ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА ПРАКТИКИ ОК 14 «ВИРОБНИЧА ПРАКТИКА»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
_____ Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
_____ Володимир ВОРОТНІКОВ

Розробник: кандидат технічних наук, доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки Юрій БРОДСЬКИЙ

Житомир
2023 – 2024 н.р.

Програма виробничої практики для здобувачів вищої освіти освітнього ступеня «магістр» спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійна програма «Кібербезпека» / Укладач Ю.Б. Бродський. – Житомир: Державний університет «Житомирська політехніка», 2023. – 16 с.

ЗМІСТ

Вступ

Метою практики для студентів, що навчаються за спеціальністю 125 «Кібербезпека та захист інформації» є оволодіння студентами сучасними методами, формами організації та інструментальними засобами у галузі інформаційних технологій, 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 умовах, виховання потреби систематично поновлювати свої знання та творчо їх застосовувати в практичній діяльності.

Виробнича практика студентів спеціальності 125 «Кібербезпека та захист інформації» є невід'ємною складовою частиною процесу підготовки фахівців (магістрів) у закладах вищої освіти і проводиться відповідно до навчального плану на третьому році навчання. Під час виробничої практики студенти мають набути навичок з експлуатації та захисту комп’ютерних систем і мереж конкретних підприємств (організацій, установ), тобто здійснити практичну підготовку до самостійної роботи із розв’язання практичних завдань на підприємстві.

Виробничу практику студенти проходять на підприємствах (організаціях, установах) різних форм власності під керівництвом викладачів кафедри комп’ютерної інженерії та кібербезпеки і призначених керівників від відповідних підприємств (організацій, установ). Така організація керівництва практикою дає змогу студентам поглибити теоретичні знання і набути досвіду практичної роботи за первинними посадами. Під час практики студенти ознайомлюються з підприємством, збирають необхідну інформацію про його господарську діяльність, здійснюють аналіз результатів діяльності підприємства і визначають наявність проблем щодо захисту інформації. У разі виявлення на підприємстві проблем пов’язаних з безпекою, студенти повинні вказати можливі шляхи їх вирішення. Свої результати роботи студенти оформлюють у вигляді звіту з виробничої практики. Оцінка результатів роботи студентів здійснюється спочатку керівниками практики від підприємства та університету у вигляді відгуку, а потім комісією по захисту звітів з практики.

Тривалість виробничої практики для студентів першого року навчання становить 4 тижні (180 год.).

1. Мета та основні завдання

Проходження виробничої практики студентами має на меті:

- засвоєння отриманих у процесі навчання теоретичних знань та практичних вмінь і навичок за фахом;
- ознайомлення з процесом виробництва на підприємствах, в організаціях, установах, компаніях, де доведеться працювати майбутнім спеціалістам;
- отримання практичного досвіду за обраною професією;
- збір документів (довідок, матеріалів тощо) для оформлення звіту з проходження виробничої практики.

Основні завдання виробничої практики:

узагальнення, закріплення і поглиблення знань, що отримані під час навчання в університеті для використання їх у подальшій роботі та обґрунтованого прийняття рішень;

отримання інформації про ринок затребуваних професій;

знайомство з порядком роботи та умовами праці на підприємстві;

отримання досвіду входження в трудовий колектив;

отримання інформації про те, які знання, отримані в університеті, і в якому напрямі необхідно поглиблювати і розвивати;

знайомство з новими технологіями в ІТ- індустрії.

Зміст виробничої практики направлений на формування ***компетентностей***, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

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

КФ-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.

КФ-2. 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.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ-4. 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.

КФ-5. 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.

КФ-6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-7. 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.

КФ-8. 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.

КФ-9. 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.

КФ-10. 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.

Отримані знання і практичний досвід під час виробничої практики стануть складовими наступних **результатів навчання** за спеціальністю 125 «Кібербезпека та захист інформації»:

РН-1. 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.

РН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН-3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН-4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН-5. 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.

РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН-9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН-11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН-12. 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.

РН-13. 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.

РН-14. 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.

РН-15. 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.

РН-16. 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.

РН-17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.

РН-18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

РН-19. 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.

РН-20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН-21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН-22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати

достовірність результатів досліджень, аргументувати висновки.

РН-23. 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.

