

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”

кафедра твердотільної електроніки та інформаційної безпеки



«ЗАТВЕРДЖУЮ»

Декан фізичного факультету

/Лазур В.Ю./

« 29 » 04 2022 року

Робоча програма
переддипломної практики

рівень вищої освіти другий (магістерський)

галузь знань 12 Інформаційні технології
(шифр і назва)

Спеціальність 125 Кібербезпека
(шифр і назва)

освітньо- професійна програма

Безпека інформаційних і комунікаційних систем
(шифр і назва)

спеціалізація _____

статус дисципліни обов'язкова
(обов'язкова/за вибором)

Мова навчання українська

Ужгород 2022


Робоча програма **переддипломної практики** для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **Безпека інформаційних і комунікаційних систем**.

Розробники: доктор фіз.-мат. наук, професор Різак В.М.

Робочу програму розглянуто та затверджено на засіданні кафедри твердотільної електроніки та інформаційної безпеки
протокол № 7 від «28» 04 2022 р.

Завідувач кафедри  Різак В.М.

Схвалено науково-методичною комісією фізичного факультету
протокол № 10 від «29» 04 2022 р.

Голова науково-методичної комісії  Карбованець М. І.

© Різак В.М. 2022 р.

© ДВНЗ «Ужгородський
національний університет», 2022 р.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Розподіл годин за навчальним планом
	Денна форма навчання
Кількість кредитів ЄКТС – 3	Рік підготовки:
Загальна кількість годин - 90	2
Кількість модулів – 1	Семестр:
Індивідуальне завдання (назва)	3
	Лекції:
	Практичні (семінарські):
	Лабораторні:
	Самостійна робота:
Вид підсумкового контролю: залік	90
Форма підсумкового контролю: усна	

2. МЕТА ТА ЗАВДАННЯ ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

Переддипломна практика студентів ДВНЗ «Ужгородський національний університет» є невід’ємною частиною освітньо-професійної програми підготовки фахівців, основним завданням якої є практична підготовка випускника за освітньо-кваліфікаційним рівнем магістр. Вона проводиться на оснащених відповідним чином базах університету та інших навчальних закладів, а також на підприємствах, установах, організаціях різних галузей господарства і державного управління.

У відповідності з навчальним планом до освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» для другого (магістерського) рівня спеціальності 125 Кібербезпека, студенти проходять переддипломну практику у III семестрі другого року навчання впродовж 2 тижнів. Загальний обсяг переддипломної практики складає 90 годин (3 кредити).

Метою практики є оволодіння студентами сучасними методами, формами організації та знаряддями праці в галузі кібербезпеки, формування у них, на базі одержаних у вищому навчальному закладі знань, професійних умінь і навичок для прийняття самостійних рішень під час конкретної роботи в реальних ринкових і виробничих умовах, виховання потреби систематично поновлювати свої знання та творчо їх застосовувати в практичній діяльності. Під час практики поглиблюються та закріплюються теоретичні знання з усіх дисциплін

навчального плану, збирається матеріал для виконання дипломної роботи.

Фокус переддипломної практики є: узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профільюючими дисциплінами, що вивчені за спеціальністю "Кібербезпека"; отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз; розроблення плану кіберзахисту інформаційної системи.

Місце дисципліни в структурі освітньо-наукової програми: курс відноситься до дисциплін нормативної частини циклу професійної підготовки, за результатами яких здобувачі здають залік та виконують навчальний процес по спеціальності 125 Кібербезпека.

Відповідно до Стандарту вищої освіти України для другого (магістерського) рівня спеціальності 125 Кібербезпека, вивчення дисципліни сприяє формуванню у здобувачів другого рівня вищої освіти таких компетентностей:

Інтегральна: Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність проводити дослідження на відповідному рівні (КЗ-2).
3. Здатність до абстрактного мислення, аналізу та синтезу (КЗ-3).
4. Здатність оцінювати та забезпечувати якість виконуваних робіт (КЗ-4).
5. Здатність спілкуватися з представниками інших професійних груп різного рівня (експертами з інших галузей знань / видів економічної діяльності) (КЗ-5).

