МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ім. ІВАНА ФРАНКА
ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ
КАФЕДРА КІБЕРБЕЗПЕКИ

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри Петро ВЕНГЕРСЬКИЙ

ПРОГРАМА
виробничої (переддипломної) практики

для студентів 4-го курсу освітнього ступеня «бакалавр»

спеціальності 125 «Кібербезпека та захист інформації»

2023

Робоча програма виробничої (переддипломної) практики студентів 4 курсу освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека та захист інформації». – 13 стор.

Розробники програми: Венгерський П.С., д.фіз-мат.н., проф. кафедри Кібербезпеки

Робоча програма затверджена на засіданні кафедри кібербезпеки.

Протокол № 15/23 від “28” серпня 2023 року.

ВСТУП

Практика студентів є однією із основних форм навчального процесу, спрямованих на формування і виховання висококваліфікованих фахівців.

Основним навчально-методичним документом, що визначає проведення виробничої (переддипломної) практики й регламентує навчальну діяльність студентів та роботу викладача, є робоча програма виробничої (переддипломної) практики.

Дана програма забезпечує комплексний підхід до організації практичної виробничої підготовки, системності, неперервності й послідовності навчання студентів та є основою для розроблення завдань виробничої (переддипломної) практики, що враховують особливості баз виробничої (переддипломної) практики та конкретні умови її проходження.

Бази виробничої (переддипломної) практики обираються кафедрою кібербезпеки (КБ) згідно до вимог освітньо-кваліфікаційної характеристики бакалавра з спеціальності 125 «Кібербезпека та захист інформації». Студенти можуть самостійно, з дозволу кафедри, підбирати для себе місце проходження виробничої (переддипломної) практики та пропонувати його для використання.

Базами виробничої (переддипломної) практики можуть бути адміністративні та виробничі відділи або служби підприємств промисловості, науково-дослідних, проектних, комп'ютерних центрів, комерційних, банківських та інших. За потреби виробнича (переддипломна) практика може проводитись на кафедрі КБ. Місце виробничої (переддипломної) практики вказується у договорі, що оформляється на кафедрі КБ, які видаються кожному студенту керівником виробничої (переддипломної) практики від університету.

Навчальним планом підготовки бакалавра передбачено проведення виробничої (переддипломної) практики у 8-му семестрі терміном 2 тижні. На практику направляються студенти, які не мають академічної заборгованості.

1. Мета і завдання виробничої «переддипломної» практики

Метою виробничої «переддипломної» практики є узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профілюючими дисциплінами, що вивчені, за спеціальністю 125 «Кібербезпека та захист інформації», отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз та розроблення плану кіберзахисту інформаційної системи.

Завдання переддипломної практики:

1. Ознайомлення з діяльністю бази виробничої (переддипломної) практики та її підрозділів, з посадовими обов'язками інженерно-технічних працівників підрозділів.
2. Ознайомлення з комплексною системою забезпечення інформаційної

безпеки і захисту інформації підприємства.

3. Вивчення нормативної бази, що регулює забезпечення інформаційної безпеки і захисту інформації, що використовується та обробляється даним підприємством.
4. Поглиблення та закріплення теоретичних знань з фахових дисциплін.
5. Опрацювання наукової, періодичної літератури й методичних матеріалів з питань, що розробляються студентом у кваліфікаційній роботі.

6. Вивчити на практиці сучасні методи реалізації несанкціонованого доступу (НСД) та захисту інформації від стороннього впливу.

7. Вивчити специфіку інформаційного потоку конкретного об'єкта управління що підлягає захисту.

8. Розробити вимоги щодо захисту інформації об'єкта управління від НСД.

9. Проаналізувати сучасні існуючі засоби захисту інформації в інформаційно-комунікаційних системах (ІКС) від витоку її технічними каналами.

10. Розробити вимоги щодо використання засобів захисту інформації в ІКС від витоку її технічними каналами за об'єктом управління.

Компетентності, які формуються у здобувачів освіти, відповідно до виробничої (переддипломної) практики.