БАЗА ПРАКТИКИ

Виробнича практика студентів закладів вищої освіти проводиться на підприємствах (організаціях, установах, компаніях), що мають відповідати вимогам програми. З базами практики (підприємствами, організаціями, установами будь-яких форм власності) Державний університет "Житомирська політехніка" завчасно укладають договори на її проведення. Приклад типового договору на проведення виробничої практики наведено у додатку 1.

2. Зміст практики

Виробнича практика є обов'язковою формою поглибленого навчання в системі підготовки фахівців за ступенем вищої освіти «магістр».

Зміст виробничої практики повинен забезпечувати виконання мети і всіх завдань програми підготовки магістрів. Перед початком практики кожен студент отримує індивідуальне завдання на період практики, яке підписується студентом і керівником практики. Основні завдання практики відображаються в індивідуальному графіку. Під час практики студент повинен ознайомитись з проблемою створення, експлуатації та захисту сучасних комп'ютерних систем, які використовуються на підприємствах (організаціях, установах) за місцем практики, ознайомитись з політиками безпеки, засобами та пакетами програм, які використовуються для забезпечення безпеки інформації. У ході роботи відповідно до отриманого індивідуального завдання студент повинен вести щоденник практики та написати звіт з виробничої практики.

Зміст виробничої практики:

№ з/п	Найменування розділів практики і перелік виконуваних робіт	Кількість годин
	Розділ 1. Техніка безпеки і охорона праці	**6**
1	Техніка безпеки і охорона праці на базі практики Знайомство з правилами внутрішнього розпорядку підприємства, інструктаж з техніки безпеки та охорони праці, бесіда спеціалістів.	2
2	Вивчення техніки безпеки і охорони праці у структурному підрозділі	2

3	Вивчення техніки безпеки і охорони праці на робочих місцях. Інструктаж з техніки безпеки та охорони праці на робочому місці.	2
	Розділ 2. Загальні відомості про об'єкт практики	**12**
4	Знайомство з підприємством. Екскурсія по відділам підприємства та службам, що забезпечують його роботу.	2
5	Вивчення роботи основних структурних підрозділів.	2
6	Ознайомлення з обчислювальним центром підприємства (організації, установи, компанії).	2
7	Ознайомлення з підрозділами підприємства. Вивчення особливостей роботи окремого структурного підрозділу	2
8	Вивчення запропонованої керівником документації (вимоги, стандарти, звіти) у сфері кібербезпеки, які можуть бути необхідні або корисні при виконанні навчально-виробничих завдань.	2
9	Вивчення процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур на підприємстві (в організації чи установі).	2
	Розділ 3. Виконання обов'язків згідно посади практики на підприємстві (організації, установі, компанії)	**102**
10	Ознайомлення з обов'язками згідно з місцем роботи у підрозділі підприємства (організації, установи, компанії).	4
11	Робота дублером фахівця з захисту інформації.	4
12	Робота зі стандартним обладнанням та програмним забезпеченням.	4
13	Робота в середовищі сучасних операційних систем та баз даних.	4
14	Налаштування обладнання комп'ютерних систем та мереж, апаратних, програмних, локальних та мережевих засобів, між мережевих екранів.	6
15	Робота дублером адміністратора комп'ютерних систем та мереж.	4
16	Обслуговування засобів комп'ютерних систем та мереж	6
17	Аналіз працездатності мереж та пошук в них вразливостей за допомогою спеціального програмного забезпечення.	6
18	Робота дублером ремонтника апаратних засобів комп'ютерних систем та мереж.	6
19	Аналіз апаратних засобів комп'ютерних систем та мереж.	6

20	Аналіз апаратних засобів комп'ютерних систем та мереж спеціальним програмним забезпеченням.	8
21	Аналіз вразливостей комп'ютерних систем та мереж	6
22	Визначення задач захисту інформації, що обробляється в інформаційно-телекомунікаційних системах підприємства (організації, установи), що використовують чи потребують використання сучасних методів та засобів криптографічного захисту інформації.	6
23	Аналіз та оцінка ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в згідно встановленої політики інформаційної та\або кібербезпеки.	8
24	Розробка рекомендацій щодо покращення захищеності комп'ютерних систем та мереж	8
25	Розробка пропозицій по заходах з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах підприємства (організації, установи).	8
26	Розробка пропозицій щодо реалізації комплексної системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів.	8
	Розділ 4. Робота над індивідуальним завданням	**40**
27	Виконання теоретичної частини (розбір статей, інформаційних схем, комп'ютерних програм і відповідної документації, пошук інформації з літератури та Інтернету, складання оглядів і т.п.).	10
28	Виконання практичної частини.	10
29	Підбір фактичного матеріалу на підприємстві (організації, установі, компанії) для написання курсових і наукових робіт.	10
30	Вирішення інших питань відповідно до індивідуального завдання.	10
	Розділ 5. Підготовка і оформлення звітних матеріалів	**20**
31	Заповнення щоденника виробничої практики.	4
32	Отримання відгуку керівника практики від підприємства.	2
33	Отримання відгуку керівника практики від університету.	2
34	Узагальнення та систематизація матеріалу щодо	6

