Міністерство освіти і науки України

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ «КІБЕРПОРТ»
Кафедра інформаційних технологій, кібернетики та захисту інформації

ВСТУП ДО ФАХУ ТА АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ

Методичні вказівки до проведення навчальної (комп'ютерної) практики

для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання спеціальності 125 Кібербезпека та захист інформації

ХАРКІВ
2024

Міністерство освіти і науки України
ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут «Кіберпорт»

Кафедра інформаційних технологій, кібернетики та захисту інформації

ВСТУП ДО ФАХУ ТА АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ

Методичні вказівки
до проведення навчальної (комп'ютерної) практики

для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання спеціальності 125 Кібербезпека та захист інформації

Затверджено рішенням
Науково-методичної комісії
ННІ Кіберпорт
Протокол №8 від 21 травня 2024 р.

Харків
2024

УДК 004:37
Н2

Схвалено на засіданні кафедри інформаційних технологій, кібернетики та захисту інформації
Протокол № 10 від 15 травня 2024 р.

Рецензенти:
С. О. Тимчук, д-р техн. наук, проф. кафедри інформаційних технологій СумДУ;
С. М. Коваленко, канд. техн. наук, доц. кафедри програмної інженерії та інтелектуальних технологій управління НТУ "ХПІ".

Н2 Вступ до фаху та академічна доброчесність:
методичні вказівки до проведення навчальної (комп'ютерної) практики для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання спеціальності 125 Кібербезпека та захист інформації / Держ. біотехнологічний ун-т; авт.-уклад.: І. В. Чалий, Т. А. Бутенко, Ю.В. Синявіна, Ю. Є. Мегель (ХНУРЕ), А. В. Левкін, О. Д. Міхнова – Харків : [б.-в.], 2024 – 56 с.

Методичні вказівки розроблені згідно з робочою програмою дисципліни «Навчальна (комп'ютерна) практика». Вони містять структуру викладання навчальної дисципліни для денної та заочної форм навчання здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації. Основна складова методичних вказівок включає поглиблення основних положень дисциплін «Вступ до фаху та академічна доброчесність» і «Теоретичні основи захисту інформації».

УДК 004:37
Відповідальний за випуск: І.В. Чалий, канд. техн. наук доцент

ЗМІСТ

Вступ

Підготовка кваліфікованих фахівців з захисту інформації є складним і багатогранним процесом, який передбачає формування у них необхідних знань, умінь і навичок. Однією з найважливіших проблем у цьому процесі є визначення того, які саме знання та навички повинні бути у майбутнього фахівця, щоб він міг успішно виконувати свої професійні обов'язки.

Модель майбутнього фахівця з захисту інформації повинна визначатися тими завданнями, які він повинен вирішувати під час своєї професійної діяльності. Ці завдання можна поділити на теоретичні та практичні.

Теоретичні завдання включають розуміння основ комп'ютерних технологій, теорії захисту інформації та правових аспектів захисту інформації. Практичні завдання включають вміння застосовувати теоретичні знання на практиці, а також вміння використовувати сучасні засоби і технології захисту інформації.

У сучасних умовах, коли високі комп'ютерні технології міцно увійшли в усі сфери людської діяльності, особливо важливим є формування у майбутніх фахівців з захисту інформації саме практичних навичок.

Практика здобувачів вищої освіти є невід'ємною складовою їх підготовки до професійної діяльності. Вона є важливим етапом у процесі формування у них професійних компетентностей, необхідних для успішної роботи в обраній галузі.

Для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 125 Кібербезпека та захист інформації на першому курсі передбачена навчальна (комп'ютерно-ознайомча) практика. Вона проходить в ДБТУ на кафедрі інформаційних технологій, кібернетики та захисту інформації протягом 6-ти тижнів у II семестрі.

Питання навчальної (комп'ютерно-ознайомчої) практики стосовно методології її проведення, бази практики, керівництва практикою, обов’язків здобувачів вищої освіти при проходженні практики, критерії оцінювання практики, техніки безпеки та

деякі інші важливі речі в подробицях розглянуті в методичному посібнику [1].

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ.

1. Структуру та загальний зміст практики.

Частина 1 навчальної (комп'ютерно-ознайомчої) практики поглиблює знання, отримані протягом вивчення на першому курсі дисциплін: Вступ до фаху кібернетичної безпеки, Теоретичні основи захисту інформації.

Матеріали цій частини практики присвячені ознайомленню з основами кібербезпеки та захисту інформації.

Це включає вивчення таких тем, як:

- Основи кібербезпеки;
- Термінологія з інформаційних технологій та кібербезпеки;
- Загальні поняття кіберзагроз, інцидентів, атак;
- Ресурси для самостійного навчання основам кібербезпеки;
- Правові аспекти кібербезпеки;
- Основні рішення та матеріали корпорації Microsoft стосовно безпеки й конфіденційності;
- Дослідження деяких важливих Інтернет-ресурсів офіційних організацій з захисту інформації;
- Дослідження деяких важливих Інтернет-ресурсів основних гравців на ринку захисту інформації;
- ...

Студенти готують звіт про проходження цієї складової практики, який наприкінці практики разом зі звітами по іншим частинам практики [1] оформлюються як єдиний остаточний документ.

Частина 1 є вступною частино всієї навчальної практики і є важливою складовою підготовки майбутніх фахівців з кібербезпеки та захисту інформації. Вона дозволяє їм:

- Закріпити теоретичні знання, отримані в процесі навчання за дисциплінами: Вступ до фаху кібернетичної безпеки, Теоретичні основи захисту інформації, та набути практичних навичок, необхідних для успішної роботи в галузі.

• Розвинути критичне мислення та вміння застосовувати отримані знання та навички в реальному середовищі.

• Отримати досвід роботи в команді та самостійно.

• Практика здобувачів вищої освіти в ДБТУ може допомогти їм знайти роботу після закінчення університету, оскільки дає їм можливість познайомитися з потенційними роботодавцями та отримати рекомендації від них.

Деякі конкретні завдання, які можуть бути поставлені перед практикуючими, включають:

• Опрацювання лекцій та семінарів з основних тем кібербезпеки.

• Організація практичних занять, на яких студенти зможуть ознайомитися з сучасними інформаційними технологіями та засобами кіберзахисту.

• Залучення студентів до виконання моделей реальних завдань у галузі кібербезпеки.

Перед початком практики здобувачі вищої освіти проходять інструктаж з техніки безпеки та охорони праці, пожежної безпеки, ознайомлюються з правилами внутрішнього розпорядку підприємства, порядком отримання документації та матеріалів.

Результатом інструктажу є підпис кожного студента у відповідному «Журналі реєстрації інструктажів з питань безпеки життєдіяльності для здобувачів вищої освіти» [1].

Під час дії особливого періоду і студентам і викладачам потрібно дотримуватися всіх правил поведінки та безпеки, встановлених або рекомендованих Міністерством освіти і науки України, а також внутрішніми розпорядженнями та наказами керівництва Державного біотехнологічного університету [2].

Після закінчення терміну практики здобувачі вищої освіти звітують про виконання індивідуального завдання.

Для частини 1 це може бути:

– матеріали з охорони праці та безпеки життєдіяльності під час роботи у комп'ютерному класі (з урахуванням роботи під час дії особливого періоду);

– термінологія з інформаційних технологій та кібербезпеки;

– особистий список сайтів та програмного забезпечення що може в подальшому стати у нагоді при навчанні та роботі за фахом;

– знання з практики корпоративної безпеки;

– знання асоціації фахівців з безпеки інформації;

– профіль у LinkedIn як вигідна професійна перевага;

– поглиблення навичок пошуку, аналізу, візуалізації та узагальнення досягнень у сфері науково-технічної, законодавчої та загальнонаукової інформації у галузі кібербезпеки;

– знання про штучний інтелект та проблеми кібербезпеки;

– короткий опис основних стандартів у галузі забезпечення кібербезпеки;

– знання про міжнародні організації, що діють у сфері інформаційної безпеки;

– курси та сертифікати з кібербезпеки;

– інші матеріали з кібербезпеки;

Письмовий звіт разом з іншими документами (щоденником, характеристикою, рецензіями, сертифікатами та ін.) подається на розгляд керівникові практики від кафедри.

Перед початком проходження навчальної практики студенти одержують від викладачів кафедри індивідуальні завдання, які вони повинні виконати в період проходження практики.

Теми індивідуальних завдань видаються з урахуванням умов проходження практики, роботи установ – баз практики на основі теоретичних знань, які вони одержали в університеті.

Індивідуальне завдання студент виконує самостійно, використовуючи різноманітні за своїм складом та можливостями Інтернет-ресурси, технічну літературу та консультації керівників практики.

2 Узагальнений календарний план навчальної практики*

Робочі дні по порядку	Тема заняття, основний зміст роботи
1	Вступне заняття «Організація практики та техніка безпеки». Розподіл здобувачів за безпосередніми керівниками. Вивчення здобувачем програми практики. Отримання індивідуальних завдань.
2-9	Виконання здобувачем індивідуального завдання, виданого керівником.
9-10	Формування та оформлення проміжного звіту по відповідному розділу практики.

