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 № 9/24 від 29 серпня 2024 р.)

Завідувач кафедри Петро ВЕНГЕРСЬКИЙ

НАСКРІЗНА РОБОЧА ПРОГРАМА ПРАКТИКИ

здобувачів вищої освіти другого (магістерського) рівня

ОПП «Технології штучного інтелекту в кібербезпеці»
спеціальності 125 «Кібербезпека та захист інформації»

2024

Наскрізна робоча програма практики студентів другого освітнього (магістерського) рівня спеціальності 125 «Кібербезпека та захист інформації». – 18 стор.

Розробники програми: Венгерський П.С.., д.фіз-мат.н., в.о. завідувача кафедри кібербезпеки

Робоча програма затверджена на засіданні кафедри кібербезпеки.

Протокол № 9/24 від “29” серпня 2024 року.

ВСТУП

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

Наскрізна програма практики здобувачів вищої освіти є основним навчально-методичним документом, який визначає порядок проведення виробничих практик у першому та другому роках навчання.

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

Практику проводять на оснащених відповідним чином базах навчального закладу, підприємств і організацій, які розробляють і використовують сучасне програмне забезпечення. Бази практики обираються кафедрою кібербезпеки (КБ) згідно до вимог освітньо-кваліфікаційної характеристики магістра з спеціальності 125 «Кібербезпека та захист інформації». Студенти можуть самостійно, з дозволу кафедри, підбирати для себе місце проходження практики та пропонувати його для використання.

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

Вона є одним з важливих етапів формування фахівця, здатного самостійно вирішувати конкретні завдання в діяльності установ та організацій різних форм власності, а також джерелом матеріалів для курсової роботи (яку виконують упродовж першого року навчання) та випускної кваліфікаційної (магістерської) роботи.

Розроблена програма покликана забезпечити системність, єдиний комплексний підхід до організації практичної підготовки, неперервність і наступність навчання студентів, органічне поєднання з практичними й лабораторними заняттями для отримання студентами достатнього обсягу практичних знань і умінь відповідно до освітнього ступеня «магістр».

1. Мета і завдання практики

Метою проєктної практики є систематизація, розширення професійних знань у сфері обраної спеціальності, формування і розвиток в магістрантів навичок до самостійної наукової праці, проведення досліджень і експериментів, закріплення отриманих теоретичних знань за дисциплінами напряму і спеціальним дисциплінам магістерських програм.

Метою переддипломної практики є узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профілюючими дисциплінами, що вивчені, за спеціальністю ″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, виховання потреби систематично поновлювати свої знання та творчо застосовувати їх у практичній діяльності.

Основними завданнями проєктної практики є:

- поглиблення та закріплення теоретичних знань з фахових дисциплін;
- вивчення на практиці сучасних методів реалізації несанкціонованого доступу (НСД) та захисту інформації від стороннього впливу та застосування сучасних існуючих засобів захисту інформації;
- ознайомлення з організацією виробничого процесу на підприємствах різних форм власності;
- набуття досвіду виконання виробничих і/або дослідницьких робіт на підприємствах і установах;
- збір необхідних матеріалів для підготовки і написання курсової роботи та кваліфікаційної роботи;
- формування професіональної позиції, світогляду, стилю поведінки і засвоєння професійної етики.

Основними завданнями виробничої (переддипломної) практики є:

- зібрати матеріал за темою кваліфікаційної роботи для оцінювання стану системи захисту об′єкта управління;
- вивчити на практиці сучасні методи реалізації несанкціонованого доступу (НСД) та захисту інформації від стороннього впливу.
- вивчити специфіку інформаційного потоку конкретного об'єкта управління що підлягає захисту.
- розробити вимоги щодо захисту інформації об'єкта управління від НСД.
- проаналізувати сучасні існуючі засоби захисту інформації в інформаційно-комунікаційних системах (ІКС) від витоку її технічними каналами.
- 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 практики.

Проєктна практика, перший рік навчання.

Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Здатність проводити дослідження на відповідному рівні.

ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки

Виробнича (переддипломна) практика, другий рік навчання.

Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Здатність проводити дослідження на відповідному рівні.

ЗК 3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові компетентності:

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки

КФ11. Здатність використовувати технології та засоби штучного інтелекту для виявлення вразливостей та захисту інформаційних ресурсів об’єктів інформаційної діяльності та критичної інфраструктури, швидкого аналізу аномалій, загроз та реагування на них.