	проходження виробничої практики.	
35	Оформлення звіту з виробничої практики.	6
	Диференційований залік	
	Всього	**180**

3. Форми та методи контролю

Після закінчення терміну практики студенти звітують про виконання програми та індивідуального завдання.

Форма звітності студента за практику – подання звіту та щоденника практики, оцінених і підписаних керівником практики від підприємства (організації, установи).

Звіт разом з щоденником практики подається на рецензування відповідальному за організацію виробничої практики на кафедрі.

Звіт має містити відомості про виконання студентом усіх розділів програми практики та індивідуального завдання, висновки і пропозиції, список використаної літератури тощо.

Звіт захищається студентом у комісії, призначеній завідувачем кафедри. До складу комісії входять відповідальний за організацію виробничої практики на кафедрі, викладач-керівник студента та керівник практики від підприємства (організації, установи).

Комісія приймає диференційований залік у студентів у встановленому порядку згідно розкладу.

Студент, який не виконав програму практики без поважних причини, відраховується з навчального закладу.

Якщо програма практики не виконана студентом з поважної причини, то навчальним закладом надається можливість студенту проходження практики повторно через рік. Таке ж право надається і студенту, який на підсумковому заліку отримав негативну оцінку.

4. Вимоги до оформлення звіту

Всі матеріали як графічні так і текстові, зібрані в період виробничої практики, повинні бути розміщені по розділам, пронумеровані і зброшуровані у вигляді єдиного звіту. Обсяг звіту від 20 до 30 сторінок.

Документацію оформляють відповідно до ДСТУ 3008-95 на стандартних аркушах паперу з однієї сторони. Одиничний інтервал. Відступи від країв аркуша: зверху, знизу і зліва – 20 мм; справа – 10 мм. Абзац – 5 знаків.

Нумерація сторінок проставляється у правому верхньому кутку, починаючи

зі змісту (за першу сторінку приймається титульний лист). Заголовки структурних частин, розділів великими літерами посередині рядка, всі інші з абзацу малими літерами починаючи з великої.

Слово “Додатки” малими літерами з першої великої посередині рядка.

Звіт повинний мати титульний лист, зразок якого приводиться в додатку 2.

Звіт підписується керівником від підприємства і завіряється печаткою. Після повернення в університет на кафедру протягом тижневого терміну студент захищає звіт перед спеціально призначеною комісією.

5. Критерії оцінювання практики

Результат заліку за практику вноситься в заліково-екзаменаційну відомість і в залікову книжку студента за підписом відповідального за практику і враховується стипендіальною комісією при визначенні розміру стипендії разом з його оцінками за результатами підсумкового контролю.

Підсумкова оцінка знань, умінь та навичок студента, набутих на практиці, встановлюється за 100-баловою шкалою, національною шкалою та шкалою ЄКТС.

За шкалою	Диференційований залік	Бали
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73
E		60-63
FX	Незадовільно	35-59
F		0-34

Критерії виставлення оцінок при захисті звітів з практики

Вимоги	**Кількість балів**
Зміст, оформлення звіту й щоденника відповідають стандартам. Характеристика студента позитивна. Повні та точні відповіді на всі питання членів комісії щодо програми практики і виконаної індивідуальної роботи	90-100
Несуттєві зауваження щодо змісту та оформлення звіту й щоденника. Характеристика студента позитивна. У відповідях на запитання членів комісії з програми практики студент припускається окремих неточностей, хоча загалом має тверді знання.	74-89
Недбале оформлення звіту і щоденника. Переважна більшість питань програми практики висвітлена, однак мають місце окремі розрахункові й логічні помилки. Характеристика студента в цілому позитивна. При відповідях на запитання членів комісії з практики студент почувається невпевнено, збивається, припускається помилок, не має твердих знань	60-73
У звіті висвітлені не всі питання, або підготовлена не самостійно. Оформлення роботи є недбалим. Ілюстративний матеріал до захисту відсутній. Характеристика студента стосовно ставлення до практики і трудової дисципліни негативна. На запитання членів комісії студент не може дати задовільних відповідей	1-59