***** Календарний план навчальної практики наведений для першого змістовного модулю практики.

2. ЗМІСТ НАВЧАЛЬНОЇ (КОМП'ЮТЕРНОЇ) ПРАКТИКИ

2.1 Змістовні складові [3].

Зміст навчальної (комп'ютерно-ознайомчої) практики повинен охоплювати такі напрями навчального та виховного процесу: навчально-методичну, виховну та індивідуальну роботу.

Навчально-методична робота:

– ознайомлення із теоретичними основами технологій, що використовуються в рамках індивідуального завдання;

– засвоєння сучасних методів навчання.

Виховна робота:

– набуття навичок роботи у команді;

– набуття навичок самостійного ведення роботи.

Індивідуальна робота:

– виконання практичної частини відповідно до індивідуального завдання.

2.2 Орієнтовний тематичний план.*

№ п/п	Тема програми	Розподіл часу, год.
1.	Ознайомлення з програмою практики. Знайомство з підприємством (університетом), його структурою. Інструктаж з техніки безпеки, з охорони праці та безпеки життєдіяльності під час роботи у комп'ютерному класі (з урахуванням роботи під час дії особливого періоду). Видача студентам необхідних матеріалів для проходження практики.	6
2**.	Ознайомлення з Інформаційно-обчислювальним центром університету. Забезпечення комп'ютерною технікою. Програмне забезпечення та обіг даних та інформації на базі практики. Короткий аналіз постреквізитів навчальної (комп'ютерно-ознайомчої) практики.	6
3.	Основи кібербезпеки. Термінологія з інформаційних технологій та кібербезпеки.	6
4	Видача індивідуальних завдань. Самостійна та індивідуальна робота студентів є важливою складовою їх підготовки. Початкові ресурси для самостійного навчання.	6
5	Повторення та закріплення інформації отриманої за тиждень. Самостійна робота над виконанням індивідуальних завдань. Просунуті ресурси для самостійного навчання. Вивчення можливостей порталу ITExpert.	6
6.	Основні рішення та матеріали корпорації Microsoft стосовно безпеки й конфіденційності.	6
7.	Дослідження деяких важливих Інтернет-ресурсів офіційних організацій з захисту інформації.	6

8.	Дослідження деяких важливих Інтернет-ресурсів основних гравців на ринку захисту інформаціїї (частина 1).	6
9.	Дослідження деяких важливих Інтернет-ресурсів основних гравців на ринку захисту інформаціїї (частина 2).	6
10	Підведення підсумків. Узагальнення та систематизація матеріалу щодо проходження начальної практики. Оформлення проміжного звіту з практики. Остаточне заповнення щоденника практики по першим двом тижням навчання. Отримання проміжного відгуку керівника практики від підприємства.** Отримання проміжного відгуку керівника практики від університету. Оголошення та посилання стосовно проходження практики в наступні два тижня.	6
11	**Додаткова можлива тематика для досліджень.** Нормативно-правове регулювання забезпечення інформаційної безпеки. Висновки щодо рівня інформаційної безпеки бази практики. Обстеження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом. Аналіз структури підприємства. Ознайомлення з основними етапами організації системи забезпечення інформаційної безпеки, функціонального призначення окремих підрозділів, об'єктів, що захищаються, виявлення загроз, їхній аналіз та побудова окремої моделі загроз. Розробка рекомендацій щодо реалізації організаційних заходів захисту інформації на підприємстві. Технічний захист інформації. Розробка рекомендацій щодо реалізації первинних технічних заходів захисту інформації на підприємстві. Програмний захист інформації.	
	Разом:	60

*Орієнтовний тематичний план наведений для 1 розділу практики (всього розділів (модулів) 3) який продовжується 2 тижні.

** Пункти 2 (початок) та 10 безпосередньо залежить від місця бази практики та його оснащення для виконання завдань практики.

Тематичний план дійсно є орієнтовним і може бути за потреби скорегований в залежності від ряду обставин. Перш за все на нього напряму впливають умови вивчення дисциплін Вступ до фаху кібернетичної безпеки та Теоретичні основи захисту інформації.

3. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ТЕМ ПРОГРАМИ ПРАКТИКИ.

3.1 Заняття 1.

Ознайомлення з програмою практики. Знайомство з підприємством (університетом), його структурою. Інструктаж з техніки безпеки, з охорони праці та безпеки життєдіяльності під час роботи у комп'ютерному класі (з урахуванням роботи під час дії особливого періоду). Видача студентам необхідних матеріалів для проходження практики.

Передбачається після ознайомлення з безпосереднім керівництвом практикою, самою програмою практики, складання та доведення до студентів орієнтовного графіку проходження практики (додаток 5) [1].

Студентам надаються матеріали цих методичних рекомендацій, інші необхідні матеріали для проходження практики (щоденник, форма звіту про виконану роботу, посилання на час та засоби спілкування з викладачами тощо).

Інструктаж з техніки безпеки, з охорони праці та безпеки життєдіяльності під час роботи у комп'ютерному класі (з урахуванням роботи під час дії особливого періоду) проводиться безпосередньо на робочих місцях практики за допомогою матеріалів джерел [1 -6].

В умовах дії особливого періоду, коли практика може проводитися в онлайн-режимі доцільно запропонувати студентам в якості індивідуальної роботи пройти один чи декілька курсів платформи "Зрозуміло", присвячених безпеці життєдіяльності з наступних:

1. Дивись під ноги! Дивись, куди ідеш! [https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-033+dec2022/about].
2. Інформаційні операції під час війни: як розпізнати та вберегтися? [https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-037+June23/about].
3. Основи цивільного захисту для добровольців. [https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-026+aug2022/about].
4. У безпеці. [https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-032+nov2022/about].
5. Цивільна безпека та підготовка до надзвичайних ситуацій. [https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-028+sept2022/about].

Обов'язково надіслати студентам вся необхідні матеріали.

3.2 Заняття 2

Ознайомлення з Інформаційно-обчислювальним центром університету. Забезпечення комп'ютерною технікою. Програмне забезпечення та обіг даних та інформації на базі практики.

Ознайомлення з Інформаційно-обчислювальним центром університету. Забезпечення університету комп'ютерною технікою. Периферійне обладнання та комп'ютерні мережі університету. Програмне забезпечення та обіг даних та інформації на бази практики.

Забезпечення комп’ютерною технікою.

- Практиканти визначають рівень комп’ютерного забезпечення бази практики:
  - кількість серверів, персональних комп’ютерів, ноутбуків, інших обчислювальних пристроїв;

- особливості їх архітектури, апаратну конфігурацію, інтерфейси та ін.

• Аналізують периферійне (пристрої вводу-виводу, їх функціональні характеристики) та мережеве обладнання (маршрутизатори, комутатори, wifi-роутери, модеми, тощо).

• Описують характеристики зазначеного обладнання.

• Замальовують схему локальної обчислювальної мережі підприємства (навчальних класів та лабораторії кафедри інформаційних технологій, кібернетики та захисту інформації, Науково-навчального інституту Кіберпорт, Державного біотехнологічного університету).

Програмне забезпечення комп'ютерної техніки.

• Досліджують програмне забезпечення, яке встановлене на комп'ютерній техніці бази практики:

- операційні системи;
- прикладне програмне забезпечення;
- спеціалізоване програмне забезпечення;
- службове ПЗ;
- антивіруси;
- інше програмне забезпечення, яке використовується для захисту інформації.

• Аналізують його конфігурацію.

Обіг даних та інформації.

• Практиканти визначають, яка конфіденційна інформація збирається, обробляється, зберігається та передається на базі практики (в університеті).

• Визначають, яким чином забезпечується її обіг в університеті.

Аналіз основних напрямків забезпечення інформаційної безпеки на підприємстві (якщо база практики зовнішня).

• Практиканти аналізують основні напрямки забезпечення інформаційної безпеки в університеті.

• Визначають загрози щодо конфіденційної інформації бази практики.

- Досліджують організаційний та інженерно-технічний захист інформації на інформаційно-обчилювальному центрі (кафедрі).
- Визначають, яким чином відбувається організація і забезпечення робіт щодо захисту інформації.

Висновки щодо рівня інформаційної безпеки бази практики.

- Практиканти роблять висновки щодо рівня інформаційної безпеки бази практики.
- Вносять пропозиції щодо підвищення рівня інформаційної безпеки бази практики.

Вивчають електронний документообіг та електронну комерцію в університеті.

Доцільно зробити відповідну екскурсію з вивчення IT-структури бази практики. Її могли б провести провідні фахівці Інформаційно-обчислювального центру університету.

Короткий аналіз постреквізитів навчальної (комп'ютерно-ознайомчої) практики.

Доцільно ознайомити практикантів з силабусами провідних фахових дисципліни, які в подальшому будуть вивчатися за спеціальністю 125 - Кібербезпека та захист інформації.

