МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

МЕТОДИЧНІ ВКАЗІВКИ

до проведення виробничої практики

для студентів денної та заочної форм навчання
першого (бакалаврського) рівня вищої освіти за спеціальностями
125 (F5) “Кібербезпека та захист інформації”, 256 (K3) “Національна безпека
(за окремими сферами забезпечення і видами діяльності) ” та
257 (K4) “Управління інформаційною безпекою”

Затверджено
редакційно-видавничою
радою університету,
протокол № 3 від 30.10.2025 р.

Харків
НТУ “ХПІ”
2025

Методичні вказівки до проведення виробничої практики для студентів денної та заочної форм навчання першого (бакалаврського) рівня вищої освіти за спеціальностями 125 (F5) “Кібербезпека та захист інформації”, 256 (K3) “Національна безпека (за окремими сферами забезпечення і видами діяльності)” та 257 (K4) “Управління інформаційною безпекою” / уклад.: Р. В. Корольов, А. М. Ткачов, А. А. Гаврилова – Харків: НТУ “ХПІ”, 2025. – 35 с.

Укладачі: Р. В. Корольов,
А. М. Ткачов,
А. А. Гаврилова

Рецензент Д. А. Кудій

Кафедра кібербезпеки

ВСТУП

Виробнича практика, яка проводиться для бакалаврів денної та заочної форм навчання за спеціальностями 125 (F5) “Кібербезпека та захист інформації”, 256 (К3) “Національна безпека (за окремими сферами забезпечення і видами діяльності) ” та 257 (К4) “Управління інформаційною безпекою”, входить до складу профільних дисциплін та повинна проходити у строки, які встановлені в графіку навчального процесу.

Для взаємопов′язування початку навчання за спеціальностями з практичною реалізацією призначено виробничу практику. Виробнича практика, яка проводиться на третьому курсі та другому році навчання на базі молодшого спеціаліста, є зовнішньою і призначена для ознайомлення студентів із вирішенням завдань за прикладними питаннями вивчених профільних дисциплін стосовно реалізації основних процесів захисту інформації щодо баз практики, якими можуть виступати виробничі та невиробничі об’єкти економічної діяльності України.

За результатами проходження виробничої практики формується взаємозв’язок між теорією та практикою дисциплін, що викладалися на першому, другому та третьому курсах з питань методів аналізу протидії сучасним гібридним атакам, оцінки поточного рівня безпеки та вибору механізмів протидії при дослідженні стану предметної області на базі практики, аналізу інфраструктури мережі, технічних засобів комплексної системи захисту інформації, можливості її удосконалення в умовах дії сучасних загроз.

За виробничою практикою в методичних рекомендаціях вказані організаційні, змістовні та звітні аспекти реалізації досягнення мети практики.

1 ЗАГАЛЬНИЙ ОПИС ПРАКТИКИ

Денна/ заочна форма навчання денна та заочна

Курс: 3 (2)

Семестр 6 (4)

Кількість тижнів 4

Загальна кількість годин / кредитів 180/6

Робочий *(в аудиторії або на підприємстві)* час практиканта *(години)* 30

Самостійна робота (години) 180

Вид контролю: диференційований залік

Орієнтовні бази практики:

державні, муніципальні, громадські, комерційні і некомерційні організації чи підприємства, де можливий збір і вивчення матеріалів, пов'язаних з аналізом стану безпеки інформаційних ресурсів, а також у навчальних та наукових підрозділах університету за напрямом підготовки студентів

Обов'язки здобувача вищої освіти:

– повністю виконати завдання, передбачені програмою практики;

– виконувати чинні на підприємстві правила внутрішнього розпорядку;

– пройти інструктаж і суворо дотримуватися правил охорони праці, техніки безпеки і виробничої санітарії;

– виконувати та нести відповідальність за виконану роботу на підприємстві за дорученням керівника практики нарівні зі штатними співробітниками;

– вести щоденник практики за етапами її проходження;

– подати на кафедру письмовий звіт про виконання виробничої практики та індивідуального завдання разом із відгуком, підписаним керівником (куратором) практики від підприємства;

– підготувати та надати на кафедру в електронному вигляді презентацію докладу за результатами звіту;

– захистити основні положення, відображені у звіті.

Обов’язки керівника практики:

– надає консультації студентам за попередньо узгодженим графіком та проводить перевірку проходження практики студентами та надає їм консультації на тих базах практики, які зазначені в графіку виїзду;

– встановлює зв′язок із керівниками практики від організації і спільно з ними складає робочу програму проведення практики;

– сприяє формуванню загальної схеми виконання завдання, графіка проведення практики, режиму роботи студентів і здійснює систематичний контроль ходу практики і роботою студентів;

– бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

– несе відповідальність разом із керівником практики від організації за дотримання студентами правил техніки безпеки;

– здійснює контроль дотримання термінів практики та її змісту;

– надає методичну допомогу студентам під час виконання ними поставлених завдань і збору матеріалів для курсової роботи з веббезпеки;

– оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента

– координує самостійну роботу студентів за завданнями практики у період її проходження щодо збору необхідних матеріалів, надає відповідну консультаційну допомогу;

– дає рекомендації щодо вивчення спеціальної літератури;

– бере участь у роботі конференції з ведення підсумків виробничої практики

2 МЕТА І ЗАВДАННЯ ВИРОБНИЧОЇ ПРАКТИКИ

Виробнича практика є частиною навчального процесу й організовується для студентів 3 (2) курсу денної та заочної форм навчання за спеціальностями 125 (F5) “Кібербезпека та захист інформації”, 256 (K3) “Національна безпека (за окремими сферами забезпечення і видами діяльності)” та 257 (K4) “Управління інформаційною безпекою” у 6-му (4-му) семестрі.