Фахові компетенції (ФК)

1. 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 (КФ1).

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

3. Здатність досліджувати, розробляти і проваджувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури (КФ3).

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

5. Здатність досліджувати, розробляти та проваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури правління, контролю та розслідування, а також надавати рекомендації щодо попередження та агізу кіберінцидентів в цілому (КФ7).

6. Здатність досліджувати, розробляти, проваджувати та супроводжувати методи інформаційної 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 (КФ8).

7. 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 (КФ10).

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» для другого (магістерського) рівня спеціальності 125 Кібербезпека,

проходження повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (РН):

Програмні результати навчання	
Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	РН 3
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.	РН5
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	РН6
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН11
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.	РН14
Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	РН15
Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	РН16
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.	РН19
Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	РН20
Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	РН21
Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	РН23

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після проходження переддипломної практики:

1. Оволодіння знаннями здобувачами про сучасні засоби фізичного захисту інформації для проведення дослідницької та/або інноваційної діяльності в сфері інформаційної безпеки та/або кібербезпеки (РН3).

2. Знати сучасні вимоги щодо захисту інформації від несанкціонованого доступу для критичного осмислення 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 (PH5).

3. Набути практичних навичок щодо аналізу та оцінки захищеності систем, комплексів та засобів кіберзахисту (PH6).

4. Знати методи реалізації несанкціонованого доступу та захисту інформації від стороннього деструктивного впливу для забезпечення ефективного функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації (PH11).

5. Набуття практичних навичок щодо проведення аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та/або кібербезпеки в цілому (PH14).

6. Вміти обґрунтувати висновки про необхідність модернізації і розвитку системи інформаційної безпеки та зрозуміло і недвозначно доносити власну думку з проблем інформаційної безпеки та/або кібербезпеки (PH15).

7. Вміння проводити аналіз проблеми безпеки інформації за науково-технічними джерелами та приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень (PH16).

8. Розробляти типові вимоги щодо захисту інформації від несанкціонованого доступу та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі (PH19).

9. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик (PH20).

10. Застосовувати засоби захисту інформації в інформаційно-комунікаційних системах, використовуючи методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів (PH21).

11. Вміти на основі сучасних знань у суміжних галузях та іншої доступної інформації обґрунтовувати вибір програмного забезпечення, устаткування та інструментів в галузі інформаційної безпеки та/або кібербезпеки (PH23).

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ Форми та методи контролю

Поточний контроль здійснюється керівником практики впродовж проходження студентами практики шляхом аналізу та оцінки їх систематичної роботи.

Підсумковий контроль здійснюється у кінці проходження практики шляхом оцінювання цілісної систематичної діяльності студентів протягом конкретного періоду.

При виставленні заліку студенту враховується рівень теоретичної підготовки майбутнього фахівця, якість виконання завдань практики, рівень оволодіння вміннями і навичками, якість оформлення документації та час її подання.

Вимоги до звіту

Звіт студента повинен відповідати наступним **правилам оформлення:**

1. Обсяг звіту складає довільну кількість сторінок комп'ютерного набору. До загального обсягу входять титульна сторінка, план, вступ, основна частина, висновки, список використаних джерел та додатки.

2. Текст набирається на аркушах паперу стандартного формату А-4 з використанням шрифтів текстового редактора Times New Roman, кеглем 14, через 1,5 інтервали з дотриманням таких розмірів полів: верхнього і нижнього – 20 мм, лівого – 30 мм, правого – 10мм.

3. Титульна сторінка оформляється за встановленою формою (див. Додаток 4).

4. Заголовки розділів виконують великими літерами, симетрично до тексту, наприклад: ЗМІСТ, ВСТУП, ОСНОВНА ЧАСТИНА, ВИСНОВКИ, СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ, ДОДАТКИ. Крапку в кінці заголовку не ставлять.