Це особливо важливо коли студенти будуть складати особистий список сайтів та програмного забезпечення, що може в подальшому стати у нагоді при навчанні та роботі за фахом.

Список та зміст силабусів провідних фахових дисципліни надаються практикантам окремим файлом.

3.3 Заняття 3.

Основи кібербезпеки. Термінологія з інформаційних технологій та кібербезпеки.

Викладачі використовуючи різні матеріали нагадують основи кібербезпеки та термінологію з інформаційних технологій та кібербезпеки.

Так переважна більшість питань з основ кібербезпеки розглянуті в матеріалах дисциплін Вступ до фаху кібернетичної безпеки та Теоретичні основи захисту інформації.

При викладанні даної тематики важливо використати різноманітні матеріали; лекції, практичні роботи, презентації, численні відеоматеріали. Бажано чергувати вже знайомі студентам відомості та нові матеріали. Після цього переходимо до питань термінології.

Питань, пов'язаних з інформаційною безпекою взагалі та, особливо, безпосередньо з кібербезпекою дуже багато, а масштаби різних кіберзагроз прийняли останнім часом такий розмах, що орієнтуватися в них повинна кожна сучасна людина.

Згідно з новими програмами навчальних дисциплін значно скорочено аудиторне (перш за все лекційне) навантаження студентів [7]. З іншого боку коло питань, пов'язаних з сучасними інформаційними технологіями, якими повинен володіти майбутній фахівець зростає з кожним роком. Вихід полягає в стимулюванні систематичної самостійної роботи студентів протягом усього навчання. Така робота має на увазі самостійну роботу з відповідною літературою, використання спеціальних мультимедійних навчаючих електронних програм – посібників, необмежених ресурсів Інтернет.

Але, як показав багаторічний досвід викладання, в цьому випадку значні труднощі перед студентом виникають в питаннях термінології. Вивчаючи будь-яку науку, ми спочатку засвоюємо мову науки (основні терміни та поняття), потім поступово переходячи від простого до більш складного, опановуємо вершини науки. Це особливо справедливо відносно сучасних інформаційних технологій, де питання термінології завжди стояли гостро. Справа навіть не в великій кількості термінів, яка постійно зростає, а в тому що в Україні довгий час наукові публікації, науково-технічна документація та викладання у навчальних закладах велись російською мовою. Оскільки більшість термінів має американське походження, а потім вони свого часу були перекладені російською мовою, адекватний їх переклад на українську мову є досить важкою проблемою. Процес становлення україномовної термінології триває і зараз.

Будь-яка галузь теорії й практики базується на строгому понятійному апараті. Безумовно, формування більш повного переліку термінів, їх визначення й інтерпретація таким чином, щоб забезпечувалося однозначне розуміння кожного з них, має першорядне значення й для розвитку теоретичного базису інформаційної безпеки. У сфері захисту інформації, як і в будь-якій іншій сфері діяльності, існує специфічна термінологія (професійна і жаргонна), що відображає концептуальні підходи до розв'язання конкретних проблем.

В практичному плані студентам треба запропонувати ознайомитися як з класичними підручниками та методичними посібниками [7 -11] так і ресурсами Інтернет:

- Комп'ютерна термінологія Вікіпедія [https://uk.wikipedia.org/wiki/Комп%27ютерна_термінологія].
- Термінологічний словник з інформатики. Вікіпідручник. [https://uk.wikibooks.org/wiki/Термінологічний_словник_з_інформатики].
- Ресурс. [https://eng-rus-comp-security-dict.slovaronline.com/].
- Мінцифри представило "словник термінів з онлайн-безпеки". Джерело: [https://censor.net/ua/p3225693].
- NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES. [https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary].
- Withdrawn NIST Technical Series Publication. Glossary of Key Information Security Terms [https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf].
- Бесплатные программы для удалённого устного перевода. [https://globerland.com/blog/besplatnye-programmy-dlya-udalyonnogo-ustnogo-perevoda].

Студентом доцільно запропонувати знайти і інші ресурси, особливо стосовно сленгу кібербезпеки.

3.4 Заняття 4.

Видача індивідуальних завдань. Самостійна та індивідуальна робота студентів є важливою складовою їх підготовки. Початкові ресурси для самостійного навчання.

Самостійна та індивідуальна робота студентів є важливою складовою їх підготовки з будь-якої дисципліни. Вона дозволяє студентам закріпити отримані знання, розвинути навички самостійного навчання та критичного мислення, а також підготуватися до самостійної професійної діяльності.

Існує багато засобів та підходів до організації самостійної та індивідуальної роботи студентів. Класичними є такі форми самостійної роботи, як написання есе, рефератів, презентацій тощо.

При підготовці студентів з дисциплін «Кібербезпека», «Вступ до фаху кібернетичної безпеки» та «Основи кібербезпеки» можливо застосувати додатково підхід, пов'язаний з використанням онлайн-ресурсів Інтернет. Цей підхід дозволяє студентам:

- Ознайомитися з актуальними знаннями та інформацією з кібербезпеки, які не завжди сучасно представлені в підручниках та навчальних посібниках.
- Розвивати навички самостійного пошуку та обробки інформації.
- Підготуватися до самостійної професійної діяльності в умовах інформаційного суспільства.

Застосування онлайн-ресурсів Інтернет.

Для використання онлайн-ресурсів Інтернет у процесі самостійної та індивідуальної роботи студентів необхідно:

- Розробити план самостійної роботи, який включатиме перелік онлайн-ресурсів, які будуть використовуватися.
- Надати студентам рекомендації щодо використання онлайн-ресурсів.
- Провести інструктаж щодо пошуку та обробки інформації в Інтернеті.

Ось кілька прикладів онлайн-ресурсів, які можна використовувати для самостійного вивчення дисциплін з кібербезпеки:

- Офіційні сайти міжнародних організацій, що займаються питаннями кібербезпеки, таких як НАТО, ООН, Європейський Союз.
- Сайти державних органів України, які відповідають за кібербезпеку.
- Сайти наукових установ, які проводять дослідження в галузі кібербезпеки.
- Сайти компаній, що займаються розробкою та впровадженням засобів кібербезпеки.

Вибір онлайн-ресурсів для самостійного вивчення дисциплін з кібербезпеки повинен відповідати конкретним цілям та завданням навчання.

Важливо задати правильну траєкторію проходження таких ресурсів. Бажано здійснити поступовий перехід від більш простих до більш складних.

Далі будуть пропонуватися тільки безкоштовні курси.

В цьому плані для спеціальності 125 - Кібербезпека та захист інформації на початку пропонується використати ресурси найбільш відомої національної онлайн-платформи для розвитку цифрової грамотності «Дія. Освіта» [14, 15].

В межах спеціальності 125 - кібербезпека та захист інформації увага студентів для самостійного опрацювання зверталася перш за все на такі освітні серіали як:

1. Кіберняні.
2. Електронний підпис.
3. Основи кібергігієни.
4. Нові цифрові професії.
5. Обережно! Кібершахраї.
6. Персональна кібергігієна.
7. Персональні дані.

Серіал Персональна кібергігієна чудово доповнює однойменний симулятор, який дає змогу студентам протестувати свої знання, зрозуміти, що упущено при навчанні, на що варто звернути увагу та доопрацювати.

Найкращий спосіб оцінити свою цифрову грамотність після проходження серіалів, це пройти Кіберграм. Завдання в ньому

створені за європейськими стандартами DigComp 2.1. та адаптовані українськими експертами. Після проходження серіалів та тестів кожен учасник отримує відповідні сертифікати.

Наступний Prometheus [https://prometheus.org.ua/] — ресурс з доступом до безкоштовних україномовних онлайн-курсів на різні теми від інформаційної гігієни до управління фінансами. Команда Prometheus продовжує активно працювати над новими програмами і під час війни.

Цікаві такі освітні серіали як:

1. Безпека в Інтернеті під час війни: практичний курс.
2. Цифрова безпека на персональному рівні.
3. Інформаційна гігієна. Як розпізнати брехню в соцмережах, в Інтернеті та на телебаченні.
4. Інформаційна гігієна під час війни.
5. Інформаційні війни.
6. Інформаційна безпека.
7. Основи інформаційної безпеки.

Звертаємо увагу на курс "Основи інформаційної безпеки" [https://prometheus.org.ua/course/course-v1:KPI+IS101+2014_T1]

Мета курсу – навчити користувачів основам поводження з персональною інформацією в умовах, коли фізичний та віртуальний світи все більше зближуються.

Тривалість курсу 6 тижнів ідеально підходе під формат практики. Відеолекції, завдання, форум та можливість отримати сертифікат доступні в будь-який час.

Курс " Основи інформаційної безпеки " є важливим для всіх, хто використовує Інтернет. Він допоможе вам усвідомити кіберзагрози та навчитися захищати себе від них.