Мета практики – забезпечення єдності теоретичного та практичного навчання студентів з питань використання методів аналізу протидії сучасним гібридним атакам, оцінки поточного рівня безпеки та вибору механізмів протидії при дослідженні стану предметної області на базі практики, аналізу інфраструктури мережі, технічних засобів комплексної системи захисту інформації, можливості її удосконалення в умовах дії сучасних загроз.

Завданнями практики є:

1) закріплення, поглиблення та доповнення теоретичних знань, які набуваються під час засвоєння дисциплін:

a) “Математичні основи криптології”, “Фізичні основи технічних засобів розвідки”, “Правове регулювання кібербезпеки”, “Комп'ютерні мережі”, “Основи криптографічного захисту”;

b) “Цифрова криміналістика”, “Безпека в інформаційно-комунікаційних системах”, “Організація документообігу з обмеженим доступом”, “Основи математичного моделювання систем безпеки”;

2) підготовка до вивчення профілюючих дисциплін: “Безпека інтернет-речей”, “Веббезпека”, “Комплексні системи захисту інформації”, “Антивірусний захист інформації”, “Основи машинного навчання для кібербезпеки”, “Інформаційно-комунікаційні системи у сфері національної безпеки”, “Промисловий та офісний шпіонаж”, “Гібридні війни та національна безпека», “Інтернет-розвідка”;

3) збір матеріалів для виконання курсового проєкту за дисципліною

“Веббезпека”.

Під час проходження практики необхідно зібрати матеріал у рамках поставленої керівником задачі та виконати наступне:

1) навести схему організаційної структури підприємства з вказівкою які інформаційні ресурси обробляються в мережі, технічні засобі та програмні застосунки забезпечення безпеки даних. Окремо вказати місце підрозділу, де безпосередньо проходитиме практика, склад посадових осіб конкретного підрозділу та їх функції, вказати завдання, які вирішує кожний структурний підрозділ згідно штатного розкладу та інформаційні зв’язки цього підрозділу з ближнім оточенням;

2) навести опис існуючої інформаційної системи/модулів яка/які використовуються для автоматизації вирішення певних завдань і яка/які є тими, що треба захищати, вказати наслідки несанкціонованого доступу до неї/них; описати використовувану систему управління інформаційною безпекою та існуючі технічні засоби для забезпечення безпеки даних;

3) навести перелік та надати характеристику загроз, які представляють небезпеку для бази практики та представити наслідки кожної загрози для управління її діяльності;.

4) подати опис основних термінів за звітом у вигляді глосарію; надати характеристику бази практики з врахуванням її розташування (кількість будівель та приміщень, їх поверховість, відстань між ними) та розміщення серверних й інших місць для зберігання інформації та її оброблення, результати навести у вигдяді топології мережі, яку сформувати за допомогою засобів Packet Traker та надати опис, вказати за допомогою яких складових схеми забезпечується захист інформації; провести аналіз контуру системи безпеки бази практики та привести сучасні підходи щодо підвищення її рівня безпеки;

5) сформувати висновки та пропозиції щодо розроблення або удосконалення профілів безпеки окремого робочого місця працівника бази практики.

Глосарій представити в табл. 1.

Таблиця 1 – Глосарій за звітом

Термін	Опис терміну
1. Основні поняття та категорії предметної області	
2. Користувачі системи	
3. Загрози щодо системи	
4. Програмні застосунки виявлення аномалій від нормальної роботи	
5. Основні заходи політики безпеки організації	

Контур системи безпеки <об’єкту> складають засоби його захисту, які представлені п’ятьма групами:

1)фізичні засоби захисту,

2)технічні засоби захисту,

3)апаратні засоби захисту,

4)програмні засоби захисту,

5)адміністративні засоби захисту.

Кожну із груп складають інструменти захисту, наявність яких на <об’єкті> демонструє рівень захисту. В табл. 4.1 представлено зміст кожної групи захисту.

Таблиця 2 – Визначення рівнів захисту контуру системи безпеки за групами засобів захисту та <об’єктом> в цілому

№ з/п	Засіб захисту	Наявність (так=1/ні=0)
1	2	3
І ФІЗИЧНІ ЗАСОБИ ЗАХИСТУ		
1	електронні замки	
2	спеціально посилені двері	
3	спеціальні перегородки і кабіни	
4	грати на вікнах	
5	екранувальні екрани	
6	огорожі	

Закінчення табл. 2

1	2	3
II ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ		
1	електронні засоби відеоспостереження та сигналізації	
2	лазерні, оптичні, інфрачервоні сигналізації при проникненні в приміщення	
III АПАРАТНІ ЗАСОБИ ЗАХИСТУ		
1	смарт-картки	
2	USB-токени	
3	апаратні криптографічні модулі	
4	ключі безпеки	
IV ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ		
1	програми-детектори	
2	програми-лікарі	
3	програми-ревізори	
4	програми-фільтри	
5	програми-вакцини	
V АДМІНІСТРАТИВНІ ЗАСОБИ ЗАХИСТУ		
1	вимоги щодо використання, надання, скасування та контролю доступу до інформаційної системи об'єкта	
2	вимоги до забезпечення захисту від зловмисного коду та організації захисту від зловмисного коду	
3	використання криптографічних засобів для захисту інформації	
4	вимоги щодо використання електронної корпоративної пошти	
5	вимоги щодо використання пристроїв для робочих цілей	
6	вимоги щодо процесу управління інцидентами інформаційної безпеки	

За представленою табл. 2 провести аналіз контуру системи безпеки <об’єкту> як за кожною групою, так й комплексно за <об’єктом> в цілому.