5. Список використаної літератури та інших документальних джерел, використаних під час роботи, розміщуються після висновків і оформляється відповідно до чинних стандартів.

Критерії оцінювання

Переддипломна практика студентів оцінюється за всіма видами діяльності відповідно до розробленої системи балів

Види роботи	Кількість балів (максимальна)
Вивчення інформаційної діяльності підприємства та визначення об'єктів захисту – інформації з обмеженим доступом, технічного обладнання, інформаційно-комунікаційних систем і мереж	10 балів
Виявлення слабких місць у системах захисту та уразливостей в інформаційній системі бази практики	15 балів
Розробка рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах бази практики	15 балів
Практична реалізація і впровадження власної програмної або інженерно-технічної розробки	30 балів
Оформлення звітної документації	10 балів
Захист практики	20 балів

Порядок перерахунку рейтингових показників нормованої 100-бальної університетської шкали оцінювання в традиційну 4-бальну шкалу та європейську шкалу ECTS.

Шкала оцінювання згідно ЄКТС та національна

За шкалою ECTS	За шкалою університету	За національною шкалою
A	90 – 100 (відмінно)	5 (відмінно)
B	85 – 89 (дуже добре)	4 (добре)
C	75 – 84 (добре)	
D	70 – 74 (задовільно)	3 (задовільно)
E	60 – 69 (достатньо)	

FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)	

Дотримання академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил (<https://vumonline.ua/course/academic-integrity-at-the-university/>), якими мають керуватися учасники освітнього процесу з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності науково-педагогічним складом передбачає: посилення на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати досліджень та власну наукову діяльність.

Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилення на джерела інформації у разі використання ідей, тверджень, відомостей; надання достовірної інформації про результати власної наукової діяльності.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності як повторне проходження оцінювання (підготовка індивідуального завдання за іншою темою тощо).

Перевірка усіх індивідуальних робіт здобувачів на наявність академічного плагіату проводиться викладачем або спеціально призначеним для цього працівником УжНУ за допомогою програмного продукту, що використовується в УжНУ з визначення рівня унікальності роботи.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Завдання проходження переддипломної практики

Під час практики студенти виконують такі **завдання**: зібрати матеріал за темою дипломного проекту для оцінювання стану системи захисту об'єкта управління; вивчити на практиці сучасні методи реалізації несанкціонованого доступу 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 несанкціонованого доступу; проаналізувати сучасні існуючі засоби захисту інформації в інформаційно-комунікаційних системах від витіку її технічними каналами; розробити вимоги щодо використання засобів захисту інформації в інформаційно-комунікаційних системах від витіку її технічними каналами за об'єктом управління.

5.2. Терміни проходження. Бази практики

Згідно навчальних планів практика проводиться на 2 курсі навчання за магістерською програмою загальною тривалістю два тижні. Практика студентів проводиться на базах практики, діяльність яких відповідає напряму підготовки «КІБЕРБЕЗПЕКА» та може забезпечити усі необхідні умови для виконання студентом програми практики. При підготовці фахівців за цільовими напрямленнями підприємств, організацій, установ бази практики зазначаються у відповідних договорах. У випадку, коли підготовка спеціалістів університету здійснюється за замовленням фізичних та/або юридичних осіб, бази для проходження практики забезпечують відповідні замовники, або університет, що визначається умовами відповідних договорів. Проходження практики студентів оформляється відповідним наказом по підприємству, організації, установі - базі практики. Студенти можуть самостійно з дозволу

керівника практики від факультету і за погодженням завідувача кафедрою твердотільної електроніки та інформаційної безпеки підбирати для себе місце проходження практики і пропонувати його як базу практики. З базами практик університет/факультет завчасно укладає договори на проведення практики за затвердженою формою, визначеною в Додатку 1. Тривалість дії договорів погоджується договірними сторонами. Вона може охоплювати період конкретного виду практики (Додаток 1.1.) або діяти впродовж 5 років (Додаток 1.2.). На основі укладеного довгострокового чи короткострокового договору, студентіві видається направлення на практику (Додаток 2).