- Ви дізнаєтеся, що таке фішинг, розвідка, кібератаки на критичну інфраструктуру тощо.
- Ви зрозумієте, що кіберзлочинці можуть бути як одинаками, так і цілими групами, які діють за замовленням.
- Ви дізнаєтеся, що найчастіше жертвами кібератак стають звичайні люди, а не великі компанії.
- Ви отримаєте поради, як захистити свою особисту інформацію, наприклад, використовувати складні паролі,

двофакторну аутентифікацію та безпечне програмне забезпечення.

- Ви дізнаєтеся, як захистити свій мобільний пристрій від вірусів, шкідливих програм та інших загроз.
- Тощо.

Наступний рівень це Мережна академія Cisco [https://www.netacad.com/ru] —унікальна програма, що поєднує міць технологій і сучасних методик навчання. Це глобальна програма, яка допомагає людям розвивати кар'єру в галузі IT. Вона пропонує широкий спектр курсів, які покривають різні аспекти мережевої інженерії. Розкриваються тут і питання кібербезпеки. Приєднатися до Мережної академії Cisco може будь-яка людина з будь-якої країни. Для цього необхідно лише пройти реєстрацію на веб-сайті академії.

На час створення цих методичних вказівок пропонувалося 5 курсів з питань кібербезпеки. Але зараз звернемо увагу на два безкоштовних курси, які перекладені українською мовою:

1. Introduction to Cybersecurity
2. Cybersecurity Essentials

Преамбула до курсу Introduction to Cybersecurity [https://www.netacad.com/ru/courses/cybersecurity/introduction-cybersecurity].

У сучасному взаємозалежному світі кожен відкритий для кібератак. Незалежно від того, хочете ви зробити професійну кар'єру у сфері кібербезпеки або просто зацікавлені у безпечному використанні Інтернету та соціальних мереж, цей вступний курс буде вам корисним. У ньому ми досліджуємо кібертенденції та кіберзагрози, торкаючись актуальних аспектів ширшої теми кібербезпеки. Наприклад, ви дізнаєтесь, як захистити персональні дані в Інтернеті, і отримаєте уявлення про проблеми, з якими сьогодні стикаються компанії, урядові та освітні установи. Без попередніх вимог.

Ви отримаєте такі ключові навички та знання:

❖ Дізнайтеся, що таке кібербезпека і як вона зачіпає вас.

❖ Отримайте уявлення про найбільш поширені загрози, атаки та вразливості.

❖ Дізнайтеся про способи, якими компанії захищаються від атак.

❖ Ознайомтеся з останніми тенденціями ринку праці і дізнайтеся, чому сегмент кібербезпеки продовжує зростати.

Тривалість курсу 15 годин.

Преамбула до курсу Cybersecurity Essentials [https://www.netacad.com/ru/courses/cybersecurity/cybersecurity-essentials].

Основні принципи боротьби з кіберзлочинністю.

Один витік даних може мати величезні наслідки для роботи та фінансового стану організації, що сильно вплине на повсякденне життя мільйонів людей. Саме тому попит на фахівців із безпеки продовжує зростати. Скористайтеся цим і поглибить свої знання в галузі кібербезпеки, а також про технології та процедури, що використовуються для захисту мереж. Визначте, чи цікава вам робота мережного фахівця або фахівця в галузі мережевої безпеки початкового рівня. Рекомендується для студентів, які планують підготовку до сертифікації CCNA чи CyberOps Associate. Попередні вимоги: рекомендується пройти Introduction to Cybersecurity або мати аналогічну кваліфікацію.

Ви отримаєте такі ключові навички та знання:

❖ Вивчення засобів управління безпекою мереж, серверів та додатків.

❖ Вивчення ключових принципів забезпечення безпеки та методів складання відповідних політик.

❖ Впровадження належних процедур для забезпечення конфіденційності та доступності даних.

❖ Розвиток критичного мислення та навичок вирішення проблем при використанні фізичного обладнання та Cisco Packet Tracer.

Тривалість курсу 30 годин.

Цей курс ідеально підходе для тої частини практики, яка поглиблює знання з дисципліни Комп'ютерні системи та мережі, їх безпека.

Також згадаємо курси від ресурсу EdEra [https://ed-era.com/]: «Very Verified: онлайн-курс з медіаграмотності», Захист персональних даних, Захист персональних даних (поглиблений),

Курси від Відкритого університету (ВУМ) [https://vum.org.ua/complex/ : Цифрова безпека та комунікація в онлайні, Інформаційна безпека у цифровому світі, Верифікація в Інтернеті].

3.5 Заняття 5.

Повторення та закріплення інформації отриманої за тиждень. Самостійна робота над виконанням індивідуальних завдань. Просунуті ресурси для самостійного навчання. Вивчення можливостей порталу ITExpert.

ITExpert це IT-рекрутингова агенція, яка вже більше восьми років на ринку. Вони займаються пошуком IT-спеціалістів в Україні та в усьому світі: від США до Ізраїля. Працюють з продуктами та аутсорсами, підбирають core team для стартапів та шукають таланти для R&D-центрів. Шукають розробників, QA, DevOps, CTO для FinTech, E-commerce, Web3, SaaS та PaaS-продуктів, Machine Learning і AI та інших сфер. Обіцяють, що технічний спеціаліст у їх команді глибоко проаналізує ваші вимоги та налаштує точний пошук. Так ви отримаєте лише релевантні CV.

Задача практикантів спочатку комплексно дослідити цей портал так як він може стати у нагоді для вирішення багатьох завдань як під час навчання у ВНЗ так і при подальшій роботі за фахом (наприклад працевлаштування). Звернути увагу на розділи блог та новини. Занести те, що зацікавило до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

Далі основна складова заняття. Переходимо по посиланню [https://itexpert.work/uk/bezkoshtovni-onlajn-kursy-ta-resursy-dlya-it-speczialistiv/] і отримуємо (див. рис. 1).

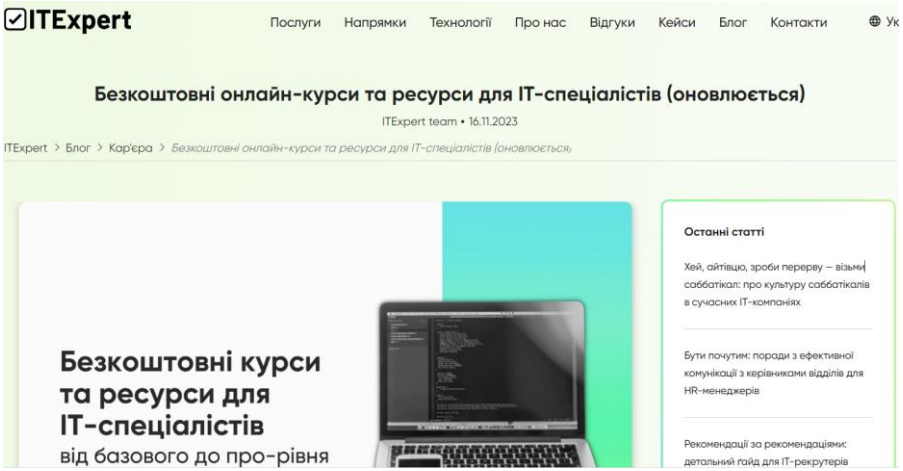


Рис. 1 Безкоштовні онлайн-курси та ресурси для IT-спеціалістів

Найбільш цікавий для нас розділ «Платформи з IT-курсами».

- Genius — до деяких дат платформа пропонує безкоштовний доступ українцям до всіх своїх курсів. Можна зареєструватись на курс Fullstack-розробника, Frontend-розробника, тестувальника ПЗ, JavaScript-розробника, HTML/CSS-фахівця, UI/UX дизайнера тощо.
- IT-Generation — грантове навчання для українців на різних IT-курсах від Мінцифри. Воно доступне для світчерів та студентів без досвіду роботи у сфері. Доступні курси з розробки, діджитал-маркетингу, тестування тощо. Серед шкіл-партнерів: StartUp Academy, IAMPM, Choice31, Laba, DAN.IT та інші.
- EPAM University — набір курсів та менторингових програм від компанії EPAM. Кожний напрямок має свої унікальні вимоги та потребує здачі вступного іспиту (єдина загальна вимога — знання англійської на рівні B1).
- Coursera — відома платформа з безкоштовними курсами та навчальними програмами по всьому світу. За тематикою

Informational Technologies, Data Science та Computer Science можна знайти понад 170 курсів англійською мовою.

