МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

МЕТОДИЧНІ ВКАЗІВКИ
до практичних занять та виконання розрахунково-графічної роботи
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
Кібербезпеки та математичного
моделювання
Протокол №4
від 15 квітня 2024 р.

Чернігів 2024

Інформаційна безпека держави. Методичні вказівки до практичних занять та виконання розрахунково-графічної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с.

Укладачі: ЛАРЧЕНКО МАРИНА ОЛЕКСАНДРІВНА, доцент кафедри кібербезпеки та математичного моделювання, кандидат юридичних наук, доцент.
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – МЕХЕД ДМИТРО БОРИСОВИЧ,
доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук, доцент

ЗМІСТ

ВСТУП

Метою проведення практичних занять з навчальної дисципліни «Інформаційна безпека держави» є формування у студентів знань щодо сутності інформаційної безпеки як складного багаторівневого явища, що має соціальні, психологічні й технічні виміри; засвоєння студентами основ сучасних методів захисту інформації (зокрема технічного, інженерного, криптографічного та організаційного); вивчення нормативно-законодавчої бази України щодо захисту інформації; придбання практичних навичок реалізації захисту персональних даних в процесі введення, виведення, передавання, оброблення, накопичення і зберігання інформації; застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності.

Після завершення практичних занять здобувач має:

знати:

- поняття інформаційна безпека держави, суспільства та особи;
- стан інформаційного простору та інформаційної безпеки держави;
- джерела загроз інформаційній безпеці;
- проблеми інформаційної безпеки держави;
- небезпеки для інформаційної безпеки держави, особи та суспільства;
- методи запобігання та ліквідації загроз інформаційній безпеці;
- основні об'єкти та суб'єкти забезпечення інформаційної безпеки;
- різновиди інформаційної безпеки особи, суспільства і держави;
- проблеми у сфері інформаційних відносин;
- основи системного підходу до забезпечення інформаційної безпеки суспільства і держави;
- нормативно-правову базу, що регулює і забезпечує інформаційну безпеку держави;

вміти:

- визначати та враховувати у практичній діяльності основні тенденції розвитку сучасних інформаційних технологій та оцінювати їх можливий вплив на національну безпеку;
- визначати вплив факторів, загроз на забезпечення інформаційної безпеки держави;
- використовувати методи запобігання та ліквідації загроз інформаційній безпеці;
- визначати методи та засоби захисту життєва важливих інтересів особистості, суспільства, держави в інформаційній сфері;
- виявляти, давати оцінку джерел загроз інформаційній безпеці;
- давати оцінку загроз та засобів впливу на інформаційну безпеку;
- розрізняти основні напрями і можливості вдосконалення системи забезпечення інформаційної безпеки на національному і міжнародному рівнях, її проблемні аспекти;
- виявляти причини інформаційних воєн;

- оволодіти навичками прогнозування розвитку соціально-політичних процесів в контексті інформаційних операцій та воєн;

- формувати стратегічні рішення у сфері забезпечення інформаційної безпеки за результатами моніторингу і аналізу в інформаційній сфері;

- захищати права та інтереси суб'єктів інформаційної діяльності;

- творчо застосовувати у практичній діяльності вимоги нормативно-правових актів, що забезпечують інформаційний суверенітет та інформаційну безпеку держави.

Ключові слова: інформаційна безпека, захист інформації, конфіденційність інформації, несанкціонований доступ, інформаційні ресурси, вразливості, кібервійна, кібертероризм, кібершпигунство.

Методи навчання

Пояснювально-ілюстративний метод – застосовується в ході лекцій та у процесі самостійної роботи студентів для передачі великих масивів навчальної інформації в опрацьованому вигляді.

Репродуктивний метод – застосовується в ході практичних занять і процесі самостійної роботи, передбачає набуття студентами навичок використання визначених алгоритмів вирішення навчальних та професійних завдань.

Метод проблематизації та евристичний метод – застосовуються в ході лекційних, лабораторних занять, самостійної та індивідуальної роботи.

Поради з планування і організації вивчення навчальної дисципліни

Практична робота здобувача є одним із важливих засобів оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять. Зміст практичної роботи при вивченні дисципліни «Інформаційна безпека держави» визначається робочою програмою дисципліни, завданнями та вказівками викладача, даними методичними вказівками. Головною метою практичної роботи є закріплення, розширення та поглиблення набутих у процесі аудиторної роботи знань, вмінь та навичок, а також самостійне вивчення та засвоєння нового матеріалу під керівництвом викладача. Питання, що виникають у здобувачів стосовно виконання запланованих завдань, вирішуються на консультаціях, які проводяться згідно графіку, затвердженого кафедрою кібербезпеки та математичного моделювання НУ «Чернігівська політехніка».

Практична робота здобувачів під час вивчення навчальної дисципліни «Інформаційна безпека держави» включає такі форми:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;

- вивчення окремих тем і питань, які передбачені для самостійного опрацювання;

- підготовка до практичних занять;

- систематизація вивченого матеріалу дисципліни перед проведенням модульних контрольних заходів;

- підготовка наукової статті (есе) за програмою дисципліни;

- підготовка доповідей та участь в наукових студентських конференціях, круглих столах, тощо.

Всі завдання самостійної роботи здобувачів поділяються на обов'язкові та вибіркові, виконуються у встановлені терміни, з відповідною максимальною оцінкою та передбачають певні форми звітності щодо їх виконання. Обов'язкові завдання виконуються кожним без винятку здобувачем у процесі вивчення навчальної дисципліни, вибіркові завдання є альтернативними.

Після виконання обов'язкових та вибіркових завдань у встановлені терміни студент звітує викладачеві, а набрані ним бали враховуються як кількість балів за поточну успішність в навчальній роботі.

Оцінювання результатів поточної роботи (завдань, що виконуються на практичних заняттях та консультаціях, результати самостійної роботи студентів) проводиться за такими критеріями (у відсотках від кількості балів, виділених на завдання із заокругленням до цілого числа):

а) 100 % - завдання виконано правильно, вчасно і без зауважень;

а) 80 % - завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (розмірності, висновки, оформлення тощо);

а) 60 % - завдання виконане повністю, але містить суттєві помилки у розрахунках або в методиці;

б) 40 % - завдання виконане частково та містить суттєві помилки методичного або розрахункового характеру;

б) 0 % - завдання не виконане.

У процесі вивчення здобувачами дисципліни «Інформаційна безпека держави» передбачено наступні види роботи викладачів зі здобувачами:

- індивідуальні консультації за графіком, затвердженим кафедрою кібербезпеки та математичного моделювання;

- перевірка виконання індивідуальних завдань поточного контролю та модульних контрольних робіт;

- індивідуальні консультації зі здобувачами з метою підвищення рівня їхньої підготовки та розвитку індивідуальних здібностей, результатом яких може бути підготовка наукових доповідей, статей.

Контроль практичної роботи здобувачів здійснюється на практичних заняттях у формі поточного контролю, модульних контрольних робіт та перевірки якості виконання домашніх завдань.

1. РОБОЧА ПРОГРАМА (у скороченому вигляді)

1.1 **Опис навчальної дисципліни**

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань
12 – Інформаційні технології</td><td>обов’язкова</td></tr>
<tr><td></td><td rowspan="4">Спеціальність
125 – Кібербезпека та захист інформації</td><td>Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>1</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>Семестр</td></tr>
<tr><td>1</td></tr>
<tr><td rowspan="10">Тижневих годин: аудиторних – 1,875 год. самостійної роботи здобувача – 5,625 год.</td><td rowspan="10">Перший (бакалаврський) кваліфікаційний рівень:
бакалавр з кібербезпеки та захисту інформації</td><td>Лекції</td></tr>
<tr><td>16 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>-</td></tr>
<tr><td>Практичні</td></tr>
<tr><td>14 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>90 год.</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>Диференційований залік</td></tr>
</table>

Дисципліна є складовою частиною професійної підготовки та відноситься до навчальних дисциплін циклу «Обов’язкові дисципліни» за спеціальністю «Кібербезпека та захист інформації» (бакалавр з кібербезпеки та захисту інформації).