Інтегральна компетентність

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності:

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- комунікацтйних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники в інформаційному просторі та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання.

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
ПРН 11.Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі,

сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- 11 телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
ПРН 36. Виявляти небезпечні сигнали технічних засобів;
ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

2. Організація і керівництво виробничою (переддипломною) практикою

2.1. Терміни проведення, тривалість. Виробнича (переддипломна) практика для студентів спеціальності 125 «Кібербезпека та захист інформації» ОПП «Кібербезпека» проводиться в час, визначений навчальним планом, а саме: Виробнича (переддипломна) практика триває два тижні наприкінці восьмого семестру. Обсяг НД 38 Виробнича (переддипломна) практика – 3 кредити ЄКТС.

2.2. База практики. Базою виробничої (переддипломної) практики може бути підприємство, організація або установа, що має у своєму складі підрозділи, які здійснюють забезпечення інформаційної безпеки та/або кібербезпеки підприємства.

Студентам надається можливість самостійно обрати базу виробничої (переддипломної) практики. В якості такої, наприклад, може бути використана

організація, в якій вони вже працюють. У цьому випадку здобувач подає на кафедру офіційного листа від організації з проханням/згодою прийняти його на виробничу (переддипломну) практику. Розподіл студентів, які не представили у встановлений термін дані про проходження виробничої (переддипломної) практики, здійснюється з урахуванням наявних можливостей і вимог конкретних місць виробничої (переддипломної) практики до рівня підготовки студентів.

2.3. Керівництво виробничою (переддипломною) практикою. Виробничою (переддипломною) практикою керують спільно керівник виробничої (переддипломної) практики від факультету, керівник виробничої (переддипломної) практики від кафедри і керівник від бази виробничої (переддипломної) практики. Керівник від факультету забезпечує загальну організацію проведення виробничої (переддипломної) практики і координує роботу керівників виробничої (переддипломної) практики від кафедр. Керівників виробничої (переддипломної) практики від кафедр призначає завідувач кафедри з числа досвідчених викладачів. Вони здійснюють методичне керівництво роботою практикантів, консультують студентів з питань виконання програми виробничої (переддипломної) практики, формулюють висновок про звіти студентів про проходження виробничої (переддипломної) практики і беруть участь у роботі комісії по захисту звіту з виробничої (переддипломної) практики. Керівник виробничої (переддипломної) практики від бази призначається з числа працівників підприємства чи установи адміністрацією бази виробничої (переддипломної) практики. До його обов'язків входить:

- допомога при оформленні на виробничу (переддипломну) практику, проведення інструктажу з техніки безпеки і охорони праці;
- забезпечення практикантів робочими місцями;
- формулювання індивідуального завдання на виробничу (переддипломну) практику і його погодження з керівником від кафедри;
- контроль за роботою студентів-практикантів і за дотриманням ними трудової дисципліни;
- контроль за веденням щоденників, перевірка звіту і підготовка відгуку з оцінкою про виробничу (переддипломну) практику студента.

3. Права і обов'язки студентів у період виробничої (переддипломної) практики

На студентів, які проходять виробничу (переддипломну) практику на підприємстві (організації, установі), розповсюджується законодавство України про працю та правила внутрішнього розпорядку підприємства (організації, установи).

Тривалість робочого часу студентів під час проходження виробничої (переддипломної) практики регламентується законодавством України про працю. За наявності вакантних місць студенти можуть бути зараховані на штатні посади, якщо робота на них відповідає вимогам програми виробничої (переддипломної) практики. При цьому не менше половини робочого часу відводиться на загально-професійну підготовку за програмою виробничої (переддипломної) практики.

Студент-практикант зобов'язаний:

- повністю виконувати завдання, передбачені програмою і календарним планом виробничої (переддипломної) практики, нести відповідальність за виконувану роботу та її результати;
- строго дотримуватись діючих на базі виробничої (переддипломної) практики правил внутрішнього трудового розпорядку, правил охорони праці, техніки безпеки і виробничої санітарії;
- вести регулярні записи в щоденнику про характер виконаної роботи і надавати його для перевірки керівнику від бази виробничої (переддипломної) практики;
- у 5-денний термін після завершення виробничої (переддипломної) практики надати керівнику практики від кафедри письмовий звіт про виконання всіх завдань і захистити його.