Всі відповіді щодо наявності складових зазначити через 1 (“так”) та через 0 (“ні”).

За кожною групою засобів захисту визначити рівень контуру безпеки системи <об’єкту>:

$$R_K = \frac{\sum_{k=1}^{K} x_{k_i}}{N_k}, \qquad (1)$$

де x – i-ий елемент захисту k-ої групи засобів захисту;

K – кількість груп засобів захисту;

N_k – кількість елементів захисту в k-ій групі засобів захисту.

Визначити комплексний показник рівня захищеності контуру системи безпеки <об’єкту>:

$$R_{заг} = \frac{\sum_{i=1}^{N}\sum_{k=1}^{K} x_{k_i}}{N}, \qquad (2)$$

де N – загальна кількість елементів захисту.

Провести оцінку отриманих значень за такою шкалою:

- для фізичних засобів захисту:

значення	якісний опис
x=6	необхідний рівень
6<x>3	середній рівень
x<=3	низький рівень

- для технічних засобів захисту:

значення	якісний опис
x=2	необхідний рівень
x<2	низький рівень

- для апаратних засобів захисту:

значення	якісний опис
x=4	необхідний рівень
x<4	низький рівень

- для програмних засобів захисту:

значення	якісний опис
x=5	необхідний рівень
x<5	низький рівень

- для адміністративних засобів захисту:

значення	якісний опис
x=23	високий рівень
23<x>12	прийнятний рівень
x=12	середній рівень
12<x>10	задовільний рівень
x=10	низький рівень
x<10	критично низький рівень

- для комплексного показника показник рівня захищеності контуру системи безпеки <об’єкту>:

значення	якісний опис
x=23	необхідний рівень
23<x>12	прийнятний рівень
x=12	середній рівень
12<x>10	задовільний рівень
x=10	низький рівень
x<10	критично низький рівень

Кібербезпека – це захист комп’ютерних систем від крадіжки або пошкодження зловмисниками через Інтернет. Вона включає різні аспекти захисту мережі, програмного забезпечення та даних.

На відміну від цього, інформаційна безпека зосереджена на захисті даних, як фізичних (документи, флешки), так і цифрових (файли, бази даних). Інформаційна безпека є особистою відповідальністю кожного працівника і є першим бар’єром на шляху до захисту критично важливої інформації.

Тому, на сьогодні, сучасними підходами щодо підвищення рівня безпеки є:

1) надійні паролі та двофакторна автентифікація;

Використання надійних паролів і двофакторної автентифікації є основою безпеки. Паролі повинні бути унікальними для кожного облікового запису і містити літери, цифри та спеціальні символи. Двофакторна автентифікація додає додатковий рівень безпеки, ускладнюючи зловмисникам доступ до даних.

2) регулярне оновлення програмного забезпечення;

Системне, прикладне та антивірусне програмне забезпечення слід

регулярно оновлювати. Ці оновлення не лише покращують функціональність, але й усувають вразливості, якими можуть скористатися зловмисники.

3) безпека приватної/корпоративної електронної пошти;

Фішингові атаки залишаються одним із найпоширеніших методів, які використовують зловмисники. Треба з уважністю відноситися до підозрілих електронних листів, не відкривати вкладення від невідомих відправників і не переходити за підозрілими посиланнями.

4) безпечне зберігання даних;

Важливу інформацію слід зберігати на зашифрованих носіях або у хмарних сервісах із надійними засобами захисту. Не рекомендується залишати конфіденційні дані на робочих столах або в легкодоступних місцях.

5) навчання та обмін досвідом.

Інформаційна безпека – це не лише індивідуальна, але й колективна відповідальність. Підтримання культури безпеки на робочому місці, регулярне проходження курсів з безпеки та розповсюдження своїх знань між колегами. Організація семінарів для обговорення нових загроз і методів захисту.

Профіль безпеки (ПБ) – набір заходів захисту, які застосовуються до інформації або інформаційної системи для задоволення вимог чинної нормативної бази, а також спрямовані на захист потреб з метою управління ризиками безпеки.

Тому, надати опис заходам захисту, які не використовуються, але повинні використовуватися на <об'єкті> для забезпечення інформаційної безпеки (конфіденційність, цілісність, доступність), безпеки застосунків (програм, даних) та безпеки мереж (технічний стан). Визначити чого не вистачає для необхідного профілю безпеки та яким чином ліквідувати цю нестачу.

Для організації виконання заходів кіберзахисту для <об'єкта> повинно бути розроблено 2 профілі кібербезпеки – поточний і цільовий. Для їх розробки необхідно провести оцінку ризиків, що впливають на порушення стандартного режиму функціонування об'єкту.