5.3. Організація практики

Студенти направляються на практику наказом ректора університету. Відповідальність за організацію, проведення і контроль практики покладається на першого проректора університету. Навчально-методичне керівництво і виконання програми практики забезпечує кафедра твердотільної електроніки та інформаційної безпеки. До керівництва практикою студентів залучаються досвідчені науково-педагогічні працівники кафедри.

Керівник практики від кафедри: перед початком практики перевіряє готовність баз практики та здійснює всі необхідні заходи для проведення практики на належному рівні; заздалегідь подає керівнику практики від університету пропозиції на виготовлення усіх необхідних бланків документів для проведення практики; готує та реєструє у журналі договори про проведення практики та виписує студентам відповідне направлення; у перший день практики забезпечує проведення всіх організаційних заходів (проводить цільовий інструктаж з техніки безпеки та охорони праці, видає студентам пакет усіх необхідних документів, роз'яснює порядок ведення щоденника практики (Додатки 3), виконання індивідуальних завдань та знайомить студентів із вимогами щодо оформлення звітів про проходження практики); готує проект наказу про направлення студентів на практику; у тісному контакті з керівником практики від бази практики забезпечує високу якість її проходження згідно з програмою; контролює забезпечення нормальних умов праці й побуту студентів та проведення з ними обов'язкових інструктажів з охорони праці й техніки безпеки; у складі комісії приймає залік з практики; після закінчення практики подає завідувачу кафедри звіт про проведення практики.

Завідувач кафедри в кінці кожного навчального року подає керівнику практик університету узагальнений звіт про проходження студентами практики за рік.

5.4. Обов'язки студента-практиканта

Студент-практикант зобов'язаний розпочати і завершити практику у визначений термін. Студент повинен своєчасно прибути на інструктивну нараду та отримати від керівника практики від кафедри консультацію щодо оформлення всіх необхідних документів; своєчасно прибути на базу практики; у повному обсязі виконувати всі завдання, передбачені програмою практики та вказівки керівників; дотримуватись правил охорони праці, техніки безпеки і виробничої санітарії, а також підготувати всі необхідні звітні документи згідно вимог і відзвітуватись за виконану роботу.

5.5. Зміст практики

Зміст переддипломної практики визначається вимогами освітньо-кваліфікаційної характеристики та освітньо-професійної програми підготовки магістрів за спеціальністю 125 - Кібербезпека. Практиканти покроково працюють над індивідуальними завданнями, використовуючи знання набуті під час підготовки за спеціальністю, формують практичні навички щодо порядку проведення робіт з захисту інформації. Під час практики потрібно більш детально розглянути положення основних державних стандартів у галузі захисту інформації. Для формування вмінь та навичок у цей час особливу увагу потрібно приділити нормативним документам розроблених державною службою спеціального зв'язку та захисту інформації України. Це дасть змогу виконати завдання практики у повному обсязі. Індивідуальне завдання є однією з форм набуття фахових компетентностей, яка має на меті поглиблення, узагальнення та закріплення знань, які студенти отримали у процесі теоретичного навчання, та застосування цих знань в практичній діяльності. Напрями і