1.2 **Мета навчальної дисципліни**

Метою викладання навчальної дисципліни «Інформаційна безпека держави» є оволодіння ЗВО поняттями забезпечення інформаційної безпеки, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство.

Завданням вивчення дисципліни «Інформаційна безпека держави» є:

1) формування знань щодо концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки;

2) ознайомлення з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою;

3) вироблення навичок використання знань теорії і практики інформаційної безпеки у практиці публічного управління;

4) підготувати студентів до використання отриманих знань і навиків у вивченні спеціальних предметів та розв'язуванні практичних задач.

Загальний фокус дисципліни направлений на формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо забезпечення інформаційної безпеки національних інтересів у будь-якій сфері.

Спеціальний фокус дисципліни направлений на опанування основними термінами та категоріями інформаційної безпеки на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі діяльності майбутнього спеціаліста з інформаційної безпеки та/або кібербезпеки.

Дисципліна спрямована на досягнення здобувачами ступеня бакалавра з кібербезпеки та захисту інформації зі спеціальності 125 – кібербезпека та захист інформації**:**

1) загальні:

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

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

КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенство права, прав і свобод людини і громадянина України.

2) спеціальні (фахові):

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Очікувані результати навчання з дисципліни

В процесі вивчення дисципліни студенти повинні отримати такі **програмні результати навчання:**

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та/або кібербезпеки;

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

1.3 **Критерії оцінювання результатів навчання**

З тими ЗВО, які до проведення підсумкового семестрового контролю не встигли виконати всі обов'язкові види робіт та мають підсумкову оцінку від 0 до 19 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни.

Дисципліну можна вважати такою, що засвоєна, якщо ЗВО:

1) знає:

- концептуальні основи інформаційної безпеки України;
- складові елементи системи інформаційної безпеки України;
- критерії формування життєво важливих сфер життєдіяльності;
- основні об'єкти та суб'єкти забезпечення інформаційної безпеки;
- основні концепції інформаційної безпеки;
- основні підходи до визначення ключових понять (безпека, загроза, система безпеки, забезпечення національної безпеки);
- стадії формування загроз та небезпек;
- основні підходи до забезпечення інформаційної безпеки;
- нормативно-правову базу, що регулює суспільні безпекові відносини.

2) вміє:

- визначати вплив факторів зовнішньополітичного середовища на забезпечення інформаційної безпеки в контексті зародження і переростання кризової ситуації у конфлікт;
- визначати та враховувати у практичній діяльності основні тенденції розвитку геополітичного простору та оцінювати їх можливий вплив на інформаційну безпеку України;
- використовувати понятійно-категорійний апарат при аналізові інформаційної, політичної, економічної, воєнної, екологічної та інших функціональних сфер національної безпеки при виборі та реалізації концептуальних підходів щодо управління інформаційної безпекою;
- пропонувати організаційно-правові заходи підвищення ефективності діяльності органів державної влади у сфері забезпечення інформаційної безпеки у зовнішньополітичній сфері.

У цьому випадку ЗВО може отримати підсумкову оцінку «задовільно» - 60 балів – Е (в т.ч. й під час ліквідації академічної заборгованості з дисципліни).

1.4 Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з дисципліни є поточний та семестровий контроль. Поточний контроль складається з опитувань, які проводяться під час лекцій, а також лабораторних/практичних занять. Семестровий контроль проводиться у вигляді диференційованого заліку, запитання до якого на початку семестру розміщується у системі дистанційного навчання.

1.5 Програма навчальної дисципліни

Змістовий модуль 1. Загальні основи інформаційної безпеки держави

Тема 1. Концептуальні засади інформаційної безпеки

Базові поняття щодо інформації та інформаційної безпеки. Поняття та загальні властивості інформації. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері. Об'єкти, суб'єкти та види інформаційної безпеки. Інформаційний вплив та його різновиди. Визначення об’єктів інформаційного впливу. Інформаційна безпека як складова частина національної безпеки держави.

Тема 2. Загрози інформаційній безпеці держави, суспільства та особи

Поняття загроз інформаційній безпеці. Види загроз інформаційній безпеці. Дестабілізуючі фактори загроз. Фактори загроз інформаційній безпеці. Джерела загроз інформаційній безпеці. Етапи розвитку засобів інформаційних комунікацій.

Тема 3. Кібертероризм в аспекті глобалізації: актуальні проблеми національної та міжнародної кібербезпеки

Кібертероризм: історія розвитку та сучасні тенденції. Загрози кібертероризму та найбільш відомі кібератаки в сучасному цифровому суспільстві як інформаційні виклики національній безпеці. Правові засади формування та розвитку державної системи протидії кібертероризму в Україні як загрозі інформаційній безпеці. Зарубіжний досвід щодо розвитку систем протидії загрозам кібертероризму на державному рівні: національні структури, які забезпечують кібербезпеку у зарубіжних країнах, а також кібервійська провідних держав світу, їх можливості та перспективи.

Тема 4. Реагування на надзвичайні комп’ютерні інциденти на державному та глобальному рівні

Національні команди реагування на надзвичайні комп’ютерні інциденти CERT/CSIRT. Основні завдання національних команд реагування

CERT/CSIRT/. Міжнародні структури, які забезпечують кібербезпеку на глобальному рівні. Суб'єкти національної системи кібербезпеки України.

Тема 5. Кібертероризм та інформаційна безпека України

Кіберпростір як сфера геополітичного протистояння. Кіберзброя – суспільно небезпечний продукт цифрових технологій у міжнародних конфронтаціях. Проблематика міжнародної кібербезпеки – кібератаки, кібервійни, інформаційні війни, мережевоцентричні війни, їх ознаки та особливості. Кібертероризм, політичний хактівізм, кібершпигунство, кібердиверсії та кіберекстремізм як сучасні загрози національній та міжнародній безпеці. Стратегії кібербезпеки у зарубіжних країнах. Загрози кібертероризму критичній інфраструктурі та забезпечення її кібербезпеки у зарубіжних країнах. Запровадження в Україні кращих практик реалізації державних стратегій та імпліментація вимог міжнародно-правових документів з протидії кібертероризму. Правові засади кіберзахисту критично важливих об'єктів України. Розробка національної стратегії протидії кібертероризму для об'єктів критичної інфраструктури України.

Змістовий модуль 2. Основи безпеки інформаційних технологій

Тема 6. Основи безпеки інформаційних ресурсів

Загрози безпеці інформації та інформаційних ресурсів. Збитки як категорія класифікації загроз. Загрози безпеці інформації при забезпеченні конфіденційності. Джерела загроз безпеці інформації. Класифікація уразливостей безпеці. Моделі порушень інформаційних ресурсів. Побудова моделі порушника.

Забезпечення безпеки інформації та інформаційних ресурсів. Основні напрями забезпечення безпеки інформації. Правовий захист. Організаційний захист. Служба захисту інформації. Інженерно-технічний захист. Фізичні засоби захисту. Системи контролю доступу. Апаратні засоби захисту. Програмні засоби захисту. Криптографічні засоби захисту.