Програмні результати навчання, відповідно до практики.

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі, зокрема з вкиористанням технологій, методів, інструментів штучного інтелекту.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення, та штучного інтелекту. *(тільки ОК6)*

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення та методів інтелектуальної автоматизації, штучного інтелекту і машинного навчання для виявлення поведінкових аномалій і усунення загроз.*(тільки ОК5)*

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки та штучного інтелекту. *(тільки ОК5)*

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. *(тільки ОК6)*

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. *(тільки ОК5)*

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. *(тільки ОК6)*

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. *(тільки ОК5)*

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки, штучного інтелекту і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки та штучного інтелекту. *(тільки ОК6)*

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. *(тільки ОК6)*

РН24. Ідентифікувати, виявляти та впроваджувати адаптивні інтелектуальні системи для виявлення вразливостей, розпізнавання аномальних активностей та ефективного реагування на кібератаки; розробляти та вдосконалювати моделі машинного навчання, які сприяють підвищенню рівня кібербезпеки, забезпечуючи надійний захист цифрових систем та даних від потенційних загроз. *(тільки ОК6)*

2. Організація і керівництво практикою

2.1. Терміни проведення, тривалість. Практика для студентів спеціальності 125 Кібербезпека та захист інформації ОПП «Технології штучного інтелекту в кібербезпеці» проводиться в час, визначений навчальним планом, а саме: ОК 5 Проєктна практика – впродовж першого та другого

семестрів без відриву від навчання; ОК 6 Виробнича (переддипломна) практика триває чотири тижні наприкінці третього семестру з десятого по тринадцятий тижні включно.

Обсяг ОК 5 Проєктна практика – 9 кредитів ЄКТС, обсяг ОК 6 Виробнича (переддипломна) практика – 6 кредитів ЄКТС.

2.2. База практики. Основним базовим об'єктом проєктної практики є кафедра кібербезпеки та лабораторії університету, 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 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 практику. Розподіл студентів, які не представили у встановлений термін дані про проходження практики, здійснюється з урахуванням наявних можливостей і вимог конкретних місць практики до рівня підготовки студентів.

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

- допомога при оформленні на практику, проведення інструктажу з техніки безпеки і охорони праці;
- забезпечення практикантів робочими місцями;
- формулювання індивідуального завдання на 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 практику студента.

3. Права і обов’язки студентів у період практики

На студентів, які проходять 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 практики регламентується законодавством України про працю. За наявності вакантних місць студенти можуть бути зараховані на штатні посади, якщо робота на них відповідає вимогам програми практики. При цьому не менше половини робочого часу відводиться на загально-професійну підготовку за програмою практики.

Студент-практикант зобов’язаний:

- повністю виконувати завдання, передбачені програмою і календарним планом практики, нести відповідальність за виконувану роботу та її результати;
- строго дотримуватись діючих на базі 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 практики;
- у 5-денний термін після завершення 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 практики від бази або від кафедри. Студент, який не виконав програму практики, або отримав негативний відгук керівника від бази практики, або незадовільну оцінку на захисті, вважається таким, що не виконав навчального плану поточного семестру.

4. Зміст проєктної практики

Під час проходження проєктної практики студентами належить вирішити такі завдання:

- вивчити організацію і управління діяльністю відповідного підрозділу чи підприємства, що потребують захисту;
- вивчити технологічні процеси і виробниче обладнання бази практики;
- вивчити діючі стандарти, технічні умови, положення та інструкції по експлуатації засобів обчислювальної техніки, вимірювальних приладів та технологічного обладнання, що використовується у виробничій діяльності;
- вивчити на практиці сучасні методи реалізації несанкціонованого доступу та захисту інформації від стороннього впливу та застосування сучасних існуючих засобів захисту інформації;
- зібрати та опрацювати матеріал для написання курсової роботи.

5. 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;
- проаналізувати стан системи безпеки об'єкта управління;
- проаналізувати існуючі методи реалізації несанкціонованого доступу, які можуть бути застосовані для об'єкта управління;
- проаналізувати існуючі методи захисту інформації від несанкціонованого доступу;
- розробити вимоги щодо захисту інформації від несанкціонованого доступу
- зібрати матеріал, організувати та виконати наукове дослідження за обраною темою магістерської роботи.
- виконати огляд літературних джерел за темою дослідження.
- оформити власні результати, отримані в межах роботи над кваліфікаційною роботою. Підготувати матеріали до захисту магістерської роботи.
- оформити звіт про 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 практики.