Поточний профіль кібербезпеки – відображає поточний стан кіберзахисту об’єкта. Цільовий профіль кібербезпеки – описує бажані результати із забезпечення кібербезпеки (сучасні практики захисту, сучасні практики управління ризиками, поточне середовище ризику, правові та нормативні вимоги, цілі діяльності та завдання, організаційні обмеження).

Приклад

Поточна практика захисту віддаленого доступу включає:

а) використання зашифрованої віртуальної приватної мережі (VPN) з одночасним використанням цифрового сертифікатута авторизації (логін, пароль);

б) доступ до VPN надається тільки для затверджених установою користувачів;

в) доступ до VPN надається тільки для затверджених установою сервісів;

г) доступ до VPN заборонений за допомогою програм TeamViewer, AnyDesk, RDP-з’єднань тощо.

Цільова практика захисту віддаленого доступу включає:

а) використання зашифрованої віртуальної приватної мережі (VPN) з одночасним використанням цифрового сертифікатута авторизації (логін, пароль);

б) доступ до VPN надається тільки для затверджених установою користувачів;

в) дані про VPN-акаунти оновлюються кожен рік (відключаються, видаляються, продовжуються);

г) доступ до VPN надається тільки для затверджених установою операційних систем;

д) доступ до VPN надається тільки після проведення антивірусних заходів;

є) доступ до VPN надається тільки для затверджених установою сервісів;

е) кожен VPN-акаунт ідентифікований (за IP-адресою, MAC-адресою тощо);

ж) доступ до VPN заборонений за допомогою програм TeamViewer, AnyDesk, RDP-з’єднань тощо;

з) діяльність під час надання віддаленого доступу записується та контролюється;

і) усі спроби несанкціонованого підключення до VPN реєструються;

к) встановлено обмеження щодо тривалості VPN-сесії.

За наведеним прикладом визначити поточний та цільовий профіль кібербезпеки на <об’єкті>.

Також вказати способи вирішення поставлених завдань та досягнення мети, а також надати пояснення щодо отриманих результатів.

3 КОМПЕТЕНТНОСТІ СТУДЕНТА

Після проходження практики студент повинен

знати:

– методи та засоби формування політики безпеки;

– засади проєктування баз даних;

– засади побудови комплексної системи захисту інформації;

– типи організації виробництва та їх характеристику;

– структурні, процесні, статистичні методи дослідження предметної області за завданням;

– засади проєктування системи безпеки робочого місця користувача;

– структуру та зміст технічного, програмного, програмно-апаратного забезпечення безпеки даних у системі;

вміти:

– аналізувати використовувану систему управління інформаційною безпекою;

– оцінювати існуючі технічні засоби для забезпечення безпеки даних;

– надавати характеристику загроз, які представляють небезпеку та представити наслідки кожної загрози для управління діяльністю;

– визначати критичні місця в мережі організації;

– створювати засобами Packet Traker топологію мережі із зазначенням складових безпеки;

– визначати рівні захисту контуру системи безпеки за групами засобів захисту та за об’єктом в цілому;

– проєктувати профіль безпеки для окремого користувача;

– складати звіт з аналізу поточного стану безпеки окремого користувача в системі згідно із встановленими правилами та вимогами;

придбати навички:

– спілкування з адміністративним апаратом організації для пошуку відповідей за питаннями практики;

– використання системного підходу щодо формування профілю безпеки, аналізу можливих загроз, технічних засобів протидії;

– обґрунтування необхідності та можливості удосконалення або розробки нових заходів із забезпечення захисту інформації.

4 ЗМІСТ ПРАКТИКИ

Перед початком практики проводяться консультаційні збори, на яких надається вся необхідна інформація з порядку проведення виробничої практики та консультація з техніки безпеки. За результатами зборів студенти заповнюють щоденники, в яких наводять: відомості про себе, назву бази практики, вид практики, період проходження практики, календарний графік із переліком запланованих до виконання робіт (додаток А). Календарний графік студенти завіряють підписом керівника від університету та підписом керівника від бази практики. За необхідності студентом на базу практики надається направлення від університету (додаток Б).

На першому тижні практики студент повинен:

– отримати завдання для проходження виробничої практики;

– узгодити графік консультацій зі своїм керівником на кафедрі та ознайомитися з графіком відвідувань даної бази практики уповноваженими викладачами-консультантами;

– завірити підписом календарний графік у завідуючого кафедри “Кібербезпеки” або уповноваженою ним особою (для тих, хто проходить практику на кафедрі), або у керівника іншої бази практики (для тих, хто проходить практику за межами університету/кафедри);

– завірити підписом та печаткою керівництва бази практики прибуття студента на практику;

– пройти інструктаж із техніки безпеки на базі практики.

На останньому тижні практики студент повинен:

– після закінчення терміну проходження практики за результатами виконаних робіт оформити робочі записи у щоденнику та отримати відгуки керівника від університету (додаток В) та керівника від бази практики (додаток Г);

– завірити підписом та печаткою керівництва бази практики вибуття студента з практики;

– сформувати звіт, титульний аркуш якого підписати з боку студента, керівника від університету та керівника від бази практики; якщо базою практики не є університет, то на підпис керівника від бази практики поставити печатку підприємства (організації, установи) (додаток Д).