тематика індивідуальних завдань для студентів-практикантів розробляються на кафедрі твердотільної електроніки та інформаційної безпеки, виходячи з теми і завдань магістерської роботи, здібностей та уподобань студентів. Індивідуальне завдання є особистим для кожного студента, визначається керівником практики спільно з керівником магістерської роботи та виконується у відповідності до її тематики. Індивідуальні завдання виконують студенти самостійно під керівництвом керівника практики. У кожному конкретному випадку програма переддипломної практики може змінюватись і доповнюватись для кожного здобувача вищої освіти залежно від особливостей бази практики та особистих професійних інтересів магістра. Орієнтовний перелік індивідуальних завдань на переддипломну практику: вивчення технологій ідентифікації та аутентифікації користувачів в інформаційно-комунікаційних системах та мережах, захисту інформації на віртуальних цифрових носіях, забезпечення безпеки документів в системах електронного документообігу, вибору проектної альтернативи системи захисту інформації корпоративної інформаційно-аналітичної системи, управління інцидентами інформаційної безпеки з використанням можливостей DLP-систем, протидії соціальному інжинірингу на об'єктах інформаційної діяльності; освоєння методів контролю оперативного стану інформаційної системи, формування профілів користувачів безпроводових мереж, контролю цілісності та автентифікації інформації в АС 2, протидії спаму в інформаційно-комунікаційних системах, аналізу механізмів впливу відмов апаратного забезпечення на стабільність роботи дата-центрів й інформаційної безпеки при розгортанні систем широкосмугового зв'язку Wi-Fi; дослідження безпеки соціотехнічних систем від складних інформаційних атак, безпеки віртуальних спільнот в інтернет середовищі соціальних мереж, системи протидії впливу зловиякісного коду, шпигунського і завідомо фальшивого програмного забезпечення; забезпечення захисту інформації від копіювання на Web-ресурсі, в системах електронного документообігу, засобами операційних систем, при використанні електронної пошти, у телекомунікаційних системах, системи «розумний дім» та захисту Internet of Things, бездротових мереж й баз даних.

На першому етапі студенти знайомляться з відомчим підпорядкуванням бази практики, основними нормативно-правовими документами, що лежать в основі її діяльності; - з режимом роботи і правилами внутрішнього розпорядку; з вимогами, які пред'являються до працівників бази практики, їх професійних компетентностей в сфері інформаційних технологій та захисту інформації.

Другий, основний, етап практики включає виконання заздалегідь отриманого від керівника практики індивідуального завдання. Для цього студенти повинні проаналізувати системи забезпечення інформаційної безпеки на підприємстві та виявити слабкі місця в системах захисту та уразливості в інформаційній системі бази практики. Наступним кроком практиканти повинні розробити рекомендацій щодо вдосконалення системи захисту інформації, підвищення рівня захищеності інформації в інформаційних системах бази практики або практично реалізувати і впровадити власну програмну або інженерно-технічну розробку. На цьому етапі студентам потрібно сформулювати свої пропозиції керівництву бази практики щодо вдосконалення існуючої системи захисту інформації, підвищення рівня захищеності інформації в їх інформаційних системах, тощо. А у випадку відсутності системи захисту інформації на базі практики – запропонувати кроки щодо її впровадження.

На третьому, заключному, етапі практики студенти оформлюють та підписують звітну документацію (щоденник практики, звіт про проходження практики, звіт про виконання індивідуального науково-дослідного завдання, додатки, відгук керівника практики від підприємства, характеристика, тощо.). Завершується практика обговоренням результатів на засіданні кафедри.

6. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання,

експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.

Для дистанційного навчання використовується Moodle(e-learn.uzhnu.edu.ua) та Google Meet.

Рекомендована література

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
- 3.Юлія Лісовська, Кібербезпека. Ризики та заходи. К.: Кондор , 2019 , 272с
4. Юрій Когут, Кібербезпека та ризики цифрової трансформації компанії. Видавництво Консалтингова компанія Сідкон 2021 , 372с. ISBN 978-966-97546-9-1
5. Марк Гудмен, Злочини майбутнього, Видавництво Фабула , 2019, 592с.
6. Юрій Когут, Кібертероризм. Історія, цілі, об'єкти . Видавництво Консалтингова компанія Сідкон 2021 , 304с.

Нормативні документи

1. Про вищу освіту [Текст]: Закон України No 1556-VII від 01.07.2014 // Відомості Верховної Ради, 2014, No 37-38, ст. 2004.
3. Закон України «Про інформацію» від 02.10.1992 No 2657-XII
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No 80/94-ВР
5. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 No373
6. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
7. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
10. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
- 11.НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
12. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.
- 13.НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
14. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
15. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

16. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

17. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.

18. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

19. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

20. 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.

21. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ДОГОВІР № _____
про проведення практики студентів фізичного факультету
Державного вищого навчального закладу
«Ужгородський національний університет»

Місто Ужгород

« _____ » _____ 20 _____ р.

Ми, що нижче підписалися, з однієї сторони, фізичний факультет Державного вищого навчального закладу «Ужгородський національний університет» в особі декана факультету _____, що діє на підставі Положення про факультет Державного вищого навчального закладу «Ужгородський національний університет», і, з другої сторони

(назва підприємства, організації, установи)

(надалі - База практики) в особі _____, діючого на підставі _____

(посада, прізвище та ініціали)

(далі - сторони), уклали між собою договір: (статут підприємства, розпорядження, доручення)

1. БАЗА ПРАКТИКИ ЗОБОВ'ЯЗУЄТЬСЯ:

1.1 Прийняти студентів (список додається у направленні) на проходження практики згідно з графіком навчального процесу:

№ з/п	Напрямок підготовки/ спеціальність	Курс	Вид практики	Кількість студентів	Термін практики (початок - кінець)

1.2 Призначити наказом кваліфікованих фахівців для керівництва практикою.

1.3 Створити належні умови для виконання студентами програми практики, не допускати їх використання до виконання робіт, що не відповідають програмі практики та майбутньому фаху.

1.4 Забезпечити студентам умови безпечної праці на конкретному робочому місці. Проводити обов'язкові інструктажі з охорони праці: вступний та на робочому місці. У разі потреби навчати студентів-практикантів безпечних методів праці.

1.5 Надати студентам можливість користуватися матеріально-технічними засобами та інформаційними ресурсами, необхідними для виконання програми практики.

1.6 Забезпечити облік виходів на роботу студентів-практикантів. Про всі порушення трудової дисципліни, внутрішнього розпорядку та про інші порушення повідомляти вищій навчальний заклад.

1.7 Після закінчення практики надати характеристику на кожного студента-практиканта, в котрій відобразити виконання програми практики, якість підготовленого ним звіту тощо.

1.8 Надавати студентам можливість збору усієї необхідної інформації для написання курсових та дипломних робіт (проектів) за результатами діяльності підприємства, що відповідають програмі практики і не становлять комерційної таємниці.

2. ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД ЗОБОВ'ЯЗУЄТЬСЯ:

2.1 До початку практики надати Базі практики для погодження витяг з робочої програми практики, а не пізніше ніж за тиждень - список студентів, яких направляють на практику.

2.2 Призначити керівниками практики кваліфікованих викладачів.

2.3 Забезпечити дотримання студентами трудової дисципліни і правил внутрішнього

трудового розпорядку. Брати участь у розслідуванні комісією Баз практик нещасних випадків, якщо вони сталися зі студентами під час проходження практик.

2.4 Не розголошувати використану студентами інформацію про діяльність Баз практик.

3. ВІДПОВІДАЛЬНІСТЬ СТОРІН ЗА НЕВИКОНАННЯ ДОГОВОРУ:

3.1 Сторони відповідають за невиконання покладених на них обов'язків щодо організації і проведення практик згідно із законодавством про працю в Україні.

3.2 Усі суперечки, що виникають між сторонами за договором, вирішуються у встановленому порядку.

3.3 Договір набуває сили після його підписання сторонами і діє до кінця практик згідно з календарним планом.

3.4 Договір складено у двох примірниках: один для Баз практик, один для Університету.

Юридичні адреси та підписи сторін

**Державний вищий навчальний заклад
«Ужгородський національний університет»
Адреса: 88000, м. Ужгород, вул. Підгірна, 46**

База практик

Адреса: _____

(підпис)

(посада, прізвище та ініціали)

(підпис)

(посада, прізвище та ініціали)

М.П «__» «_____» 20__ р.