Тема 7. Захист інформаційних, інформаційно - комунікаційних систем та мереж

Джерела конфіденційної інформації. Інформаційна система як об'єкт захисту інформації. Технічні засоби обробки інформації. Інформаційна система як об'єкт захисту інформації. Рівні захисту інформаційних систем. Корпоративна інформаційна система. Класи корпоративних інформаційних систем. Аналіз вразливостей корпоративних інформаційних систем. Основні принципи захисту інформації.

Визначення інформаційно-комунікаційних систем. Багаторівневі моделі інформаційно-комунікаційних систем. Мережева технологія. Мережева взаємодія. Захист інформації в комп'ютерних мережах. Безпека інформаційних ресурсів у ІКСМ на базі ISO/IEC. Задачі організації безпеки інформації та інформаційних ресурсів.

Тема 8. Основи управління інформаційною безпекою

Політика інформаційної безпеки організації. Визначення політики інформаційної безпеки організації. Система забезпечення інформаційної безпеки організації. Методологія розробки політики безпеки організації Концепція інформаційної безпеки в організації. Аналіз та оцінка ризиків. Основні правила інформаційної безпеки організації. Вибір основних рішень з забезпечення безпеки інформації Правила побудови системи забезпечення інформаційної безпеки. Вибір варіанту побудови системи забезпечення інформаційної безпеки. Оцінювання витрат на СЗІБ. Визначення вимог до заходів, методів та засобів захисту. Вибір основних рішень з забезпечення безпеки інформації. Правила розмежування доступу користувачів та процесів до ресурсів інформаційної сфери організації. Документальне оформлення політики безпеки. Заходи управління інформаційною безпекою.

Тема 9. Забезпечення інформаційної безпеки України

Інформаційна безпека і її місце в системі національної безпеки України. Принципи забезпечення безпеки. Основні реальні та потенційні загрози інформаційній безпеці України. Загрози національній безпеці України в інформаційній сфері.

Тема 10. Система та політика забезпечення інформаційної безпеки України

Основні функції системи забезпечення інформаційної безпеки України. Мета функціонування, завдання системи забезпечення інформаційної безпеки. Політика інформаційної безпеки і її реалізація в Законодавстві України. Органи забезпечення інформаційної безпеки і захисту інформації. . Методи та заходи забезпечення інформаційної безпеки України.

Інформаційна безпека України у сфері прав і свобод людини. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина. Структура конституційного права на інформацію. Нормативно-правове забезпечення інформаційної безпеки України.

1.6 **Розподіл балів, які отримують студенти**

Поточний модульний контроль

Модуль за робочим планом дисципліни та форма контролю		**Кількість балів**
Семестр 1		**0… 60**
Модуль 1		**0… 45**
1	Повнота відповідей на запитання на практичних заняттях	0… 5х7
2	Модульне контрольне завдання (тестування)	0… 10
	Всього	0… 45
Модуль 2		**0… 15**

1	Якість підготовки розрахунково-графічної роботи	0… 10
2	Результати захисту розрахунково-графічної роботи	0… 5
	Всього	0… 15

Підсумковий семестровий контроль

Вид контролю		**Кількість балів**
Семестр 1		**0… 100**
1	Модульна оцінка за семестр	0… 60
2	Відповіді на запитання під час заліку	0… 40
	Всього	0… 100

Шкала оцінювання: національна та ECTS

Оцінка в балах	**Оцінка ECTS**		**Оцінка за національною шкалою**
			для екзамену (диференційованого заліку)
90 – 100	**A**	*Відмінно* – відмінне виконання лише з незначною кількістю помилок	відмінно
82-89	**B**	*Дуже добре* – вище середнього рівня, але з деякими поширеними помилками	Добре
75-81	**C**	*Добре* –в цілому правильне виконання, але з помітними помилками	
66-74	**D**	*Задовільно* – виконання в повному обсязі, але зі значною кількістю недоліків	задовільно
60-65	**E**	*Достатньо* – виконання відповідно до мінімальних вимог	
0-59	**FX**	*Незадовільно* – недостатньо: необхідно допрацювати	незадовільно з можливістю повторного складання

1.7 Рекомендована література

Базова

1. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній: практичний посібник / Ю.І. Когут. – Київ: Консалтингова компанія «СІДКОН», 2021. – 372 с.

2. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право.* Том 2 № 77 (2023). С. 121-127.

3. Нестеренко Галина. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.

5. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Іва-на Франка, 2017. 725 с.

6. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Ч. 2. Хар-ків: Вид. ХНЕУ, 2018. 196 с.

7. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

8. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В.Л.Бурячок, Г.М.Гулак, В.Б.Толубко. — Київ: ТОВ «СІК ГРУП Україна», 2015. - 449 с.

9. Дудикевич В.Б. Забезпечення інформаційної безпеки держави: навч. посібник / В.Б.Дудикевич, І.Р.Опірський, П.І.Гаранюк, В.С.Зачепило, А.І.Партика. – Львів. Видавництво Львівської політехніки, 2017. – 204 с.

10. Інформаційна безпека держави: підручник / В.М.Петрик, М.М.Присяжнюк, Д.С.Мельник та ін. ; в 2 т. – Т.1. / за заг. ред. В.В.Остроухова – К.: ДНУ «Книжкова палата України», 2016. – 264 с.

11. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл

12. Інформаційна безпека. Методичні вказівки до технологічної практики для студентів напряму підготовки (спеціальності) 6.170103 «Управління інформаційною безпекою», 125 « Кібербезпека» / Укл.: Зейналова Е.Ф., Гур'єв В.І. – Чернігів: ЧНТУ, 2018. – 25 с.

13. Лісовська Ю.П. Інформаційна безпека України: навч.посіб. / Лісовська Ю.П. – К.: Видавничий дім «Кондор», 2018. – 172 с.

14. Стратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14

15. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року No 47/2017 URL: https://zakon.rada.gov.ua/go/47/2017.

16. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року No 152/2022 URL: https://zakon.rada.gov.ua/go/152/2022.

17. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення

забороненої інформаційної продукції. Закон Украї-ни. URL: https://zakon.rada.gov.ua/laws/show/2110-20#Text.

18. Указ Президента України № 449/2014. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» // www.president.gov.ua.

19. Указ Президента України № 96/2016. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року " Про Стратегію кібербезпеки України" // www.president.gov.ua.

20. Указ Президента України від 26.05.2015 р., № 287/2015. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". Офіц. вид. - К.: Урядовий кур'єр від 29.05.2015, № 95. // www.president.gov.ua.

21. Указ Президента України від 12.10.2018 р., № 320/2018. Про рішення Ради національної безпеки і оборони України від 12 жовтня 2018 року «Про невідкладні заходи щодо захисту національних інтересів на Півдні та Сході України, у Чорному та Азовському морях і Керченській протоці» // www.rnbo.gov.ua.

22. Kristan Stoddart. Cyberwarfare Threats to Critical Infrastructure. Springer Nature Switzerland AG, 2022. 564 p. URL: https://doi.org/10.1007/978-3-030-97299-8

Допоміжна

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / МВС України, Ун-т внут. справ - Х., 2010. -366с.

2. Безпека інформації. Науковий журнал «Безпека інформації» засновано у 1995 році. Засновником та видавцем є Національний авіаційний університет.

3. Юдін О.К. Інформаційна безпека. Нормативно-правове-забезпечення: Підручник. – К.: Видавництво Національного авіаційного університету «НАУ-друк», 2011. – 640 с.

4. Глобалізація і безпека розвитку / [Білорус О. Г., Гончаренко М. О., та ін.]; НАН України, Київ. нац. екон. ун-т. - К.: КНЕУ, 2011. - 733 с.

5. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : Навч. посіб. для вищих навч. закладів / Українська Академія держ. управління при Президентові України; Академія держ. податкової служби України. — К. : Преса України, 2010. — 304 с.

6. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

7. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

8. Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett- Packard Company.

9. Kiountouzis, E.A.; Kokolakis, S.A. Information systems security: facing the information society of the 21st century. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4

Інформаційні ресурси

1. Офіційний портал Верховної Ради України: http://zakon1.rada.gov.ua/
2. Урядовий портал (КМУ) : http://www.kmu.gov.ua/
3. Офіціальний сайт Президента України: http://www.president.gov.ua/
4. Офіціальний сайт МВС України: http://mvs.gov.ua/mvs/
5. Офіціальний сайт СБУ України http://www.sbu.gov.ua/
6. Офіціальний сайт МНС України http://www.mns.gov.ua/
7. Офіціальний сайт УДО України http://www.do.gov.ua/
8. Офіціальний сайт ДАІ МВС України http://www.sai.gov.ua/
9. Офіціальний сайт ВВ МВС України http://vv.gov.ua/
10. Офіціальний сайт ДСО МВС України http://dso.gov.ua/
11. Офіційний сайт Держспецзв'язку України https://cip.gov.ua/ua
12. Офіційний сайт Управління охорони ДТ Міністерства оборони України https://www.mil.gov.ua/ministry/struktura-aparatu-ministerstva/ypravlinnia-ohoroni-derzhavnoi-taemniczi.html

ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

1. Основи безпеки інформаційних ресурсів

1.1 Вирішувані питання

1. Загрози безпеці інформації та інформаційних ресурсів.

2. Збитки як категорія класифікації загроз. Загрози безпеці інформації при забезпеченні конфіденційності. Джерела загроз безпеці інформації.

3. Класифікація вразливостей безпеці. Моделі порушень інформаційних ресурсів. Побудова моделі порушника.

4. Забезпечення безпеки інформації та інформаційних ресурсів, основні напрями: правовий захист, організаційний захист, служба захисту інформації, інженерно-технічний захист.

5. Фізичні засоби захисту. Системи контролю доступу. Апаратні засоби захисту. Програмні засоби захисту. Криптографічні засоби захисту.

1.2 Основні поняття

Види загроз інформаційній безпеці, наслідки порушення конфіденційності інформації, джерела загроз, класифікація вразливостей, способи порушення безпеки інформаційних ресурсів, профіль порушника безпеки інформаційних ресурсів, запобігання порушенням, класифікація видів захисту, особливості окремих засобів захисту інформації та інформаційних ресурсів.

2. Захист інформаційних, інформаційно-комунікаційних систем та мереж

2.1 Вирішувані питання

1. Джерела конфіденційної інформації. Інформаційна система як об’єкт захисту інформації.

2. Технічні засоби обробки інформації. Рівні захисту інформаційних систем.

3. Корпоративна інформаційна система. Класи корпоративних інформаційних систем. Аналіз вразливостей корпоративних інформаційних систем.

4. Визначення інформаційно-комунікаційних систем. Багаторівневі моделі інформаційно-комунікаційних систем. Мережева технологія. Мережева взаємодія.

5. Захист інформації в комп’ютерних мережах. Безпека інформаційних ресурсів на базі ISO/IEC. Задачі організації безпеки інформації та інформаційних ресурсів.

2.2 Основні поняття

Конфіденційність інформації, захист інформаційної системи, основні принципи захисту інформації, рівні захисту, особливості корпоративної інформаційної системи, аналіз вразливостей, інформаційно-комунікаційні системи, мережева технологія та взаємодія, безпека інформаційних ресурсів, організація безпеки.

3. Основи управління інформаційною безпекою

3.1 Вирішувані питання

1. Політика інформаційної безпеки організації. Система її забезпечення.
2. Методологія розробки політики безпеки організації. Концепція інформаційної безпеки в організації. Аналіз та оцінка ризиків.
3. Основні правила інформаційної безпеки організації. Вибір основних рішень з забезпечення безпеки інформації.
4. Правила побудови системи забезпечення інформаційної безпеки. Визначення вимог до заходів, методів та засобів захисту та вибір основних рішень.
5. Правила розмежування доступу користувачів та процесів до ресурсів інформаційної сфери організації. Документальне оформлення політики безпеки.

3.2 Основні поняття

Політика інформаційної безпеки, система забезпечення інформаційної безпеки, політика безпеки організації, концепція інформаційної безпеки, оцінка ризиків, основні правила інформаційної безпеки, методи та засоби захисту інформації, правила розмежування доступу користувачів, документальне оформлення політики безпеки.

4. Забезпечення інформаційної безпеки України

4.1 Вирішувані питання

1. Місце інформаційної безпеки в системі національної безпеки України. Розмежування понять: «інформаційна безпека», «національна безпека», «кібербезпека».
2. Принципи забезпечення національної та інформаційної безпеки.
3. Основні реальні та потенційні загрози інформаційній безпеці України.
4. Основне законодавство з питань захисту національної безпеки України на сучасному етапі.

4.2 Основні поняття

Національна безпека, кібербезпека, принципи забезпечення безпеки, реальні та потенційні загрози інформаційній безпеці, законодавство із захисту національної безпеки.

5. Система та політика забезпечення інформаційної безпеки України

5.1 Вирішувані питання

1. Основні функції системи забезпечення інформаційної безпеки України. Мета функціонування, завдання системи забезпечення інформаційної безпеки.

2. Політика інформаційної безпеки і її реалізація в Законодавстві України. Органи забезпечення інформаційної безпеки і захисту інформації.

3. Методи та заходи забезпечення інформаційної безпеки України.

4. Інформаційна безпека України у сфері прав і свобод людини. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина.

5.2 Основні поняття

Функції системи забезпечення інформаційної безпеки, мета та завдання системи забезпечення інформаційної безпеки, політика інформаційної безпеки, органи захисту інформації, методи забезпечення інформаційної безпеки, права і свободи людини, інформаційні права та свободи.

6. Основи інформаційного протиборства

6.1 Вирішувані питання

1. Інформаційне протиборство, інформаційна експансія, інформаційна війна. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія.

2. Механізми реагування на загрози інформаційній безпеці. Інтернет-ресурси як об’єкти загроз інформаційній безпеці держави. Система моніторингу інтернет-ресурсів.

3. Методики оцінювання загроз інформаційній безпеці у соціальних інтернет-сервісах.

4. Сучасні інформаційні війни. Вплив на інфраструктуру систем життєзабезпечення: телекомунікації, транспортні мережі, електростанції тощо.

5. Промисловий шпіонаж. Хакінг. Кібервійна. Мережева війна. Електронна війна. Психологічна війна. Радіоелектронна боротьба.

6.2 Основні поняття

Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційна акція, інформаційна атака, інформаційна операція,

інформаційна кампанія, інтернет-ресурси, система моніторингу інтернет-ресурсів, соціальні інтернет-сервіси, методики оцінювання загроз, інформаційні війни, вплив на системи життєзабезпечення, кібершпигунство, хакінг, кібервійна, мережева війна, електронна війна, психологічна війна, радіоелектронна боротьба.

7. Основні загрози національній безпеці держави в інформаційній сфері

7.1 Вирішувані питання

1. Загрози національній безпеці України в інформаційній сфері: інформаційний тероризм, комп'ютерна злочинність.
2. Розголошення інформації з обмеженим доступом.
3. Розвідувально-підривна діяльність іноземних спецслужб.
4. Конкурентоспроможність вітчизняної продукції, що обслуговує інформаційну сферу.
5. Шляхи та моделі забезпечення інформаційної безпеки України.