Індивідуальний план виробничої практики студента повинен бути узгоджений з планом роботи організації, що є базою практики. У період практики студенти підкоряються всім правилам внутрішнього розпорядку і техніки безпеки, встановленим у підрозділі і на робочих місцях.

5 ЗАХОДИ КОНТРОЛЮ

Після закінчення практики студенти оформляють всю необхідну документацію відповідно до вимог програми виробничої практики табл. 3.

Таблиця 3 – Програма виробничої практики з розподілом за днями

№ з/п	Зміст роботи	Кількість днів
1	Проходження інструктажу з техніки безпеки	в перший день початку практики
2	Проведення аналізу систему безпеки ІС підприємства (організації) та її відповідність цілям та задачам бізнес-діяльності	2
3	Ознайомлення з методами реалізації НСД	3
4	Ознайомлення з методами захисту інформації від стороннього деструктивного впливу	2
5	Вивчення типових вимог щодо захисту інформації від НСД	3
6	Вивчення технічних каналів як комунікаційної складової інформаційної інфраструктури	4
7	Проведення аналізу захисту інформації в ІКС через виток її технічними каналами	5
8	Оформлення звіту згідно з ДСТУ	протягом практики

Робочий час практиканта 30 год/тиждень

Самостійна робота 180 год

За підсумками виробничої практики студент надає на кафедру:

– щоденник виробничої практики студента;

– розгорнутий звіт про результати виробничої практики, який складається з титульного листа, завдання на практику, змісту, вступу, основної частини у встановленій формі, висновків (самостійного оцінювання роботи), списку використаної літератури, додатків;

– презентацію та текст підготовленої доповіді за матеріалами виробничої практики.

Атестацію за підсумками практики проводять на підставі захисту результатів, отриманих у ході виробничої практики.

Захист звітів із виробничої практики здійснюється на захисті або на конференції, присвяченій підсумкам виробничої практики в дні, встановлені керівником від кафедри.

За підсумками захисту студенту виставляється диференційований залік згідно зі встановленою університетом шкалою оцінювання.

Оцінку за виробничу практику заносять в екзаменаційну відомість і залікову книжку, прирівнюється до оцінок (заліків) із теоретичного навчання і враховується під час підведення підсумків загальної успішності студентів.

Атестацію практики здійснюють за 100-бальною шкалою. Рівень оцінки відповідає рівню виконаної роботи і поданих матеріалів у частині опрацьованої літератури, зібраних і оброблених матеріалів, їх відповідності поставленим завданням.

Оцінка “відмінно” (90 – 100 балів) виставляється за умови повного виконання вимог з виробничої практики в становлений термін, готовності для включення поданих матеріалів у курсову роботу.

Оцінка “добре” (74 – 89 балів) виставляється в разі наявності окремих недоробок, неповноти поданих матеріалів.

Оцінка “задовільно” (60 – 73 балів) виставляється в разі некомплектного і неякісного подання матеріалів, слабкої готовності для включення в курсову роботу.

6 ВИМОГИ ДО ЗВІТУ Й ЗАХИСТУ РЕЗУЛЬТАТІВ ПРАКТИЧНОЇ ПІДГОТОВКИ

Після закінчення практики студенти складають письмові звіти і здають їх разом із щоденником практики та відгуком на студента-практиканта від керівника практики підприємства на кафедру.

Звіт про результати проходження виробничої практики складати за структурою, наведеною в табл. 4, та рекомендаціями, наданими в додатку Ж.

Таблиця 4 – Структура звіту з виробничої практики

Розділ	Кількість сторінок
Титульний аркуш	1
Завдання на виробничу практику	1
Зміст	1
Вступ	1
1 Коротка характеристика <бази практики>	4
1.1 Структурні особливості <бази практики>	2
1.2 Опис та аналіз функціонування <бази практики>	2
2 Опис існуючої інформаційної системи, системи управління інформаційної безпеки та технічних засобів забезпечення безпеки даних <бази практики>	3
3 Аналіз можливих загроз <бази практики>	3
4 Результати виконання роботи за <базою практики> під час проходження практики	4
4.1 Глосарій за звітом	1
4.2 Аналіз топології корпоративної/локальної мережі із засобами забезпечення безпеки та інформаційних ресурсів інформаційної системи <бази практики>	1
4.3 Аналіз контуру системи безпеки <бази практики>	2
5 Висновки та пропозиції щодо розроблення або удосконалення профілів безпеки окремого робочого місця працівника <бази практики>	2
Список літератури	1
Додатки	

Перший аркуш звіту з практики є титульним. Зразок його оформлення наведено в додатку Д.

Другий аркуш має назву “Завдання на практику” і повинен містити перелік завдань, які повинні бути вирішені в ході проходження практики. Цей аркуш повинен бути підписаний студентом, який має виконати ці завдання, та викладачем-керівником (додаток Е).

Рекомендації щодо оформлення звіту:

–**обсяг:** дотримуватися рекомендованого кафедрою обсягу звіту (зазвичай 20-40 сторінок без додатків);

–**оформлення:** дотримуватися вимог ДСТУ та методичних вказівок кафедри щодо оформлення звітів;

–**мова:** звіт пишеться державною мовою;

–**конфіденційність:** особливу увагу приділити питанням конфіденційності інформації, отриманої на базі практики. Не розголошувати

комерційну таємницю, персональні дані, критичні вразливості без дозволу. Усі приклади та дані мають бути узагальненими або знеособленими.