6. Рекомендована література

1. Закон України «Про вищу освіту» від 01.07.2014 р. № 1556-VII (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст. 2004).
2. Положення «Про проведення практики студентів вищих навчальних закладів України», затвердженого наказом Міністерства освіти України від 08.04.1993 р. № 93.
3. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 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 №373.
6. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі .
7. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
8. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
11. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
12. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
13. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
14. 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.
15. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
16. Корченко О.Г. Прикладна криптологія : системи шифрування: підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К.: ДУТ - ТОВ "Наш формат", 2014. – 448 с.: іл.

17. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво "Форт", 2012. – 880 с.: іл.
18. 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
19. 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.

Додаток 1

ДОГОВІР № ____
про проведення практики студентів
вищого навчального закладу

м. Житомир "___" _____ 20 р.

Ми, що нижче підписалися, з однієї сторони Державний університет «Житомирська політехніка», в особі ректора Євдокимова В.В., діючи на підставі Статуту Державного університету «Житомирська політехніка» і, з іншої сторони _____
_____
(назва підприємства, організації, установи)

(надалі – база практики) в особі_____
(посада, прізвище та ініціали)
діючого на підставі_____(далі – сторони),
(статут підприємства, розпорядження, доручення)

уклали між собою договір:

1. База практики зобов'язується:

1.1. Прийняти студентів на практику згідно з календарним планом:

№	Шифр і назва спеціальності	Курс	Вид практики	ПІБ студента	Кількість студентів	Строки практики	
						початок	закінчення
1.	125 «Кібербезпека та захист інформації»	3, група **ХХХ-ХХ**	Виробнича практика	**Петренко Петро Петрович**	1	06.01.20	31.01.20

1.2. Призначити наказом кваліфікованих фахівців для керівництва практикою.

1.3. Створити належні умови для виконання студентами програми практики, не допускати їх використання до зайняття посад та 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: ввідний та на робочому місці. У разі потреби навчати студентів-практикантів безпечних методів праці.

1.5. Надати студентам-практикантам 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 вищий 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 інформації для курсових та дипломних робіт за результатами діяльності підприємства, яка не є комерційною таємницею, на підставі направлень кафедр.

1.9. Додаткові умови_____Відсутні_____

2. Вищий навчальний заклад зобов'язується:

2.1. До початку практики надати базі практики для погодження програму практики, а не пізніше ніж за тиждень – список студентів, яких направляють на практику.

2.2. Призначити керівниками практики кваліфікованих викладачів.

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

2.4. Практика проводиться на **безоплатній основі**.

2.5. Навчальний заклад зобов'язується не розголошувати використану інформацію про діяльність підприємства через знищення курсових, дипломних робіт та звітів у встановленому порядку.

2.6. Додаткові умови_____відсутні_____

3. Відповідальність сторін за невиконання договору:

3.1. Сторони відповідають за невиконання покладених на них обов'язків щодо організації і проведення практики 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 практики згідно з календарним планом.

3.4. Договір складений у двох примірниках: по одному – базі практики і вищому навчальному закладу.

3.5. Місцезнаходження:

Підписи та печатки

Державний університет «Житомирська політехніка»: вул. Чуднівська, 103, м. Житомир, 10005 тел. (0412) 24-14-22	База практики: _____ _____ _____
Ректор університету _____ В.В.Євдокимов	База практики _____/_____
"__" _____ 20__ р.	"___" _____ 20__ р.

Додаток 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет "Житомирська політехніка"
Кафедра комп'ютерної інженерії та кібербезпеки

ЗВІТ З ВИРОБНИЧОЇ ПРАКТИКИ

Студента (ки) __ курсу групи _____
Галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека та захист інформації»
ступінь «**магістр»**

_____
(прізвище ініціали, підпис)

Керівник практики:

Кількість балів: ___ Національна оцінка: ____ ECTS:___

Члени комісії:

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

Житомир – 20__