- Prometheus — ресурс з онлайн-курсами українською. Можна знайти безкоштовні курси в тематиці основ програмування, Java, R, Python та JavaScript (для веб), Machine Learning, візуалізації даних, командного управління тощо.
- ITVDN — різні відеокурси з програмування у вільному доступі. Наявні курси з C#, TypeScript, Python, Django, Java, UI/UX-дизайну, тестування тощо.
- Projector Humanitarium — українська онлайн-школа креативних професій. Команда відкрила доступ на 12 курсів, серед яких: Історія геймдеву, Як працює композиція, Як працює колір тощо. Щоб відкрити доступ, потрібно зареєструватися та ввести промокод 0688-5072 (він буде діяти до нашої перемоги та місяць опісля).
- Фонд Projector Institute — фонд для навчання 5000 українських жінок, які через війну були змушені переселитися за кордон або у безпечніше місце всередині країни, новим професіям у креативних та IT-індустріях. Плануються курси з Project Management, Graphic Design, Motion Design, SEO Specialist, Interface Designer, PPC Specialist, Data Scientist, Data Analyst тощо.
- Skillsetter — серія курсів з теми Project та Product менеджменту: позиціонування продукту, управління командою та проєктами, взаємодія з розробниками, продуктові метрики, аналіз ринку та конкурентів, юніт-економіка і як пройти відбір до IT-компанії.
- Рекрутинг від SocialTalent — безкоштовний доступ на шість місяців до бази знань європейських фахівців з рекрутингу. Підходить для бажаючих працювати на ринку Європи та США. Необхідне знання англійської.
- 1000+ IT-стипендій від Beetroot Academy — курси від продуктової IT-компанії в Україні. Зараз у 1000+ українців є можливість отримати стипендію. Всі повнолітні можуть подати заяву на навчання з Front-end, Python або C# розробці, UI/UX

дизайну, QA Manual, HR Generalist, Project Менеджменту чи бізнес-аналізу в IT.

- Навчання від Вінницької IT-академії — багатомісячна програма для українців, бажаючих опанувати такі напрямки IT, як програмування, тестування, веб-дизайн (UI/UX), проектний менеджмент. Додатково пропонується вивчення англійської для IT.
- Грантова програма від DAN.IT — безоплатне навчання для українських волонтерів. Учасники зможуть пройти курси за одним з таких напрямів: програмування, веб-дизайн, аналітика даних, маркетинг, тестування й IT-рекрутинг.
- Курси програмування від Avada Media — безкоштовні курси зі стажуванням та можливістю працевлаштування для кращих студентів. Можна розвиватися у таких напрямках: Frontend Development, Backend Development, Mobile Development, Web Development та нейронні мережі.
- TechMagic Academy — навчальна програма від IT-компанії для початку кар'єру в IT. Активні напрямки: JavaScript, QA, DevOps, Security, Lead Generation & B2B Marketing. Під час навчання на студентів чекають онлайн-лекції з домашніми завданнями, практичні проекти, менторська підтримка від топ-спеціалістів TechMagic та Job offer для найкращих випускників.

Треба по черзі уважно дослідити ці ресурси, та вибрати курси для подальшого самостійного проходження. Список занести до щоденника.

Також фахівцям з кібербезпеки треба звернути увагу на розділ «Де вивчати англійську».

На ресурсі Coursera Inc. [https://www.coursera.org] дуже зручно шукати необхідні матеріали за певною тематикою.

На запит "information security" [https://www.coursera.org/courses?query=information%20security&language=Ukrainian] з доступом до курсів на українській мові було отримано 454 посилання на різні ресурси (див. рис. 2).

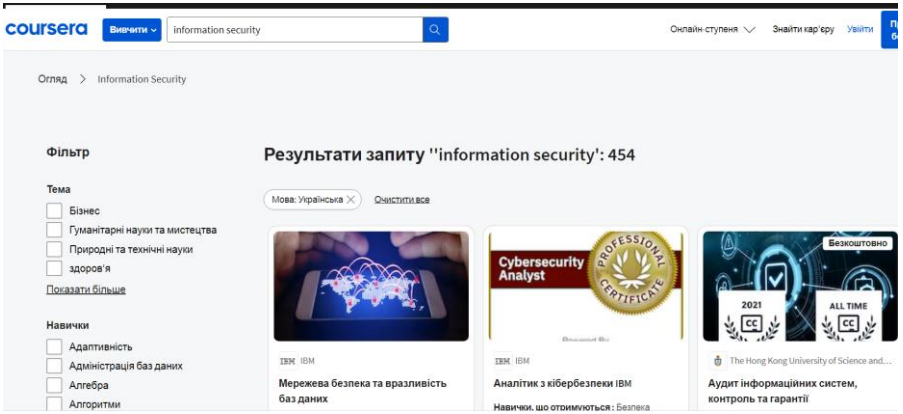
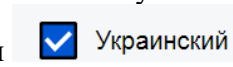


Рис. 2 Результати на запит "information security" на Coursera Inc.

Перед безпосереднім проходженням курсів бажано перейти за посиланням ознайомитися з Довідковим центром для учнів [https://www.coursera.support/s/article/208280146-Pay-for-a-course-or-Specialization?language=en_US] та зрозуміти умови на яких надається доступ до того чи іншого курсу.

В Coursera Inc. є розвинута система фільтрів для вибору необхідного для учня ресурсу. Для її застосування треба вибрати кнопку 

(зліва зверху) та встановити цілі навчання, теми, навички, рівень та багато інших налаштувань. Можливо встановити українську мову вивчення 

.

Уважно передивіться всі фільтри (на рис. 3 показано вибір необхідних навичок), виберіть те що Вас цікавить та натисніть 

На рис. 4 показано результат після застосування відповідних до нашої тематики фільтрів. Як ми бачимо отримано посилання на 156 безкоштовних он-лайн курсів. При виборі курсів можливі різні міркування. Студентам бажано співпідставити їх тематику зі списком постреквізитів навчальної (комп'ютерно-ознайомчої) практики. У міру подальшого

навчання треба звертатися до відповідних курсів для поглибленого вивчення необхідних дисциплін.

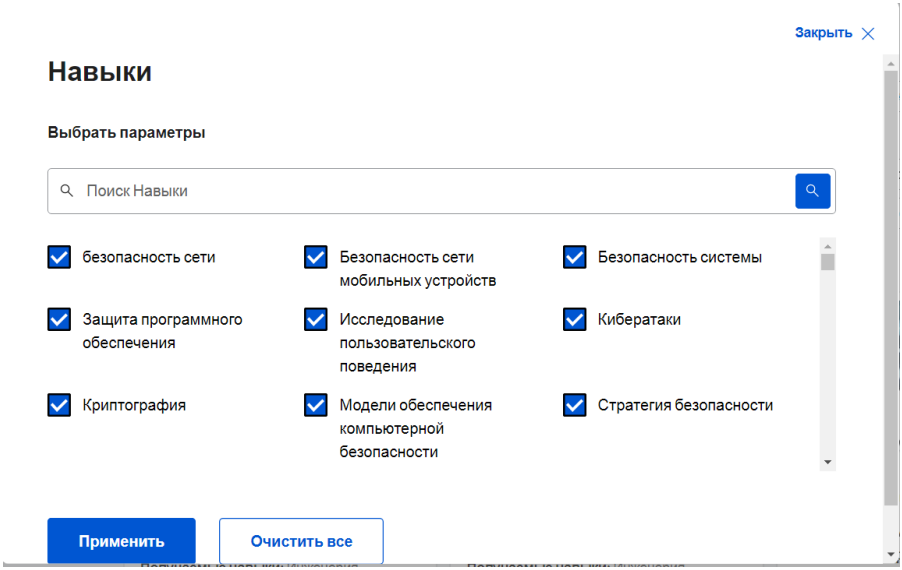


Рис. 3 Вибір необхідних навичок.

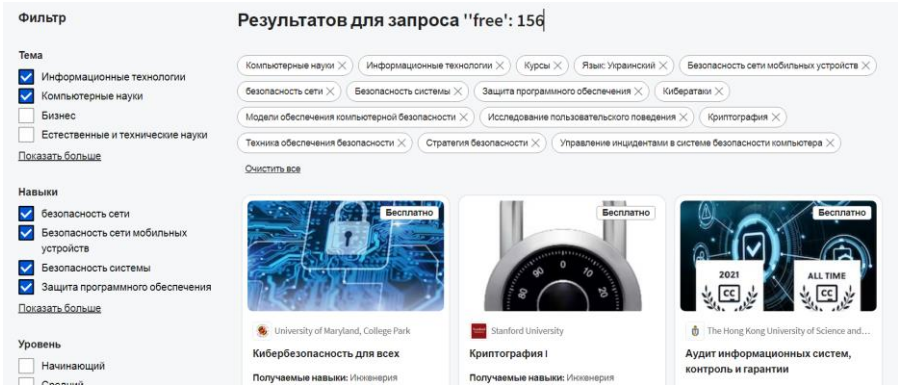


Рис. 4 Результат після застосування відповідних до тематики "кібербезпека" фільтрів.

Необхідно вибрати 1 повністю безкоштовний курс, пройти його та отримати відповідний сертифікат.

Додаткове завдання. Дослідити ресурс навчальних курсів Simplilearn Solutions [https://www.simplilearn.com/skillup-free-online-courses#Cyber-Security] та занотувати ті курси, які можливо використовувати при навчанні за фахом.

3.6. Заняття 6.