Увесь текст звіту з практики повинен бути оформлений згідно з Правилами оформлення звіту з практик кафедри кібербезпеки НТУ “ХПІ” (додаток Ж).

У рекомендованій літературі повинно бути вказано не тільки перелічені ДСТУ та законодавчі документи, які було використано під час виконання завдань практики та оформлення бібліографічного опису, але й джерела, в яких розкриваються питання предметної області, що аналізується за обраною базою практики.

Список використаної літератури необхідно оформити згідно з вимогами, представленими в додатку Ж.

СПИСОК ЛІТЕРАТУРИ

1. Інформаційні системи електронної комерції: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, К.П. Газдюк, О.Ю. Тарновецька, Л.М. Шумиляк, І.В. Аксьонова, А.А. Гаврилова. Чернівецький національний університет ім. Ю. Федьковича, Національний технічний університет "Харківський Політехнічний Інститут", Львів: Видавництво "Новий Світ-2000", 2024. 282 с.

2. Технології баз даних : навчально-практичний посібник / уклад. А. А. Гаврилова, С. С. Погасій, Р. В. Корольов, В. С. Хвостенко, Т. С. Мілевська ; за заг. ред. С. П. Євсеєва. Харків : НТУ "ХПІ", Львів : "Новий Світ-2000", 2025. 222 с.

3. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. Kharkiv: PC TECHNOLOGY CENTER, 2023. 168 p.

4. Modern Problems Of Computer Science And IT-Education: collective monograph / [editorial board K. Melnyk, O. Shmatko]. Vienna: Premier Publishing s.r.o., 2020. P. 79 – 92.

5. Synergy of building cybersecurity systems: monograph / [editer: S. Yevseiev, V. Ponomarenko, O. Laptiev and other]. Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p.

ДОДАТКИ

ДОДАТОК А

Щоденник проходження практики

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

Форма № Н-7.03.

ЩОДЕННИК ПРАКТИКИ

виробнича
(вид і назва практики)

студента Іванова Івана Івановича
(прізвище, ім'я, по-батькові)

Інститут/факультет комп'ютерних наук та інформаційних технологій

Кафедра Кібербезпеки

ступень вищої освіти бакалавр

спеціальність F5 - Кібербезпека та захист інформації
(назва)

Курс 3/2 група КН-

Рис. А 1.1 – Приклад заповнення першої сторінки щоденника з виробничої практики за спеціальністю 125 (F5) "Кібербезпека та захист інформації"

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

Форма № Н-7.03.

ЩОДЕННИК ПРАКТИКИ

виробнича
(вид і назва практики)

студента Іванова Івана Івановича
(прізвище, ім'я, по-батькові)

Інститут/факультет комп'ютерних наук та інформаційних технологій

Кафедра Кібербезпеки

ступень вищої освіти бакалавр

спеціальність К3 - Національна безпека (за окремими сферами забезпечення і видами діяльності)
(назва)

Курс 3 група КН-

Рис. А 1.2 – Приклад заповнення першої сторінки щоденника з виробничої практики за спеціальністю 256 (К3) Національна безпека (за окремими сферами забезпечення і видами діяльності)"

Продовження дод. А

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

Форма № Н-7.03.

ЩОДЕННИК ПРАКТИКИ

виробнича
(вид і назва практики)

студента Іванова Івана Івановича
(прізвище, ім'я, по-батькові)

Інститут/факультет комп'ютерних наук та інформаційних технологій

Кафедра Кібербезпеки

ступень вищої освіти бакалавр

спеціальність К4 - Управління інформаційною безпекою
(назва)

Курс 3 група КН-

Рис. А 1.3 – Приклад заповнення першої сторінки щоденника з виробничої практики за спеціальністю 257 (К4) Управління інформаційною безпекою”

Щоденник проходження практики

Студент Іванов Іван Іванович
(прізвище, ім'я, по-батькові)

Прибув на підприємство

_____
Назва підприємства

«___» _____202__р. _____
(підпис, завірений печаткою)

Посада Прізвище І.А.
(посада, прізвище та ініціали відповідальної особи)

Вибув з підприємства

_____
Назва підприємства

«___» _____202__р. _____
(підпис, завірений печаткою)

Посада Прізвище І. А.
(посада, прізвище та ініціали відповідальної особи)

Рис. А 1.4 – Приклад заповнення першої сторінки щоденника з виробничої практики

Календарний графік проходження практики

Назви робіт	Місце виконання робіт	Термін виконання тиждень (доба)	Відмітки про виконання
1	2	3	4
1. Проходження інструктажу з техніки безпеки		12.05.2025	виконано
2. Проведення аналізу систему безпеки ІС підприємства (організації) та її відповідність цілям та задачам бізнес-діяльності		13.05 –14.05.2025	виконано
3. Ознайомлення з методами реалізації НСД		15.05 – 16.05.2025 19.05.2025	виконано
4. Ознайомлення з методами захисту інформації від стороннього деструктивного впливу		20.05 – 21.05.2025	виконано
5. Вивчення типових вимог щодо захисту інформації від НСД		22.05 – 23.05.2025	виконано
6. Вивчення технічних каналів як комунікаційної складової інформаційної інфраструктури		26.05 – 28.05.2025	виконано
7. Проведення аналізу захисту інформації у ІКС через виток її технічними каналами		29.05 – 30.05.2025	виконано
8. Оформлення звіту згідно з ДСТУ			виконано

Рис. А 1.5 – Приклад заповнення сторінки з календарного планування щоденника з виробничої практики

ДОДАТОК Б

Направлення на виробничу практику

КЕРІВНИКУ

НАПРАВЛЕННЯ НА ПРАКТИКУ

(є підставою для зарахування на практику)

Згідно з договором від “____” _____ 20___ р. № _____,

який укладено з _____,

(повне найменування підриємства, організації, установи)

направляємо на практику студентів ___ курсу, які навчаються за спеціальністю

_____

освітньою програмою_____

Назва практики _____

Строки практики з _____по _____20___р.