При порушенні студентом трудової дисципліни він може бути усунутий від проходження практики за поданням керівника виробничої (переддипломної) практики від бази або від кафедри. Студент, який не виконав програму виробничої (переддипломної) практики, або отримав негативний відгук керівника від бази виробничої (переддипломної) практики, або незадовільну оцінку на захисті, вважається таким, що не виконав навчального плану поточного семестру.

4. Зміст виробничої (переддипломної) практики

Під час проходження виробничої (переддипломної) практики студентами належить вирішити такі завдання.

- Ознайомитися із структурою підприємства. Вивчити організацію і управління діяльністю відповідного підрозділу чи підприємства в цілому.
- Вивчити технологічні процеси і виробниче обладнання бази виробничої (переддипломної) практики.
- Вивчити основні законодавчі документи, що регламентують порядок написання кваліфікаційної роботи (порядок оформлення, відповідальність за плагіат).
- Зібрати матеріал, організувати та виконати наукове дослідження за обраною темою кваліфікаційної роботи.
- Виконати огляд літературних джерел за темою дослідження.

- Оформити власні результати, отримані в межах роботи над кваліфікаційною роботою. Підготувати матеріали до захисту кваліфікаційної роботи.
- Оформити звіт про виробничу (переддипломну) практику.

Робота в структурному підрозділі.

Дослідження об'єкта діяльності структурного підрозділу. Аналіз матеріальних та інформаційних потоків і їх взаємодії.

Вивчення процесів збирання, накопичення й оброблення даних у межах структурного підрозділу.

Аналіз інформаційних потреб користувачів підрозділу.

Детально вивчаються: основні положення, адміністративно-правова база, що визначає задачі, функції, структуру виробничої системи, всі типи документів та інструкцій, що циркулюють у системі. Проводяться бесіди з керівниками та фахівцями підрозділів.

Виконання завдань від бази виробничої (переддипломної) практики.

Керівник від бази виробничої (переддипломної) практики визначає завдання для виконання під час проходження виробничої (переддипломної) практики. Завдання повинно стосуватися забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки, забезпечення безпеки Web ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження, забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації, застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації тощо.

5. Документація про проходження виробничої (переддипломної) практики.

До переліку документів, необхідних для успішного захисту виробничої (переддипломної) практики, входять:

- договір, укладений між університетом і базою виробничої (переддипломної) практики;
- щоденник виробничої (переддипломної) практики;
- відгук про виробничу (переддипломну) практику студента від бази практики;
- звіт про виробничу (переддипломну) практику з результатами виконаної роботи.

5.1. Вимоги до оформлення щоденника виробничої (переддипломної) практики.

Під час перебування на виробничій (переддипломній) практиці студент веде щоденник. У ньому формулюють індивідуальне завдання на виробничу

(переддипломну) практику, складають графік її проходження і фіксують основні види виконуваних робіт. Індивідуальні завдання розробляють спільно керівники від бази виробничої (переддипломної) практики і від кафедри, після чого їх затверджує завідувач кафедри. Студент складає графік проходження виробничої (переддипломної) практики і погоджує його з керівником від бази практики. Всі види виконуваних на виробничій (переддипломній) практиці робіт студент записує у щоденник, а факт їх виконання засвідчується підписом керівника від бази.

Після завершення виробничої (переддипломної) практики студент здає заповнений щоденник керівнику виробничої (переддипломної) практики від кафедри.

5.2. Вимоги до змісту і оформлення звіту з практики. Після завершення виробничої (переддипломної) практики студент складає звіт і здає його разом зі щоденником керівнику виробничої (переддипломної) практики від кафедри.

Звіт повинен містити наступні структурні елементи:

- титульний лист;
- зміст;
- вступ;
- основну частину;
- висновки;
- перелік використаних джерел;
- додатки.

Титульний лист є першою сторінкою звіту.