Основні рішення та матеріали корпорації Microsoft [16] стосовно безпеки й конфіденційності.

Матеріал заняття 7 дуже великого обсягу, може бути поданий по різному, з різним співвідношенням аудиторної та самостійної роботи студентів.

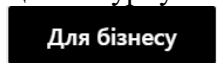
Ми почнемо знайомство з Основними рішеннями та матеріалами корпорації Microsoft стосовно безпеки з сторінки Захист і контроль інформації [https://www.microsoft.com/uk-ua/security/business/solutions/information-protection#overview].

Нові можливості захисту даних організації в хмарах, на пристроях і платформах надає Microsoft Purview - сімейство рішень з управління даними, ризиками та відповідністю вимогам, які допоможуть вашій організації керувати всією інфраструктурою даних, а також захищати та контролювати її.

По черзі треба передивитися розділи Огляд Основні продукти Ресурси. В розділі Огляд доцільно перейти за посиланням Ознайомитися з дописом у блозі та ознайомитися з публікацією "Робіть більше з меншими витратами з Microsoft Security — 3 стратегії для початку" https://www.microsoft.com/en-us/security/blog/2022/12/15/do-more-with-less-with-microsoft-security-3-strategies-to-get-you-started/. Зверніть увагу на кінець публікації де пропонується: "Щоб дізнатися більше про рішення безпеки Microsoft, відвідайте наш веб-сайт. Додайте в закладки блог безпеки , щоб бути в курсі наших експертів з питань безпеки. Також слідкуйте за нами на @MSFTSecurity, щоб отримувати останні новини та оновлення з кібербезпеки."

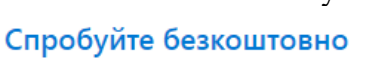
Перейдемо за посиланням Microsoft Security [https://www.microsoft.com/en-us/security/homepage-b] на сторінку під назвою "Безпека для всіх у віці ШІ" та дізнаймося про інноваційні способи впровадження новітнього штучного інтелекту з кібербезпеки у вашу організацію на цифровій події Microsoft Secure. Перегляньте всі продукти та рішення, що наведені нижче.

Перейдемо за посиланням відвідайте наш веб-сайт [https://www.microsoft.com/uk-ua/security/] на сторінку під назвою "Безпека для всіх" та дізнаймося про Захисний комплекс Microsoft, що допоможе вбезпечити користувачів і дані від кіберзагроз, щоб ви ні про що не турбувалися.. Перегляньте по черзі підрозділи 

, 

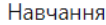
та 

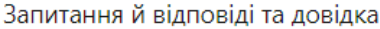
.

Звертаємо увагу студентів, що для багатьох продуктів є можливість натиснувши кнопку на кшталт 

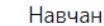
деякий час безкоштовно ознайомлюватися з їх можливостями.

Продовжити самостійне вивчення ресурсів з захисту інформації від корпорації Microsoft. Занести те, що зацікавило до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

Далі доцільно розглянути навчання за допомогою ресурсу Microsoft Learn [https://learn.microsoft.com/uk-ua/]. Уважно дослідіть головну сторінку ресурсу. Після цього переходимо до підрозділу 

[https://learn.microsoft.com/ru-ru/training/browse/?subjects=security&roles=student]. Після його перегляду переходимо до підрозділу 

. Окрім інших важливих моментів ми дізнаємося, що **навчання Microsoft Learn є безкоштовним і доступним для всіх, хто хоче дізнатися про продукти Microsoft.**

Повертаємося до підрозділу 

, встановлюємо відповідно нашим уподобанням фільтри:

,

студент при необхідності вкажіть рівень (Початківець, Проміжний або Просунутий) вибирайте ресурс і знайомтеся з його змістом. Нажаль деякі модулі недоступні українською мовою.

Початківець може почати роботу зі схеми навчання "Опис основних понять кібербезпеки" [https://learn.microsoft.com/uk-ua/training/paths/describe-basic-concepts-of-cybersecurity/] яка складається з 6 модулів, має тривати приблизно 2 години 8 хвилин.

Більш досвідчені студенти можуть досягти більш амбітні цілі: пройти серію з 9 курсів професійної сертифікації аналітика з кібербезпеки Microsoft (див. рис. 5).

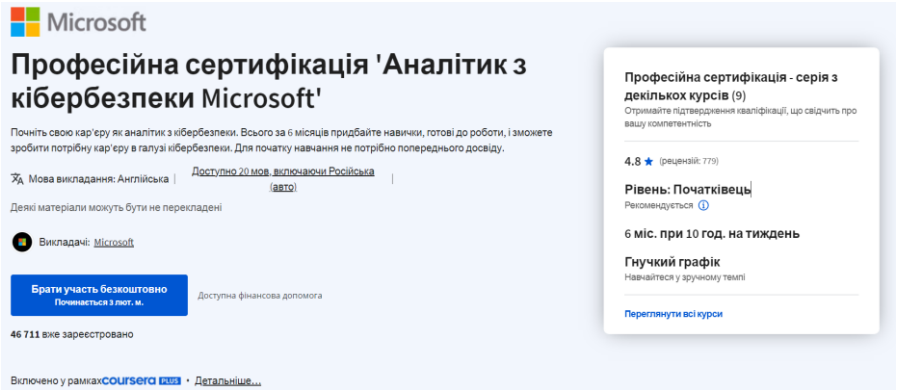


Рис. 5 Курси професійної сертифікації аналітика з кібербезпеки Microsoft (взято з [https://www.coursera.org/professional-certificates/microsoft-cybersecurity-analyst#courses]).

Повідомляється, що слухачі, які закінчать цю програму, отримають ваучер на складання сертифікаційного іспиту SC-900 зі знижкою 50%.

Занести те, що зацікавило з дослідженого вище до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

3.7 Заняття 7.

Дослідження деяких важливих Інтернет-ресурсів офіційних організацій з захисту інформації.

За браком часу обмажемося такими веб-ресурсами як сайт Державної служби спеціального зв’язку та захисту інформації України (Держспецзв'язку [https://cip.gov.ua/ua]), CERT-UA ([https://cert.gov.ua/]), який функціонує в складі Держспецзв’язку та ENISA – European Union Agency for Network and Information Security ([https://www.enisa.europa.eu/]).

Ми частково знайомі з цими ресурсами з курсу Вступ до фаху кібернетичної безпеки. Матеріали стосовно перших двох ресурсів наведені в 3 розділу лекції №9 "Функції системи суб'єктів забезпечення інформаційної безпеки України". Матеріали стосовно ENISA наведені в лекції №8 "Діяльність міжнародних організацій у сфері інформаційної безпеки" та в лабораторній роботі №10.

ДССЗЗІ України є державним органом (див. рис. 6), основною функцією якого є забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

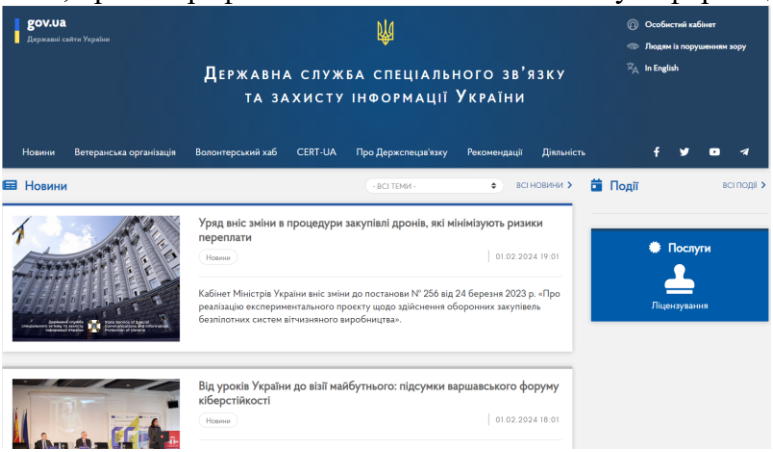


Рис. 6 Портал Державної служби спеціального зв’язку та захисту інформації України [https://cip.gov.ua/ua]

Спочатку можливо передивитися новини, оголошення та запитання. До речі, якщо перейти за посиланням ВСІ ЗАПИТАННЯ > можливо знайти багато цікавого.

Зробивши перехід Про Держспецзв'язку ▶ Послуги ▶ Ліцензування можливо передивитися матеріали стосовно ліцензованої діяльності у галузі КЗІ та ТЗІ.

Далі деякий час можливо зупинитися на матеріалах посилання ВСІ ПОДІЇ >.

Після цього студенту пропонується більш докладно зупинитися на розділі Діяльність (див. рис. 7).

У нагоді може стати інструмент - ВСІ ТЕМИ -.

