групах дає змогу структурувати лекційні або лабораторні заняття за формою і змістом, створює можливості для участі кожного студента в роботі за темою заняття, забезпечує формування особистісних якостей та досвіду соціального спілкування. Після висвітлення проблеми (при використанні проблемних лекцій) або стислого викладання матеріалу (при використанні міні-лекцій) студентам пропонується об'єднуватися у групи по 5-6 осіб та презентувати наприкінці заняття своє бачення та сприйняття матеріалу.

Презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань. Однією з позитивних рис презентації та її переваг при використанні в навчальному процесі є обмін досвідом, який здобули студенти при роботі у певній малій групі.

Лабораторні заняття (з елементами семінарської дискусії) дозволяють формувати у студентів навички особистого експериментального дослідження фізичних процесів що відбуваються під час роботи компонентів операційної системи, проводити аналіз умов її функціонування, а також розробляти нові елементи та системні компоненти відповідно до вимог, що пред'являються до них, узагальнювати отримані результати, формулювати висновки та думки, вести подальший обмін думками та поглядами з іншими учасниками щодо отриманих результатів досліджень з даної теми, а також розвивають творче мислення, допомагають формувати погляди і переконання, вчать об'єктивно оцінювати результати і пропозиції опонентів, критично підходити до власних результатів та поглядів.

Ділові та рольові ігри – форма активізації студентів, за якої вони задіяні в процесі інсценізації певної виробничої ситуації у ролі безпосередніх учасників подій.

Кейс-метод – метод аналізу конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності спеціалістів і передбачає розгляд виробничих, управлінських та інших ситуацій, складних конфліктних випадків, проблемних ситуацій, інцидентів у процесі вивчення навчального матеріалу.

Розподіл форм та методів активізації процесу навчання за темами навчальної дисципліни

Тема	Практичне застосування навчальних технологій
Тема 2. Напрямки забезпечення інформаційної безпеки	*Лекція проблемного характеру* "Принципи побудови сучасного ПЗ щодо забезпечення ІБ"
Тема 4. Основі моделі забезпечення ІБ	*Міні-лекція* "Основні вимоги щодо основних математичних моделей"
Тема 6. Управління ризиками	*Кейс-метод* "Методики оцінки економічного збитку"

МЕТОДИ КОНТРОЛЮ

Система оцінювання знань, вмінь та навичок студентів передбачає виставлення оцінок за усіма формами проведення занять. Перевірка та оцінювання знань студентів може проводитись у таких формах:

1. Оцінювання роботи студентів у процесі лабораторних занять.
2. Проведення проміжного контролю.
3. Проведення модульного контролю.

Загальна модульна оцінка складається з поточної оцінки, яку студент отримує під час лабораторних занять та оцінки за виконання модульної контрольної роботи.

Загальна оцінка з дисципліни визначається як середнє арифметичне модульних оцінок та оцінки яка отримана під час проведення екзамену.

Порядок поточного оцінювання знань студентів

Поточне оцінювання здійснюється під час проведення лабораторних занять і має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Об'єктами поточного контролю є:

1) активність та результативність роботи студента протягом семестру над вивченням програмного матеріалу дисципліни; відвідування занять;

2) виконання проміжного контролю;

3) виконання модульного контрольного завдання.

Контроль систематичного виконання самостійної роботи та активності на лабораторних заняттях

Оцінювання проводиться за 5-бальною шкалою за такими критеріями:

1) розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються;

2) ступінь засвоєння матеріалу дисципліни;

3) ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються;

4) уміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків при виконанні завдань, винесених для самостійного опрацювання, та завдань, винесених на розгляд в аудиторії;

5) логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки.

Оцінка "відмінно" ставиться за умови відповідності виконаного завдання студента або його усної відповіді до всіх п'яти зазначених критеріїв.

Відсутність тієї чи іншої складової знижує оцінку на відповідну кількість балів.

При оцінюванні практичних завдань увага приділяється також їх якості та самостійності, своєчасності здачі виконаних завдань викладачу (згідно з графіком навчального процесу). Якщо якась із вимог не буде виконана, то оцінка буде знижена.