7.2 Основні поняття

Загрози національній безпеці, інформаційний тероризм, комп'ютерна злочинність, інформація з обмеженим доступом, діяльність іноземних спецслужб, конкурентоспроможність вітчизняної продукції, моделі забезпечення інформаційної безпеки.

РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА

Тема: Модель представлення системи інформаційної безпеки держави

1. Методичні вказівки до підготовки РГР

Розрахунково-графічна робота складається з двох частин***: теоретичної та практичної.***

І. В теоретичній частині студент має описати власне бачення процесу моделювання системи інформаційної безпеки держави згідно пропонованого плану.

Орієнтовний план теоретичної частини роботи

1. Поняття моделювання процесів створення та оцінки ефективності системи захисту інформації.
2. Наслідки атак на інформацію. Категорії інформаційної безпеки.
3. Системний підхід у створенні механізмів захисту інформаційних систем.
4. Постановка задачі моделювання процесів створення систем захисту інформації.
5. Модель представлення системи інформаційної безпеки держави, вимоги до моделі.

Обсяг теоретичної частини роботи становить від 8 до 10 аркушів друкованого тексту (поля 2х2х2х2, кегль 14, шрифт Times New Roman, інтервал 1,5). Обсяг вказано без урахування титульної сторінки. Зразок титульної сторінки розміщено в додатках до цих Методичних рекомендацій.

ІІ. В практичній частині роботи студент має навести та описати власну модель представлення системи інформаційної безпеки держави, побудовану з урахуванням законодавства України, чинних нормативно-правових актів, державних стандартів із захисту інформації, інших джерел та сучасної літератури.

Модель представлення може бути наведена у вигляді блок-схеми, схеми, інтелектуальної карти, факторної таблиці, графічного відображення тощо. Для її представлення можна використовувати різноманітне програмне забезпечення, що дозволяє належним чином візуалізувати практичну розробку. Представлення може бути виконане в кольорі або в чорно-білому варіанті.

Наведена модель має супроводжуватись короткою анотацією (описом), обсягом близько 0,5 друкованої сторінки.

III. В кінці Розрахунково-графічної роботи має бути наведений список використаної студентом літератури з україномовних, англомовних джерел та/або інформаційних джерел, представлених мовами Європейського Союзу.

Розрахунково-графічна робота здається в електронному вигляді через систему дистанційного навчання Moodle. Термін здачі РГР повідомляє викладач.

Загалом РГР оцінюється в 15 балів, з яких 10 балів відводиться на оцінку якості підготовки РГР та 5 балів – оцінка за захист РГР. Захист підготовлених та зданих робіт відбудеться орієнтовно через тиждень після спливу терміну здачі, визначеному викладачем.

2. Теоретичні основи моделювання представлення системи інформаційної безпеки держави[*]

Потрібно виокремити проблеми моделювання означених систем, що пов'язані з розкриттям як природи процесу забезпечення інформаційної безпеки, так і з напрямом розробки практичних методів безпеки інформації. При цьому ретельно вивчаються статистика порушень, причини, що їх обумовлюють, особи порушників, сутність прийомів, які використовуються порушниками, обставини, за яких було виявлене порушення (модель порушника інформаційної безпеки держави).

Практичне розв'язання реалізовано частково комплексною системою захисту інформації, де обов'язковими документами, що входять до Плану захисту, є: модель загроз і модель порушника інформаційної безпеки.

Різноманітність моделей та способів моделювання підтверджує безумовну та виняткову цінність дослідження із застосуванням принципів моделювання для держави та для сфери забезпечення інформаційної безпеки.

Моделювання процесів узагальнено передбачає послідовне виконання трьох етапів дослідження. Перший – перехід від вихідної практичної проблеми до постановки теоретичного завдання. Другий – вивчення і вирішення цього завдання. Третій – перехід від висновків за результатами вирішення завдання назад до практичної проблеми.

У сфері моделювання процесів (зокрема діяльності або управління та в інших сферах застосування), доцільно виділити чотири складові, щоб досягнути цілей моделювання: чітка поставка завдання – формулювання прийнятної моделі – застосування підходящого наукового методу дослідження – визначення умов застосовності.

Перший складник моделювання – завдання, як правило, породжено потребами прикладної сфери діяльності. При цьому відбувається одна з

[*] Цитовано за Юлія Кожедуб. Функціональна модель системи забезпечення інформаційної безпеки. Information Technology and Security. July-December 2018. Vol. 6. Iss. 2 (11). DOI: 10.20535/2411-1031.2018.6.2.153488

можливих математичних формалізацій реальної ситуації. Математична формалізація зазвичай дає змогу змоделювати очікувані результати в рамках вибраної моделі й дослідити як вибрана модель може допомогти перевірити гіпотезу, що досліджується.

Завдання може бути породжено також узагальненням потреб ряду прикладних сфер діяльності. Таким чином, одна і та сама сформульована математична модель може застосовуватися для вирішення найрізноманітніших за своєю прикладною сутністю завдань. Важливо підкреслити, що виділення переліку завдань знаходиться поза законами і правилами математики – це перелік вимог технічного завдання, який фахівці різних сфер діяльності надають фахівцям з математичного моделювання для подальшої формалізації.

Вибір методу, який використовується в межах певної моделі, відбувається за законами і правилами математики, тобто йдеться, наприклад, про метод оцінювання, про метод перевірки гіпотези, про метод доказовості теореми. У подальшому розробляються і досліджуються алгоритми щодо практичного застосування і доказовості наведених припущень.

Розглянемо останній елемент четвірки – умови застосовності. Цей елемент використовують для перевірки й опису реальної дійсності процесів, що досліджуються.

Поставлені завдання:

– проаналізувати теоретичні положення основ моделювання для цілей забезпечення інформаційної безпеки;

– показати критерії і умови застосування функціональних моделей для систем забезпечення інформаційної безпеки;

– побудувати модель системи забезпечення інформаційною безпекою держави, а також створену функціональну модель відобразити блок-схемою.

Модель (фр. modèle, у перекладі з лат. modulus – «міра, аналог, зразок») – це система, дослідження якої є засобом для отримання інформації про іншу систему; уявлення деякого реального процесу, пристрою або концепції. Модель є абстрактне уявлення реальності в будь-якій формі (наприклад, в математичній, фізичній, символічній, графічній чи дескриптивній), призначене для подання певних аспектів цієї реальності, що дає змогу отримати відповіді на питання, що досліджуються.

Кількість параметрів, що характеризують поведінку не тільки реальної системи, але і її моделі, дуже значна. Для спрощення процесу вивчення реальних систем виділяють чотири рівні моделей, що розрізняються кількістю і ступенем важливості враховуваних властивостей і параметрів. Це – функціональна, принципова, структурна і параметрична моделі.

Функціональна модель призначена для вивчення особливостей роботи (функціонування) системи і її призначення у взаємозв’язку з внутрішніми та зовнішніми елементами. Функція – найсуттєвіша характеристика будь-якої системи, відображає її призначення, і те, для чого вона потрібна. Подібні моделі оперують, перш за все, з функціональними параметрами. Графічним

представленням цих моделей є блок-схеми. Вони відображають порядок дій, спрямованих на досягнення заданих цілей (так звана “функціональна схема”). Функціональною моделлю є абстрактна модель.