Занести те, що зацікавило з дослідженого вище до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

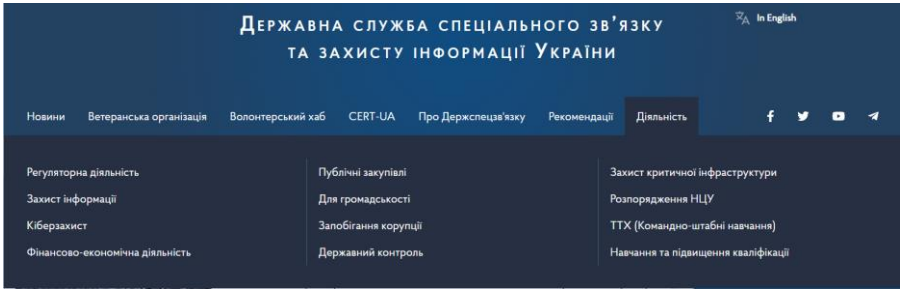


Рис. 7 Розділ Діяльність Держспецзв’язку

CERT-UA (див. рис. 8) це команда реагування на комп'ютерні надзвичайні події України — спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

Цю структуру ми поки що вивчали менш докладно. Наведемо цікавий матеріал стосовно нього (додаток 1 [17]).

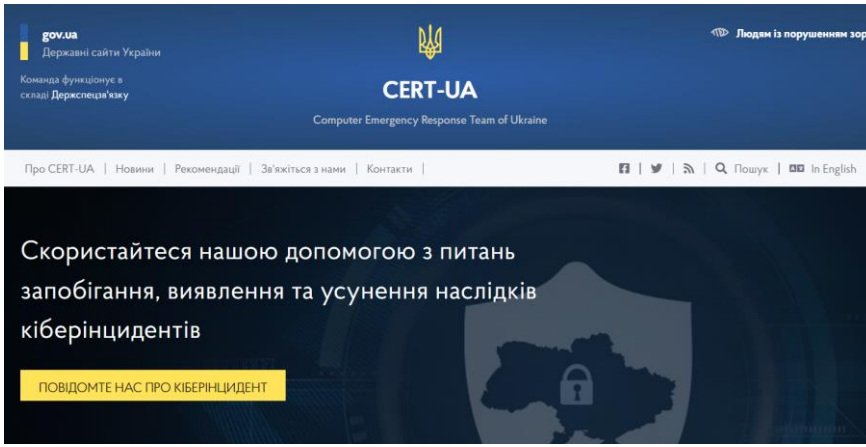


Рис. 8 Портал CERT-UA [https://cert.gov.ua/] підрозділу Держспецзв'язку.

Для більшості студентів цей ресурс стане одним з основних джерел професійної оперативної інформації. Він повинен бути завжди з вами. Тому треба уважно переглянути головну сторінку та підписатися на розсилку новин, вставивши у відповідне поле свою електронну пошту та натиснувши ПІДПИСАТИСЯ.

Крім того треба передивитися новини, оголошення та рекомендації. Зверніть увагу на розділ головної сторінки ЗВ'ЯЖІТЬСЯ З НАМИ.

Далі ознайомтеся з розділом Про CERT-UA. Зверніть увагу на завдання CERT-UA та нормативно-правову базу.

В розділі Рекомендації зверніть особливу увагу на рекомендації стосовно кіберінциндентів.

Безумовно з практичної точки зору самим важливим є розділ Новини.

Нарешті уважно передивіться для подальшого щоденного використання усі контакти CERT-UA та занесіть те, що Вас

зацікавило з дослідженого вище до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

Установу ENISA – European Union Agency for Network and Information Security ([https://www.enisa.europa.eu/] ми вже докладно вивчали на заняттях. Зусередемося на її офіційному порталі (див. рис. 9).

Рис. 9 Портал ENISA [https://www.enisa.europa.eu/].

Цей портал дає майже вичерпну інформацію стосовно практично усіх аспектів кібербезпеки Європи і не тільки. Важлива інформація, що розташована на ньому може досліджуватися багато годин і навіть днів. Враховуючи це дамо пораду студентам зосередитися після звичайного вже перегляду новин на лівій боковій панелі порталу.

Підводячи курсор до відповідних підрозділів ми отримаємо віконце, в якому дається коротка анотація цього підрозділу. Таким чином можливо підібрати необхідні матеріали для вивчення (див. рис. 10).

У випадку розгляду порталу ENISA доречно після першого ознайомлення запропонувати студентам самостійно визначитися з напрямками подальшого дослідження.

Студентам також пропонується самостійно дослідити Центр антивірусного захисту інформації [https://cazi.gov.ua/uk]

Занести те, що зацікавило з дослідженого вище до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

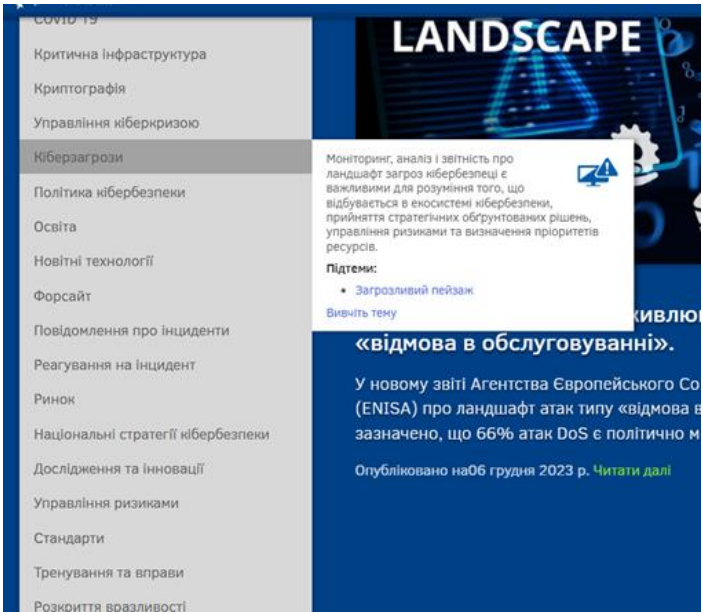


Рис. 10 Бокова панель порталу ENISA яку зручно використати для досліджень змісту.

3.8 Заняття 8.

Дослідження деяких важливих Інтернет-ресурсів основних гравців на ринку захисту інформації (частина 1).

Матеріалу, що може бути віднесений до даної тематики так багато, що все розглянуте далі носить безумовно вибірковий і суб'єктивний характер. Також слід мати на увазі, що багато з того, що може бути віднесено до даної тематики все досліджувалося студентами на попередніх заняттях цієї практики. Важливість подібних досліджень також не викликає сумніву так як сучасний фахівець повинен завжди уважно відслідковувати швидкоплинний ландшафт кібербезпекм, бути в курсі останніх технологій захисту, новітніх вразливостей, загроз тощо.

Вважаємо за доцільне розпочати дослідження з порталу IT Ukraine Association [https://itukraine.org.ua/] (див. рис. 11). Вони – найбільше об'єднання компаній-розробників програмного забезпечення в країні. Місія Асоціації – забезпечити сприятливі умови для сталого розвитку сфери інформаційних технологій в країні.

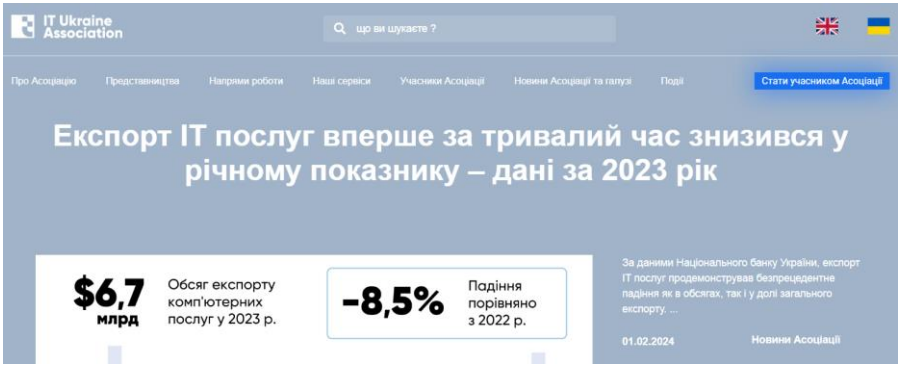


Рис. 11 Портал IT Ukraine Association.

На головній сторінці ресурсу треба звернути увагу на розділи **Наші проекти** та **Публікації**. Доречи в останньому розділі є цікавий блог, де студентам треба переглянути публікацію Як дбати про кібербезпеку в умовах війни [https://itukraine.org.ua/how-to-take-care-of-cyber-security-in-the-conditions-of-war/] (див. рис. 12).

Найбільш зацікавленим студентам пропонується вивчити матеріал додатку 2 та долучитися до IT-армії України.

Потім дослідити по-черзі інші розділи головного меню порталу починаючи з Про Асоціацію і закінчуючи **Стати учасником Асоціації**. Доречи індивідуальне членство в Асоціації не передбачається.

Треба також відмітити, що саме питанням кібербезпеки приділено на сторінках порталу невиправдано мало матеріалів.