Зміст включає назви всіх розділів і підрозділів із вказанням номерів сторінок, на яких міститься початок матеріалів розділів і підрозділів

У вступі визначаються мета і завдання виробничої (переддипломної) практики, наводиться коротка характеристика бази виробничої (переддипломної) практики.

Основна частина містить звіт про конкретно виконану роботу за період виробничої (переддипломної) практики. Зміст цього розділу повинен відповідати індивідуальному завданню і вимогам програми виробничої (переддипломної) практики.

У висновках студент повинен підсумувати результати виробничої (переддипломної) практики, внести пропозиції щодо вдосконалення роботи досліджуваного об’єкта. Перелік використаних джерел оформляють згідно з прийнятими стандартами.

5.3. Відгук бази виробничої (переддипломної) практики. Відгук про проходження студентом виробничої (переддипломної) практики оформляють за зразком, наведеним у додатку. Його підписує керівник від бази виробничої

(переддипломної) практики, завіряє печаткою бази виробничої (переддипломної) практики і передає керівнику виробничої (переддипломної) практики від кафедри разом зі звітом та щоденником виробничої (переддипломної) практики. Відгук обов'язково повинен містити оцінку (від 0 до 50 балів) результатів виробничої (переддипломної) практики студента.

6. Захист і оцінювання результатів виробничої (переддипломної) практики

Після проходження виробничої (переддипломної) практики студенти у 5-денний термін після офіційної дати її завершення подають на кафедру щоденник виробничої (переддипломної) практики, звіт і відгук бази виробничої (переддипломної) практики.

Звіт попередньо оцінює керівник виробничої (переддипломної) практики від кафедри і допускає до захисту після перевірки його відповідності вимогам даного положення.

Для захисту звітів створюється комісія(ї), в яку(і) входять керівники виробничої (переддипломної) практики від кафедри – не менше трьох осіб. Процес захисту передбачає визначення комісією рівня оволодіння студентом практичними навиками роботи і рівня застосування на практиці отриманих під час навчання в університеті теоретичних знань.

До захисту студенти готують короткі (5-10 хв.) виступи та необхідний ілюстративний матеріал.

Для оцінювання результатів виробничої (переддипломної) практики беруть до уваги кількісні і якісні показники виконання студентом завдань виробничої (переддипломної) практики, повноту, грамотність, правильність оформлення звітної документації та відгук, наданий керівником від бази виробничої (переддипломної) практики.

Роботу студента оцінюють за 100-бальною шкалою (відповідно до Положення про контроль та оцінювання навчальних досягнень здобувачів вищої освіти Львівського національного університету імені Івана Франка). Підсумкову оцінку визначають як суму наступних трьох складових:

1) оцінки проходження виробничої (переддипломної) практики керівником практики від бази (0-50 балів);
2) оцінки змісту і оформлення звітної документації (0-25 балів);
3) оцінки захисту звіту з виробничої (переддипломної) практики (0-25 балів).

Література

1. Положення про проведення практики студентів вищих навчальних закладів. України Електронний ресурс] — Режим доступу : https://zakon.rada.gov.ua/laws/show/z0035-93#Text
2. Положення про проведення практик здобувачів вищої освіти Львівського національного університету імені Івана Франка https://lnu.edu.ua/about/university-today-and-tomorrow/documents/education-process/
3. Основні вимоги до написання та оформлення кваліфікаційних робіт. Методичні рекомендації ЛНУ ім.Івана Франка, ФПМІ. – 2023. -28 с. https://ami.lnu.edu.ua/wp-content/uploads/2023/02/MasterThesis2023.pdf
4. Гаврилко Є.В., Жебка В.В. Методологія та організація проведення наукових досліджень. – К.: ДУТ, 2019. – 200 с..
5. Данильян О.Г. Методологія наукових досліджень : підручник / О. Г. Данильян, О. П. Дзьобань. – Харків : Право, 2019. – 368 с.
6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
7. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
8. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

9.НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

10.НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

11.НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

12.НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

13.НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

14.НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

15.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

16.НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.