Модель принципу дії характеризує найсуттєвіші (принципові) зв’язки і властивості реальної системи. Це основні фізичні, біологічні, хімічні, соціальні і тому подібні явища, що забезпечують функціонування системи, або будь-які інші принципові положення, на яких базується досліджуваний процес (або планована діяльність). Прагнуть до того, щоб кількість врахованих властивостей і параметрів, що її характеризують, була незначною (залишають найбільш важливі), а прозорість моделі – максимальною, так щоб трудомісткість роботи з моделлю не відволікала увагу від суті досліджуваних явищ. Як правило, описують подібні моделі параметри – функціональні, а також фізичні характеристики процесів і явищ. Принципові вихідні положення (методи, способи, напрямки тощо) покладено в основі будь-якої діяльності або роботи.

Графічним представленням моделей принципу дії слугують: блок-схема, функціональна схема, принципова схема.

Поняття “інформація” (походить від лат. informatio – ознайомлення, пояснення) і на сьогоднішній день є одним із поширених і ключових в різних сфера діяльності. Це пояснюється багатоаспектністю інформації (існуванням в живій і неживій природі, в кібернетичних системах, в суспільстві), різноманітністю її форм проявів в матеріальному світі, особливостями в способах її вивчення і використання різними областями науки і практики.

У визначенні поняття “інформація” в різні роки переважали три основні підходи: недетермінований, техноцентричний і антропоцентричний. Недетермінований підхід до визначення поняття інформації (від лат. determinare – обмежити, визначити) полягає у відмові від тлумачення інформації на тій підставі, що вона є фундаментальним поняттям, яке має необмежені рамки. Один із засновників кібернетики Норд Вінер визначав інформацію як позначення змісту, який отримується нами із зовнішнього світу в процесі пристосування до нього і приведення відповідно до нього нашого мислення. Він стверджував, що: «Інформація є інформація, а не матерія і не енергія». У розвитку цієї ідеї ряд дослідників розглядали інформацію як основу всього існуючого, первинну складову всіх явищ і процесів.

Значення техноцентричного підходу полягає в тому, що інформацію ототожнюють з даними, які мають кількісний вимір (обсяг, швидкість передачі, пропускну здатність каналу). Основоположник теорії інформації Клод Шеннон в 60-х роках XX століття обґрунтував поняття «інформації» як «упорядкованої субстанції, яку можна описати математично: кількість інформації тим більше, чим більше невизначеності усувається при отриманні цієї інформації». Цей підхід і зараз переважає в точних науках і широко застосовується під час розробки та реалізації багатьох, насамперед, апаратно-програмних засобів захисту інформації. Однак в цьому випадку не

розглядається змістовний аспект інформації, що не дає змогу використовувати вказаний підхід до правового регулювання інформаційних відносин.

Зміст антропоцентричного підходу полягає в тому, що інформацію ототожнюють з відомостями або фактами, які теоретично можуть бути отримані і засвоєні, тобто перетворені в знання. Саме цей підхід знайшов широке застосування в юридичній науці і чинному законодавстві. Модель в загальному сенсі (узагальнена модель) створюється з метою отримання і (або) зберігання інформації специфічним об'єктом (у формі уявного образу, опису знаковими засобами або матеріальної системи), що відображає властивості, характеристики та зв'язки об'єкта-оригіналу довільної природи, суттєві для задачі, розв'язуваної суб'єктом. Наприклад, для теорії прийняття рішень найбільш корисні моделі, які виражаються словами чи формулами, алгоритмами і іншими математичними засобами.

Моделі можна поділити на такі види:

1) функціональні моделі – висловлюють прямі залежності між ендогенними і екзогенними змінними (ендогенні змінні – це такі змінні, значення яких визначаються в ході діяльності компонентів (елементів) системи, тобто "всередині" системи. Екзогенні змінні – це змінні, які визначаються або дослідником, або ззовні, тобто в будь-якому випадку діють на систему ззовні);

2) моделі, виражені за допомогою систем рівнянь щодо ендогенних величин;

3) моделі оптимізаційного типу. Основна частина моделі – система рівнянь щодо ендогенних змінних, мета таких моделей – знайти оптимальне рішення для деякого показника;

4) імітаційні моделі – дуже точне відображення досліджуваного явища.

Математична формалізація через це може містити складні, нелінійні, стохастичні залежності. Моделі також можна покласифікувати на керовані і прогнозні. Керовані моделі відповідають на такі питання: "Що буде, якщо ...?", "Як досягти бажаного?", і містять три групи змінних:

1) змінні, що характеризують поточний стан об'єкта;

2) дії, що керують – змінні, що впливають на зміну цього стану і піддаються цілеспрямованому вибору;

3) вихідні дані і зовнішні впливи, тобто параметри, що задаються ззовні, і основні параметри.

У прогнозних моделях керування не виділено явно. Вони відповідають на питання: "Що буде, якщо все залишиться без змін?" Також моделі можна поділити за способом вимірювання часу на безперервні і дискретні. У будь-якому разі, якщо в моделі є наявним час, то модель називається динамічною. Найчастіше в моделях використовується дискретний час, тому що інформація надходить дискретно: звіти, баланси та інші документи складаються періодично, але з формальної точки зору безперервна модель може виявитися більш простою для вивчення.

Особливе місце займають в методології моделювання імітаційні системи. “Будь-яка модель, в принципі, імітаційна, бо вона імітує реальність”, оскільки вона аналізує процес за допомогою варіантних розрахунків. Отже, імітаційна система – це сукупність моделей, що імітують протікання досліджуваного процесу, об’єднана зі спеціальною системою допоміжних програм та інформаційною базою, що дають змогу досить просто й оперативно реалізувати варіантні розрахунки.

Таким чином, під імітацією розуміється чисельний метод проведення машинних експериментів з математичними моделями, що описують поведінку складних систем протягом тривалих періодів часу, при цьому імітаційний експеримент складається з наступних шести етапів: 1) формулювання завдання; 2) побудова математичної моделі; 3) складання програми для ЕОМ; 4) оцінка придатності моделі; 5) планування експерименту; 6) обробка результатів експерименту.

Імітаційне моделювання (simulation modelling) широко застосовується в різних областях, наприклад в економіці. Іншим застосунком може бути теорія ігор (інші назви – теорія конфлікту, або теорія конфліктних ситуацій), що зародилася як теорія раціональної поведінки двох гравців з протилежними інтересами. Теорія ігор є так само імітаційною динамічною моделлю. Вона найбільш проста, коли кожен з гравців прагне мінімізувати свій середній програш, тобто максимізувати свій середній виграш. Звідси ясно, що теорія ігор схильна надмірно спрощувати реальну поведінку в ситуації конфлікту. Учасники конфлікту можуть оцінювати свій ризик за іншими критеріями. За наявності декількох гравців можливі коаліції. Велике значення має стійкість точок рівноваги і коаліцій.

Ще один яскравий приклад застосування імітаційного моделювання – теорія дуополії (інша назва – модель конкуренції двох фірм) О. Курно. Новий поштовх теорії дуополії надано у класичній монографії Дж. Фон Неймана і О.Моргенштейна. У підручниках, присвячених цій теорії зазвичай розбирається “дилема в’язня” і точка рівноваги Неша. Будь-яку організацію можна розглядати як складну систему, для якої практично неможливо отримати єдиний опис процесу її виробничої діяльності, що відповідає на всі питання з точки зору управління, придатного для досягнення всіх ключових цілей і завдань. Будучи за своєю природою багатогранною за формами і змістом уявлення, організація як сукупність взаємопов’язаних компонентів може бути описана у вигляді цілого ряду самостійних, закінчених “проекцій”, кількість яких визначається головним чином цілями управління.

Наприклад, одна і та сама організація може бути представлена:

– деревом процесів, за допомогою яких організація виконує свою місію;

– сукупністю джерел і каналів зв’язку, потоків інформації і типів даних;

– організаційною структурою;

– інфраструктурою (території, будівлі, споруди, комунікації).