Проміжний модульний контроль

Проміжний модульний контроль рівня знань передбачає виявлення опанування студентом матеріалу лекційного модуля та вміння застосовувати його для вирішення практичної ситуації і проводиться у вигляді контрольної роботи за темами 1-го або 2-го модулю.

Проведення модульного контролю

Модульний контроль здійснюється та оцінюється за допомогою проведення контрольної роботи за всіма темами дисципліни.

Підсумковий/семестровий контроль проводиться у формі семестрового екзамену. Семестрові екзамени – форма оцінки підсумкового засвоєння студентами теоретичного та практичного матеріалу з окремої навчальної дисципліни, що проводиться як контрольний захід.

Підсумкова оцінка з дисципліни розраховується як середня з кількох складових, що враховує оцінки кожного виду контролю (дві оцінки за результатами поточного модульного контролю, оцінку за курсовий проект і оцінку за семестрову контрольну роботу).

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів

	Поточний контроль			Семестровий контроль	Всього за семестр
	КР	лр	ІНДЗ		
Підсумкові бали	75			25	100
Макс. проміжні бали	12	5	26		
Кільк. од. обліку у семестрі	*2*	*5*	*1*		
Макс. проміжних балів, всього	24	25	26		100
Коеф.. перерахунку	1				
Макс. кільк. підсумкових балів	24	25	26	31	100

Таблиця 2 – Розподіл балів за виконання курсового проекту

Пояснювальна записка	Ілюстративна частина	Захист роботи	Сума
до 25	до 25	до 50	100

Таблиця 3 – Шкала оцінювання знань та умінь: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
90 ... 100	A	відмінно
82 … 89	B	добре
74 … 81	C	
64 … 73	D	задовільно
60 … 63	E	
35 … 59	FX	незадовільно з можливістю повторного складання
0 … 34	F	незадовільно з обов'язковим повторним вивченням дисципліни

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Євсеєв С.П. Лабораторний практикум з дисципліни "Інформаційна безпека" [Електронний ресурс]. – Режим доступу: ntumoodle.com

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1 Ярочкин В.И. Информационная безопасность: Учебник для вузов – М.: Академический проект, 2008. – 544 с.

2. Богуш В. М., Юдін О. К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432с.

3. Козиол Дж., Личфилд Д., Энли К. и др. Искусство взлома и защиты систем. – С.Пб.: – 2006. – 416с.

4. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. – 636 с.

Допоміжна література

5. Остапов С. Е. Технології захисту інформації / С. Е. Остапов,

С. П. Євсеєв, О. Г. Король. – Чернівці : Видавничий дім "РОДОВІД", 2014. – 428 с.

7. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.

8. ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. management [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

9. ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Электронный ресурс]. – Режим доступа к ресурсу:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414

10. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413

11. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. – Режим доступа к ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11423

12. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. – Режим доступа к ресурсу:

http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii

13. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. – Режим доступа к ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11425

14. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. – Режим доступа к ресурсу: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005.

15. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. – Режим доступа к ресурсу: http://lindex.net.ua/ua/shop/bibl/500/doc/11427.

16. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

17. ISO/IEC 27002:2013 – Information technology -- Security techniques – Code of practice for information security controls. [Электронный ресурс]. – Режим доступа к ресурсу:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

18. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Электронный ресурс]. – Режим доступа к ресурсу:
http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+27006%3A2015+&sort=rel&type=simple&published=on.

19. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). [Электронный ресурс]. – Режим доступа к ресурсу: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf

20. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Электронный ресурс]. – Режим доступа к ресурсу: http://s-byte.com/useful/27002.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

21. Сайт дистанційного навчання ХНЕУ ім. С. Кузнеця, дисципліна "Інформаційна безпека". – Режим доступу : http://www.ikt.hneu.edu.ua.

22. ICO – Міжнародна організація по стандартизації. Розробник і видавець міжнародних стандартів [Електронний ресурс]. – Режим доступу : http://www.iso.org/iso/ru