М.П «__» «_____» 20__ р.

ДОГОВІР № _____
про проведення практики студентів Державного вищого навчального закладу
«Ужгородський національний університет»

Місто Ужгород

« ____ » « _____ » 20 ____ р.

Ми, що нижче підписалися, з однієї сторони, Державний вищий навчальний заклад «Ужгородський національний університет» в особі ректора Смоланки В.І, що діє на підставі Статуту (надалі - Університет), з однієї сторони, та

(назва підприємства, організації, установи)

(надалі - База практики) в особі _____,

(посада, прізвище та ініціали)

діючого на підставі _____ (Статут, Розпорядження, Доручення), з другої сторони (далі -Сторони) , уклали між собою Договір про наступне:

1. ПРЕДМЕТ ДОГОВОРУ

1.1 Предметом договору є проведення практики студентів ДВНЗ «УжНУ» напряму підготовки/спеціальності _____

1.2 Тривалість та терміни проведення кожного виду практики визначається навчальним планом відповідного напряму підготовки/спеціальності та графіком навчального процесу.

2. ПРАВА І ОBOB'ЯЗКИ СТОРІН

2.1 Університет зобов'язується:

2.1.1 До початку практики надати Базі практики для погодження витяг з робочої програми практики, а не пізніше ніж за тиждень - список студентів, яких направляють на практику.

2.1.2 Призначити керівниками практики кваліфікованих викладачів.

2.1.3 Забезпечити дотримання студентами трудової дисципліни і правил внутрішнього трудового розпорядку. Брати участь у розслідуванні комісією Базі практики нещасних випадків, якщо вони сталися зі студентами під час проходження практики.

2.1.3 Не розголошувати використану студентами інформацію про діяльність Базі практики.

2.2 База практики зобов'язується:

2.2.1 Прийняти студентів на проходження практики згідно з направленням від Університету.

2.2.2 Призначити наказом кваліфікованих фахівців для керівництва практикою.

2.2.3 Створити належні умови для виконання студентами програми практики, не допускати їх використання до виконання робіт, що не відповідають програмі практики та майбутньому фаху.

2.2.4 Забезпечити студентам умови безпечної праці на конкретному робочому місці. Проводити обов'язкові інструктажі з охорони праці: вступний та на робочому місці. У разі потреби навчати студентів-практикантів безпечних методів праці.

2.2.5 Надати студентам-практикантам можливість користуватися матеріально-технічними засобами та інформаційними ресурсами, необхідними для виконання програми практики.

2.2.6 Забезпечити облік виходів на роботу студентів-практикантів. Про всі порушення трудової дисципліни, внутрішнього розпорядку та про інші порушення повідомляти Університет.

2.2.7 Після закінченні практики надати характеристику на кожного студента-практиканта, в котрій відобразити виконання програми практики, якість підготовленого ним

звіту тощо.

2.2.8 Надавати студентам можливість збору усієї необхідної інформації для написання курсових та дипломних робіт(проектів) за результатами діяльності підприємства, що відповідають програмі практики і не становлять комерційної таємниці.

3. ІНШІ УМОВИ

3.1 Даний Договір вступає в силу з моменту його підписання Сторонами і діє протягом 5 років.

3.2 Договір вважається пролонгованим на такий же строк, якщо за один місяць до закінчення його дії Сторони письмово не заявили про намір розірвати Договір і продовжують виконувати його умови.

3.3 Дію Договору може бути припинено до закінчення терміну дії за взаємною згодою Сторін.

3.4 Зміни та доповнення до цього Договору вносяться за взаємною згодою Сторін, здійснюються в письмовій формі і після підписання стають його невід'ємною частиною.

3.5 Сторони відповідають за невиконання покладених на них обов'язків щодо організації і проведення практики згідно із законодавством про працю в Україні.

3.6 Всі спори, що виникають з цим Договором, вирішуються шляхом переговорів. У випадку недосягнення Сторонами згоди, спори вирішуються у встановленому законодавством України порядку.