Кожна організація (як система) створюються для того, щоб створювати додану вартість (отримувати прибуток), тому визнано, що для загального

керівництва ключовою метою є представлення об’єкта у вигляді мережі процесів, що визначають його місію. Такі процеси прийнято називати бізнес-процесами. Саме уявлення (моделювання) об’єкта у вигляді набору бізнес-процесів визначає всі інші його “проекції”.

Подібні системи завжди ґрунтуються на проведенні глибокого передпроектного обстеження діяльності організації. Результатом цього обстеження є експертний висновок, в якому окремими пунктами виносяться рекомендації щодо усунення вразливостей в управлінні діяльністю. На підставі цього висновку, безпосередньо перед проектом впровадження системи автоматизації, проводиться так звана реорганізація бізнес-процесів. Подібні комплексні обстеження організацій завжди є складними і істотно відрізняються один від одного завданнями. Процес опису об’єкта моделювання (системи) для цілей загального керівництва починають з опису процесів, що визначають цільове призначення, і продовжують до досягнення необхідного ступеня “прозорості”, достатнього для коректного аналізу і вироблення ефективних управлінських рішень.

Моделювання завжди передбачає прийняття припущень щодо ступеня важливості досліджуваного явища, процесу, системи. При цьому повинні задовольнятися такі вимоги до моделей:

– адекватність, тобто відповідність моделі вихідній реальній системі і врахування, перш за все, найбільш важливих якостей, зв’язків і характеристик. Оцінити адекватність вибраної моделі, особливо, наприклад, на початковій стадії проектування, коли вид системи, що створюється, ще невідомий, дуже складно. У такій ситуації часто покладаються на досвід попередніх розробок або застосовують методи, наприклад, послідовних наближень;

– точність, тобто ступінь збігу отриманих в процесі моделювання результатів із заздалегідь встановленими, бажаними. Тут важливим завданням є оцінка потрібної точності результатів і наявної точності вихідних даних, узгодження їх як між собою, так і з точністю використовуваної моделі;

– універсальність, тобто можливість застосування моделі до аналізу ряду однотипних систем в одному або декількох режимах функціонування. Це дозволяє розширити область застосовності моделі для вирішення більшого кола завдань;

– доцільна економічність, тобто точність одержуваних результатів і спільність рішення задачі повинні ув’язуватися з витратами на моделювання. І вдалий вибір моделі, як показує практика,

– результат компромісу між відпущеними ресурсами і особливостями використовуваної моделі.

Моделювання систем забезпечення інформаційної безпеки дає змогу визначити необхідні і достатні умови її захищеності. Організаційні питання відіграють важливу роль під час розробки технічних аспектів захисту інформації й окремих її компонентів.

Під час розробки системи забезпечення інформаційної безпеки доцільно пам’ятати, що абсолютна захищеність інформації неможлива, отже необхідно

оцінити ступінь ризику інформаційної безпеки. Під час переходу до експлуатації системи забезпечення інформаційної безпеки необхідно підтримувати заданий рівень її захищеності.

Ключовою фігурою в теорії захисту інформації є порушник, його практичні і теоретичні можливості, апріорні знання, час і місце дій. При синтезі системи забезпечення інформаційної безпеки необхідно відповісти на питання:

– якою має бути структура;

– які функції є обов'язковими;

– які тактика і стратегія щодо порушників, фактів порушень та їх наслідків.

Міжнародний стандарт (International Organization for Standardization. ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary [Online]. Available: https://www.iso.org/standard/73906.html) визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації». Тоді як міжнародний стандарт (International Organization for Standardization. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements [Online]. Available: https://www.iso.org/standard/54534.html) – це перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації організації, яка запровадила систему менеджменту інформаційної безпеки, а сам стандарт є настановою щодо впровадження.

Моделювання найбільш ефективно, коли дослідник має справу з добре структурованими проблемами, коли достатньо інформації для оцінки ситуацій і проблем, а також наявна відпрацьована методологія роботи з моделями. Найбільш відомими труднощами використання моделей у дослідженні систем управління є дуже висока вартість, недостовірна початкова інформація про об'єкт, надмірне спрощення характеристик, помилки в методології моделювання. Нові задачі застосування інформаційної системи дають змогу розгортати інформаційні процеси в бік обробки транзакцій і зв'язків між ними.

Функціональна модель – це система пов'язаних систем. Склад функціональної моделі істотно залежить від контексту конкретної системи і її може бути представлено за допомогою досить широкого спектра документів у вигляді текстової і графічної інформації.

ДОДАТКИ

1. Класифікація загроз безпеки

Класифікаційна ознака	***Класифікаційні групи***
За джерелом загрози	1) внутрішні — джерело на території України; 2) зовнішні — джерело розташоване за кордоном Держави
За природою виникнення загроз	1) викликані політикою держави; 2) ініційовані іноземними державами; 3) що надходять від кримінальних структур; 4) що надходять від конкурентів або контрагентів
За ймовірністю реалізації	1) реальні — можуть здійснюватися в будь-який момент часу; 2) потенційні — можуть реалізуватися у разі формування певних умов
Стосовно людської діяльності	1) об'єктивні — формуються незалежно від цілеспрямованої діяльності; 2) суб'єктивні — створюються свідомо, наприклад, розвідувальною, підривною й іншою діяльністю, організованою злочинністю
За об'єктом зазіхання	1) на інформацію; 2) на майно; 3) на фінанси; 4) на персонал; 5) на ділове реноме
За можливістю прогнозування	1) що прогнозуються на рівні господарюючого суб'єкта; 2) що не піддаються прогнозу
За наслідками	1) загальні — відбуваються на всій території України або більшості її суб'єктів; 2) локальні — мають вплив на окремі об'єкти
За величиною нанесеного (очікуваного) збитку	1) катастрофічні; 2) значні; 3) що спричиняють труднощі

2. Ієрархічна класифікація загроз інформаційній безпеці

Критерії загрози	*Вид загрози*
За видом властивості інформації, що порушується	Загрози конфіденційності (витік, перехват, зняття, копіювання, викрадання, розголошення) Загрози цілісності (втрата, знищення, модифікація) Загрози доступності (блокування)
За характером порушення	Порушення конфіденційності даних Порушення працездатності серверів, мережевого обладнання, робочих станцій Незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій тощо.
За тяжкістю порушення	Незначні помилки Дрібне хуліганство Серйозний злочин Природні і техногенні катастрофи
За умислом порушника	Умисне порушення Необережне порушення
За мотивацією	Корисливе Хуліганське З особистих мотивів тощо
За закінченістю	Закінчені Не закінчені
За об’єктом дії	Загрози, націлені на всю інформаційну систему Загрози, націлені на окремі компоненти СУ КСП
За причиною виникнення	Загрози, що виникли через нестачу засобів ТЗІ Загрози, що виникли через нестачу організаційних засобів
За походженням	Антропогенні Техногенні Природні
За розміром нанесеної шкоди	Незначні Значні Критичні
За типовими об’єктами інформатизації	Загрози безпеці інформації для СУ на базі автономної ЕОМ (без підключення до обчислювальної мережі) Загрози безпеці інформації для СУ на базі локальної обчислювальної мережі (без підключення до розподіленої обчислювальної мережі) Загрози безпеці інформації для СУ, підключеної до розподіленої обчислювальної мережі
За способом реалізації загроз безпеці інформації	Загрози спеціальної дії на інформацію: механічної, хімічної, акустичної, біологічної, радіаційної, термічної, електромагнітної (електричні імпульси, електромагнітне випромінювання, магнітне поле) Загрози НСД в СУ КСП Загрози витоку інформації технічними каналами: по радіоканалу, по електричному каналу, по оптичному каналу, по змішаним (параметричним) каналам; загрози витоку по каналам ПЕМВН

3. Категорійно-понятійна система інформаційної безпеки

Інформаційна безпека — складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

Інформаційні відносини — відносини, які виникають у всіх сферах життя і діяльності людини, суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційний суверенітет — здатність держави контролювати і регулювати потоки інформації поза межами держави з метою додержання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційний простір (національний):

1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави;

2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

Інформаційна інфраструктура **–** сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісного обслуговування інфраструктури і системи підготовки кадрів.