Керівник від бази практики визначає завдання для виконання під час проходження 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.

6. Документація про проходження практик

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

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

6.1. Вимоги до оформлення щоденника практики. Під час перебування на виробничій (переддипломній) практиці студент веде щоденник. У ньому формулюють індивідуальне завдання на практику, складають графік її проходження і фіксують основні види виконуваних робіт. Індивідуальні завдання розробляють спільно керівники від бази практики і від кафедри, після чого їх затверджує завідувач кафедри. Студент складає графік проходження практики і погоджує його з керівником від бази практики. Всі види виконуваних на практиці робіт студент записує у щоденник, а факт їх виконання засвідчується підписом керівника від бази.

Після завершення практики студент здає заповнений щоденник керівнику практики від кафедри.

6.2. Вимоги до змісту і оформлення звіту з практики. Після завершення практики студент складає звіт і здає його разом зі щоденником керівнику 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 практики, наводиться коротка характеристика бази практики.

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

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

6.3. Відгук бази практики. Відгук про проходження студентом практики оформляють за зразком, наведеним у додатку. Його підписує керівник від бази практики, завіряє печаткою бази практики і передає керівнику практики від кафедри разом зі звітом та щоденником практики. Відгук обов'язково повинен містити оцінку (від 0 до 50 балів) результатів практики студента.

7. Захист і оцінювання результатів практики

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

Звіт попередньо оцінює керівник 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 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 практики беруть до уваги кількісні і якісні показники виконання студентом завдань практики, повноту, грамотність, правильність оформлення звітної документації та відгук, наданий керівником від бази 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 практики керівником практики від бази (0-50 балів);
2) оцінки змісту і оформлення звітної документації (0-25 балів);
3) оцінки захисту звіту з 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 магістерських і кусових робіт Методичні рекомендації ЛНУ ім.Івана Франка, ФПМІ. – 2024. -27 с https://ami.lnu.edu.ua/wp-content/uploads/2013/11/Metodychni-rekomendatsii_kvalifikatsiyna-robota.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
9. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
10. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
11. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
12. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
13. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
14. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
15. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
16. 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
17. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

ДОДАТКИ

Зразок титульного листа щоденника практики

Львівський національний університет імені Івана Франка

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ

КАФЕДРА _____

ЩОДЕННИК

виробничої (переддипломної) практики
студента(ки) ___ курсу групи ___

_____
(П. І. Б. студента)

База практики_____
(назва підприємства, організації, установи)

Терміни практики з «__» _____20__ р.
до «__» _____20__ р.

Керівники практики:

Від бази _____
(посада, прізвище та ініціали керівника)

Від кафедри _____
(звання, прізвище та ініціали керівника)

Зразок оформлення індивідуального завдання на практику

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
.
_____
«__» _____20__ р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

_____
_____
_____
_____
_____
_____(
формулювання пунктів індивідуального завдання)
_____
_____
_____
_____
_____
_____

Завдання отримав студент
_____
(прізвище та ініціали студента) (підпис)
«__» _____ 20__ р.

Зразок титульного листа звіту з практики

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ

КАФЕДРА _____

ЗВІТ

з проєктної практики /
виробничої (переддипломної) практики
студента(ки) ___ курсу групи ___

_____
(П. І. Б. студента)

База практики_____
(назва підприємства, організації, установи)

Терміни практики з «__» _____20__ р. до «__» _____20__ р.

Виконав підпис _____
(П. І. Б. студента)

Керівник від підпис _____
бази практики (П. І. Б. керівника)

Керівник від підпис _____
Кафедри (П. І. Б. керівника)

Зразок відгуку про практику

ВІДГУК ПРО ПРАКТИКУ

студента(ки) _____(прізвище, ім’я, по батькові)

_____

_____

_____

_____

_____

_____(текст відгуку)

_____

_____

_____

_____

_____

_____

Рекомендована оцінка _____
(0-50 балів)

Керівник практики від бази

_____
(прізвище та ініціали) (підпис)

Місце печатки