Керівник практики від кафедри _____

(назва кафедри)

_____,

(посада, прізвище, ім’я, по батькові)

ПРІЗВИЩА, ІМЕНА ТА ПО БАТЬКОВІ СТУДЕНТІВ	ДОДАТКОВА ІНФОРМАЦІЯ

М.П. Керівник виробничої

Практики НТУ “ХПІ” _____ _____

(підпис) (прізвище та ініціали)

ДОДАТОК В

Відгук керівника від університету про проходження виробничої практики

У відгуку керівника практики від університету обов'язково повинно бути зазначено таке:

- вказується відповідність виконання поставлених завдань встановленим строкам календарного графіка;
- наголошується на ступені повноти вирішення питань, які розглядаються в роботі;
- звертається увага на обсяг і якість виконаної студентом роботи,
- звертається увага на своєчасність і правильність ведення щоденника практики;
- зазначається обов'язковість відвідування консультацій, які проводив керівник;
- ураховуються відгуки спеціалістів із бази практики, які надаються керівнику під час відвідування бази практики.

ДОДАТОК Г

Відгук куратора практики від підприємства

У відгуку керівника практики від підприємства повинно бути зазначено таке:

- повнота виконання студентом програми проходження виробничої практики;
- якість написання студентом звіту про проходження практики, його відповідність установленим вимогам, реаліям бази практики;
- рівень підготовленості практиканта до професійної діяльності за теоретичними знаннями і практичними навичками;
- відношення студента до роботи, його організованість і дисциплінованість;
- практична значимість пропозицій практиканта, викладених у звіті, щодо поліпшення певних аспектів завдань, що вирішуються тощо;
- вміння працювати в колективі, рівень комунікабельності, громадську позицію та інші особисті риси, що проявились під час практики.

ДОДАТОК Д

Титульний аркуш з виробничої практики

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ “ХПІ”

Кафедра кібербезпеки

Оцінка
_____
Голова комісії
_____
_____
“__” _____ 202__р.

ЗВІТ

з виробничої практики

на базі практики “_____”
(повна назва підприємства/організації)

Керівник практики
(від університету) _____ _____
(підпис) (ПІБ)

Керівник практики
(від бази практики) _____ _____
(підпис, печатка) (ПІБ)

Виконавець
студент гр. _КН-__ _____ _____
(підпис) (ПІБ)

ХАРКІВ – 20___

ДОДАТОК Е

Шаблон завдання на виконання практики

Міністерство освіти і науки України
Національний технічний університет “ХПІ”
Кафедра кібербезпеки

ЗАВДАННЯ НА ПРАКТИКУ

1. Опис та загальна характеристика предметної області, що розглядається
2. Аналіз загроз на елементи/об’єкти структури бізнес-процесів предметної області
3. Аналіз механізмів захисту елементів/об’єктів структури бізнес-процесів предметної області

Термін видачі завдання “___” _____ 20__ р.

Термін захисту практики “___” _____ 20__ р.

Найменування бази практики _____

Керівник практики
(від університету) _____ _____
(підпис) (ПІБ)

Виконавець
студент гр. КН-_____ _____ _____
(підпис) (ПІБ)

ДОДАТОК Ж

Правила оформлення звіту

Інтервал	Звіт формують на одному боці аркуша білого паперу формату А4 (210х297 мм) через 1,5 міжрядкового інтервалу; зверху, знизу – 0 пт
Шрифт	Times New Romal, кегель – мітел (14 типографських пунктів).
Абзацний відступ	1,25 см
Відступи	Ліворуч, праворуч – 0 см
Поля	Текст звіту необхідно формувати, залишаючи поля таких розмірів: ліве – 25 мм, праве – 10 мм, верхнє – 20 мм, нижнє – 20 мм
Розділи	Вступ, Висновки, Зміст, Список літератури, Назва розділу – великими літерами, посередині нового аркуша без абзацного відступу: **1 НОВА ЕРА** …
Підрозділи	Назва підрозділу – з першої великої літери, інші літери – маленькі, з абзацного відступу, вирівнюти з а шириною: **1.1 Опис**… Пустий рядок перед та після назви розділу.
Рисунки	Посилання на рисунок: статистикою, що представлена у звіті, щороку кількість скарг (або інцидентів) зростає, при цьому значно інтенсивніше й підвищуються збитки від успішно впроваджених загроз, ШПЗ, тощо (рис 1.1). Пустий рядок від рисунку зверху та знизу, рисунок – посередині, підпис під рисунком без пустого рядка посередині аркуша:

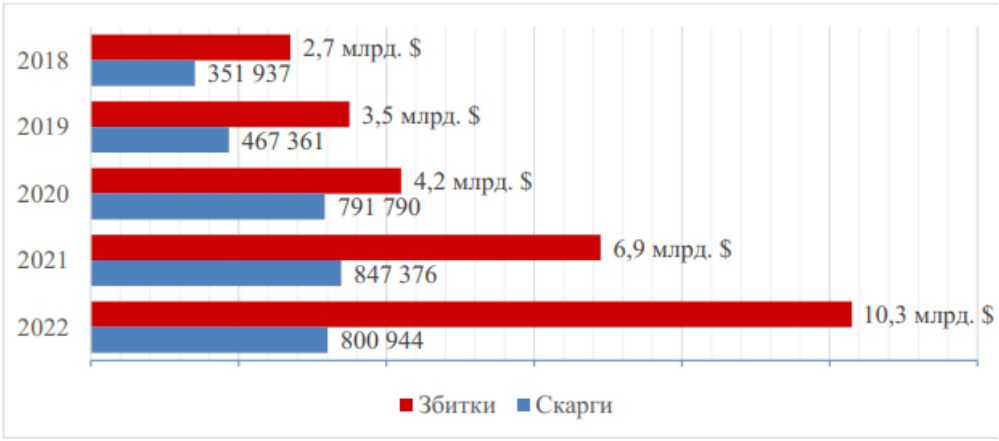
<table>
<tr><td></td><td>


Рисунок 1.1 – Скарги та збитки через кіберзагрози в 2018-2022 році
Посилання – наведено на рис. 1
</td></tr>
<tr><td>Таблиці</td><td>
Посилання на таблицю:
Використовуючи запропоновану вище процедуру отримано результуючу модель на базі НДР, описану в табл. 3.1. Побудоване НДР має значно більшу
Пустий рядок від таблиці зверху та знизу, таблиця – посередині, назва таблиці з абзацного відступу без пустого рядка за шириною аркуша:
Таблиця 3.1 – Результуюча модель на базі НДР
<table>
<tr><th>Код ознаки</th><th>Кількість нечітких множин</th><th>Використання у побудованій моделі</th><th>Код ознаки</th><th>Кількість нечітких множин</th><th>Використання у побудованій моделі</th></tr>
<tr><td>A</td><td>3</td><td>+</td><td>L</td><td>4</td><td>+</td></tr>
<tr><td>B</td><td>2</td><td>+</td><td>M</td><td>6</td><td>-</td></tr>
</table>
</td></tr>
<tr><td>Форму-ли</td><td>
Іншим прикладом є метод, що базується на показнику Херста [20, 21]
$$H = \frac{\ln\left(\frac{R}{S}\right)}{\ln(\alpha N)}, \qquad (1.3)$$
де: S – середньоквадратичне відхилення часового ряду;
R – розмах накопиченого відхилення часового ряду;
N – розмір часового ряду;
α – заданий параметр, який більший від нуля.
</td></tr>
</table>

Закінчення дод. Ж

Посилання	В роботах [24, 25] досліджено модель ідентифікації шкідливого програмного забезпечення на основі контекстно-вільних граматик. Представлена В роботах [39-42] описані різні модифікації глибоких нейронних мереж для виявлення саме ШПЗ. Разом із тим, такі моделі мають велику кількість хибних
Список літератури	Оформлюється або за алфавітом (спочатку на кириличі, потім – на латиниці), або за згадованістю по тексту (Бібліографічний опис списку використаних джерел оформлено згідно з IEEE Style, що входить до Додатку 3, Наказу МОН «Про затвердження вимог до оформлення дисертації» від 12 січня 2017 року № 40) *Електронне посилання:* 1. Australian Cyber Security Centre, *Annual Cyber Threat Report, July 2021 to June 2022* [Online]. Available: https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022 [accessed Jul. 31, 2023]. *Журнал:* 19. В. В. Челак, С. Г. Семенов, та С. Ю. Гавриленко, "Розробка шаблонів ідентифікації стану комп'ютерних систем на основі BDS-тестування", *Вісник НТУ "ХПІ". Інформатика та моделювання*, № 21, с. 118-125, Харків, 2016. *Книга:* 33. G. J. McLachlan, *Discriminant Analysis and Statistical Pattern Recognition*. Wiley Interscience, 2004, 552 с.
Зміст	Формується електронними засобами

ЗМІСТ

Навчальне видання

Методичні вказівки
до проведення виробничої практики
для студентів денної та заочної форм навчання першого (бакалаврського) рівня вищої освіти за спеціальностями 125 (F5) “Кібербезпека та захист інформації”, 256 (К3) “Національна безпека (за окремими сферами забезпечення і видами діяльності)” та 257 (К4) “Управління інформаційною безпекою”

Укладачі:
КОРОЛЬОВ Роман Володимирович
ТКАЧОВ Андрій Михайлович
ГАВРИЛОВА Алла Андріївна

Відповідальний за випуск проф. Євсеєв С. П.
Роботу рекомендував до друку проф. Євсеєв С. П.

В авторській редакції

План 2025 р., поз. 786

Підп. до друку .Гарнітура Times New Roman.
Видавничий центр НТУ “ХПІ”.
вул. Кирпичова, 2, м. Харків, 61002
Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.
Електронне видання