Інформаційна система **–** організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційні ресурси:

1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави у певній сфері життя чи діяльності.

Інформаційні технології:

1) цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

2) цілеспрямовано організована сукупність інформаційних процесів для створення і використання інформаційних продуктів або надання інформаційних послуг;

3) технологічний процес, предметом перероблення й результатом якого е інформація;

4) процес матеріалізації знань у продукцію і послуги за допомогою комп'ютерно-телекомунікаційних систем;

5) система методів і способів використання комп'ютерної техніки та систем зв'язку для створення, пошуку, одержання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформаційних продуктів.

Інформаційне середовище **–** усталене поєднання окремих суб'єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах.

Інформаційний ринок – система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

Інформаційний продукт (продукція):

1) документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

2) документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена чи застосовується для задоволення потреб користувачів;

3) створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційне забезпечення – підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь-якої іншої діяльності у всіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційне поле:

1) сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту;

2) просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

Інформаційне суспільство:

1) суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми — знань;

2) суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інформатизація:

1) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

2) діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства інформаційних технологій.

Інформатика – наукова діяльність, що вивчає інформаційні структури та процеси збирання (набуття, придбання), відображення, реєстрації, накопичення, збереження і поширення (розповсюдження, реалізацію) інформації за допомогою ЕОМ.

Інформаціологія **–** новітня загальна фундаментальна наука про інформаційні природні процеси матеріалізації та дематеріалізації в мікро- й макроструктурах Всесвіту, що самоорганізуються.

Інформація:

1) документовані або публічно проголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі;

2) відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, та навколишньому природному середовищі, незалежно від форми їх представленнями) будь-які знання про предмети, факти, поняття і т. ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

Інформаційна війна **–** процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя **–** засоби, які дозволяють вчинювати замислені дії із повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

Інформаційна загроза **–** вхідні дані, початково призначені для активізації в інформаційній системі алгоритмів, що відповідають за звичайний режим функціонування.

4. Титульна сторінка РГР

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

П І П

РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА

з дисципліни «Інформаційна безпека держави»

на тему: «Модель представлення системи інформаційної безпеки держави»

Курс І Група КБ-23_

Перевірила:
к.ю.н., доц. Ларченко М.О.

Оцінка _____

Чернігів – 2024

Джерела та література для підготовки до практичних занять та написання розрахунково-графічної роботи

1. Аналіз вразливостей корпоративних інформаційних систем / Д.Б. Мехед, Ю.М. Ткач, В.М. Базилевич, В.І. Гур'єв, Я.Ю. Усов // Захист інформації. Ukrainian Information Security Research Journal. – 2018. – №1. – С. 61–66.

2. Андріяш В. І. Державна політика: концептуальні аспекти визначення. URL: http://www.dy.nayka.com.ua/?op=1&z=626

3. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,;// Гол. ред. Ю. О. Шпак. - К.: "МК-Прес", 2015. - 432 с.

4. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.— 288 с.

6. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). URL: http://www.cbz.com.ua/

7. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD). URL: https://web.archive.org/web/20160304091010/http:/www.cbz.com.ua/resources/files/8510076024d22f2d964df2.pdf

8. Доктрина інформаційної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

9. Забезпечення інформаційної безпеки держави: Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.

10. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

12. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

13. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

14. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є.Забезпечення інформаційної безпеки держави Є.В. Іванченко [та ін.] ; за ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.

15. Інформаційна безпека держави: підручник / [В.М. Петрик. М.М. Присяжнюк., Д.С. Мельник та ін.]; в 2 т. Т. 1. / за заг. ред. В.В. Остроухова - К.: ДНУ «Книжкова палата України». 2016. 264 с.

16. Климчук О. О. Забезпечення інформаційної безпеки держави : підручник / [О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.] ; за заг.ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України», 2015. – 672 с.

17. Климчук О. О. Забезпечення інформаційної безпеки у провідних країнах світу : навч. посіб. / [О. О. Климчук, Д. С. Мельник, В. М. Панченко, В.М. Петрик та ін.] ; за заг. ред. В. М. Петрика. – К. : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. – 260 с.

18. Конституція України: прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

19. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1020

20. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. URL: http://www.dut.edu.ua/uploads/l_1023_75718671.pdf

21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1032

22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1030

23. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1031

24. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1050

25. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1036

26. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. URL: http://www.dut.edu.ua/ua/lib/1/category/919/view/1037

27. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: http://www.dut.edu.ua/uploads/l_1057_37661772.pdf

28. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та

інформаційно-телекомунікаційних системах» від 29.03.2006 №373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%EF#Text

29. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF-%EF

30. Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://www.president.gov.ua/documents/6852021-41069

31. Технічне завдання на створення автоматизованої системи. ГОСТ 34.602-89. URL: https://www.rts.ua/rus/forpro/613/0/17/

32. Про План реалізації Стратегії кібербезпеки України URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

33. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

34. Остроухов В.В., Присяжнюк М.М., Фермагей О.І., Чеховська М.М. Інформаційна безпека. Підручник. К.: Ліра-К. 2021. 412с.

35. Бобала Ю.Я., Горбатий І. В. Інформаційна безпека. Навчальний посібник / за ред. Ю. Я. Бобала та І. В. Горбатого. Л.: Видавництво Львівської політехніки. 2019 р. - 580 с.

36. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. Київ: BAITE, 2021. 106 с.

37. 2021 International Conference on Applications and Techniques in Cyber Intelligence Applications and Techniques in Cyber Intelligence (ATCI 2021) Volume 2

38. Effective Cybersecurity Operations for Enterprise-Wide Systems Festus Fatai Adedoyin Bournemouth University, UK Bryan Christiansen CYGERA, LLC, USA. 2023. 344 p.

39. Emerging Security Algorithms and Techniques. Edited by Khaleel Ahmad, M. N. Doja, Nur Izura Udzir, and Manu Pratap Singh. CRC Press Taylor & Francis Group. New York. 2019. 331 p.

40. Izzat Alsmadi, Chuck Easttom, Lo'ai Tawalbeh. The NICE Cyber Security Framework. Cyber Security Management. Springer Nature. Switzerland AG 2020. 271 p.

41. Bella Anderson. Cybercrime Criminal Threats from Cyberspace. Cybercrime. White Press Academic. 2018. 309 p.

42. Cyber Investigations. A Research Based Introduction for Advanced Studies. Edited by André Årnes. Norwegian University of Science and Technology (NTNU). 2023 John Wiley & Sons Ltd. 272 p.

43. Babak Akhgar, Andrew Staniforth, Francesca Bosco. Cyber Crime and Cyber Terrorism. Investigator's Handbook. USA. 2023. 435 p.

44. Noah Crawley. Cybersecurity: Guide To Learning The Basics Of Information Security And Discover The Best Strategies For Defense Your Devices (Including Social Engineering, Ethical Hacking, Risk Assessment). 2021. 148 p.