3.7 Якщо одна зі Сторін не виконала зобов'язань за цим Договором, інша Сторона має право в односторонньому порядку розірвати Договір до закінчення строку його дії, письмово повідомивши про це іншу Сторону не менш ніж за місяць.

3.8 Договір складено у двох автентичних примірниках, які мають однакову юридичну силу, по одному для кожної із Сторін.

ЮРИДИЧНІ АДРЕСИ ТА ПІДПИСИ СТОРІН

Державний вищий навчальний заклад
«Ужгородський національний університет»
Адреса: 88000, м. Ужгород, вул. Підгірна, 46

База практики

Адреса: _____

(підпис) Ректор Смоланка В.І.
(посада, прізвище та ініціали)

(підпис) _____
(посада, прізвище та ініціали)

М.П «__» «_____» 20__ р.

М.П «__» «_____» 20__ р.

КЕРІВНИКУ

НАПРАВЛЕННЯ НА ПРАКТИКУ
(є підставою для зарахування на практику)

Згідно з договором від « ____ » « ____ » 20 ____ року № ____, який укладено з

_____ (повне найменування підприємства, організації, установи)

направляємо на практику студентів 2 курсу навчання за магістерською освітньо-професійною програмою «**Безпека інформаційних і комунікаційних систем**»

Назва практики _____ **переддипломна** _____

Строки практики: з « ____ » « ____ » 20 ____ р. по « ____ » « ____ » 20 ____ р.

Керівник переддипломної практики від кафедри
твердотільної електроніки та інформаційної безпеки

_____ (посада, вчений ступінь, звання ПІБ)

ПРІЗВИЩА, ІМЕНА ТА ПО БАТЬКОВІ СТУДЕНТІВ

М.П. Декан фізичного факультету _____ (підпис) _____ (прізвище та ініціали)

**Висновок керівника практики від закладу вищої освіти про
проходження практики**

Додаток 3

**ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»**

ЩОДЕННИК ПРАКТИКИ

_____ переддипломна
(вид і назва практики)

Студента _____
(прізвище, ім'я, по батькові)

Факультет, інститут _____ Фізичний

Кафедра _____ твердотільної електроніки та інформаційної безпеки

Освітній рівень _____

Спеціальність _____

Освітня програма _____

Курс, група _____

Дата складання заліку « _____ » _____ 20____ року

Оцінка:
за національною шкалою _____

кількість балів _____

за шкалою ЄКТС _____

Керівник практики від закладу вищої освіти

_____ *(підпис)* _____ *(посада, прізвище та ініціали)*

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”**

**кафедра твердотільної електроніки та
інформаційної безпеки**

ЗВІТНІ МАТЕРІАЛИ
з переддипломної практики студента 2 курсу навчання
за магістерською освітньо-професійною програмою
«БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ»

(прізвище, ім'я, по-батькові)

База для проведення практики

(повна назва бази, адреса)

Термін проходження практики з _____ по _____ 20 ____ р.

Керівник переддипломної практики

(посада, вчений ступінь, звання ПІБ)

ЗВІТ

про проведення переддипломної практики студентів кафедри
твердотільної електроніки та інформаційної безпеки УжНУ

Терміни проведення _____

Кількість студентів згідно наказу № _____ від „ _____ ” _____ 20 ____ р. _____ чол.

Кількість студентів, які проходили практику _____ чол.

Кількість студентів, які не пройшли практику _____ чол.

Бази практики _____

Оцінки за практику:

“відмінно” - _____ чол.

“добре” - _____ чол.

“задовільно” - _____ чол.

“незадовільно” - _____ чол.

“не з'явилися” _____ чол.

Пропозиції щодо вдосконалення організаційних питань проведення практики: _____

Пропозиції щодо вдосконалення змісту практики: _____

Керівник

переддипломної

практики:

(посада, вчений ступінь, звання ПІБ)