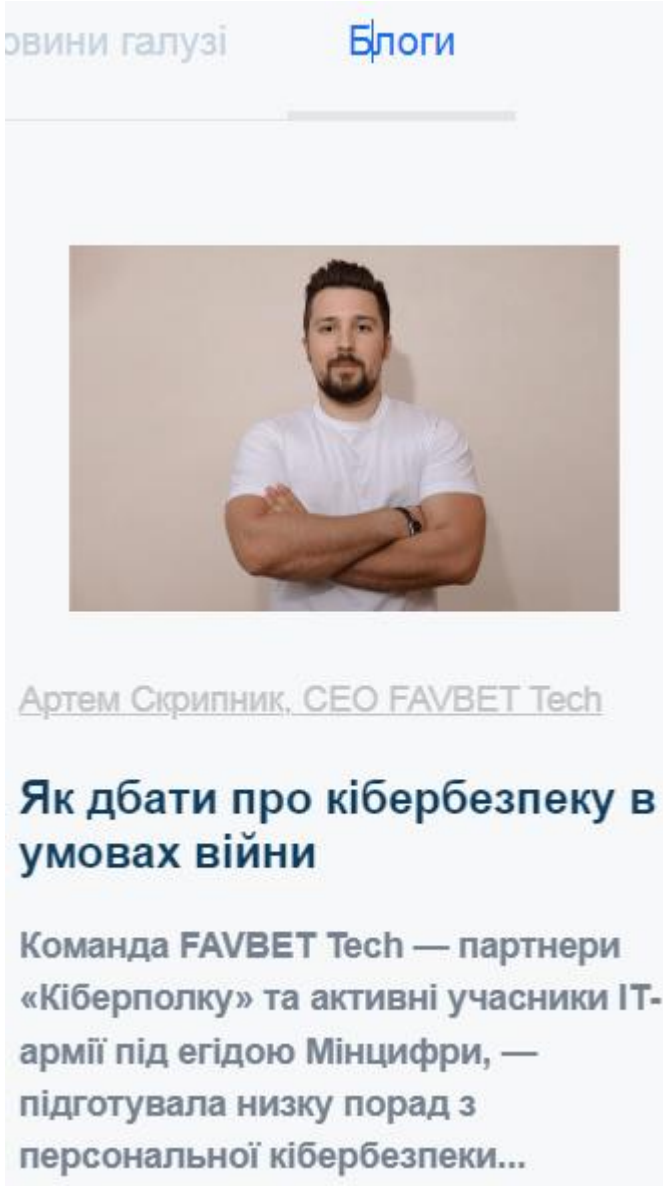


Рис. 12 Як дбати про кібербезпеку в умовах війни.

Далі розглянемо портали наших стейкхолдерів.

SOC Prime [https://socprime.com] [19] — американська компанія з українським корінням, що створила першу у світі платформу для колективного кіберзахисту (див. рис. 13). Платформа заснована на принципах Detection as Code та стандартизованого формату Sigma, що створений для опису правил виявлення кібератак та придатний для будь-якого типу лог-файлів. Десятки тисяч кіберзахисників мають доступ 24/7 до інноваційних інструментів та найбільшого репозиторію алгоритмів детектування загроз у світі. Стаючи частиною колективного кіберзахисту, спеціалісти можуть швидко та легко ідентифікувати шкідливу активність, ефективно захищаючись від кібератак.

На сьогодні понад 7000 організацій у 155 країнах світу є клієнтами SOC Prime, включаючи компанії зі списку Fortune-100, Forbes Global 2000 та державного сектору США і ЄС. SOC Prime має широку мережу партнерів, з якими успішно працює над інноваціями в галузі кібербезпеки, серед них — Microsoft Sentinel, Google Chronicle Security, Humio та інші лідери індустрії.

SOC Prime докладає усіх можливих зусиль, щоб підтримати Україну, яка перебуває на передовій кібервійни та є щитом захисту для всього світу. Наразі компанія надає консультативну допомогу та pro bono доступ до своїх технологій урядовим і комерційним організаціям України, допомагаючи захищати державу в кіберпросторі.

У своєму блозі на AIN.UA [19] SOC Prime розповідає про інноваційні технології у галузі кібербезпеки, кібервійну та побудову ефективного кіберзахисту, а також успішні кейси ведення бізнесу під час війни й економічної кризи.

Це дуже професійний і потужний ресурс тому студенти повинні знати, що на першому курсі зрозуміти всю наведену на порталі інформацію не вийде. Це перше знайомство з компанією яке буде продовжуватися протягом усіх років навчання і, сподіваємося, далі. Тому поки треба добре вивчити структуру сайту, передивитися загальні розділи та матеріали.

Рис. 13 Портал SOC Prime.

Після перегляду головної сторінки треба переглянути по-черзі з розділу **РЕСУРСИ** всі його підрозділи (див. рис. 14).

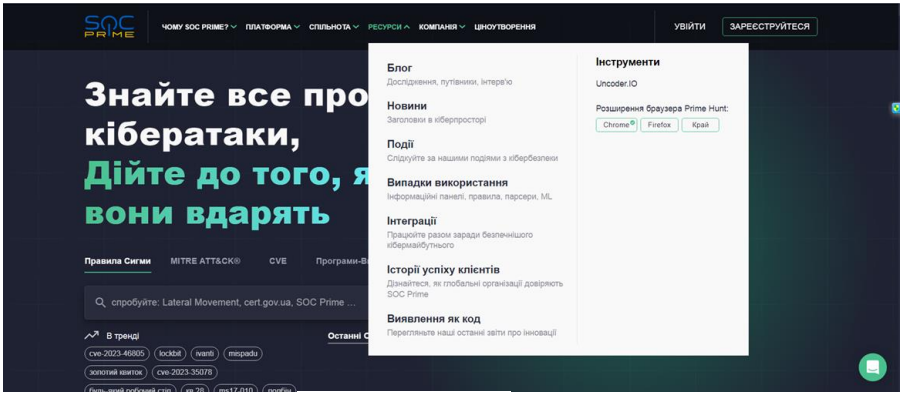


Рис. 14 Розділ Ресурси порталу SOC Prime.

Як ви побачите SOC Prime плідно співпрацює з Корпорація MITRE (творець відомого у спільноті продукту ATT&CK).

На офіційному сайті Корпорації [https://attack.mitre.org/] є навіть подяка SOC Prime за те, що стали вони першим благодійником ATT&CK.

На цьому сайті студентам поки що буде доцільно ознайомитися з розділом Ресурси. Доречи Корпорація MITRE надає вам невиключну, безоплатну ліцензію на використання ATT&CK ® для досліджень, розробок і комерційних цілей.

Далі познайомимося з порталом нашого іншого стейхолдера BALTUM BUREAU (Baltum Büroo – BCERT, [https://baltumburoo.com/uk/]) (див. рис. 15).

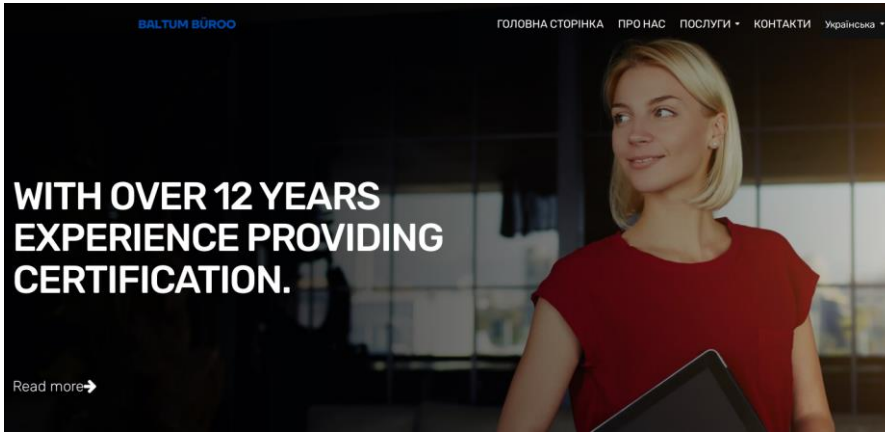


Рис. 15 Портал BALTUM BUREAU.

Як наведено на сайті, ця установа надає послуги з оцінки систем менеджменту та сертифікації ISO організаціям по всьому світу. Вони прагнуть запропонувати більше, ніж просто підхід до сертифікації – вони прагнуть працювати з клієнтами для розвитку їхнього бізнесу та допомогти їм отримати реальні комерційні вигоди від інвестицій в систему менеджменту. Їх мета-оптимізувати процес сертифікації підприємств з меншими

витратами часу і коштів, поєднуючи технічну експертизу і технології.

Нас цікавить перш за все їх зусилля по сертифікації за стандартами ISO/IEC 27001:2022 (Системи управління інформаційною безпекою) та ISO/IEC 27701:2019 (Система управління конфіденційною інформацією).

В цій царині ми докладно попрацюємо з цією установою на 2 курсі практики, а поки можливо передивитися розділи ПОСЛУГИ ▶ Послуги з кібербезпеки (див. рис. 16).

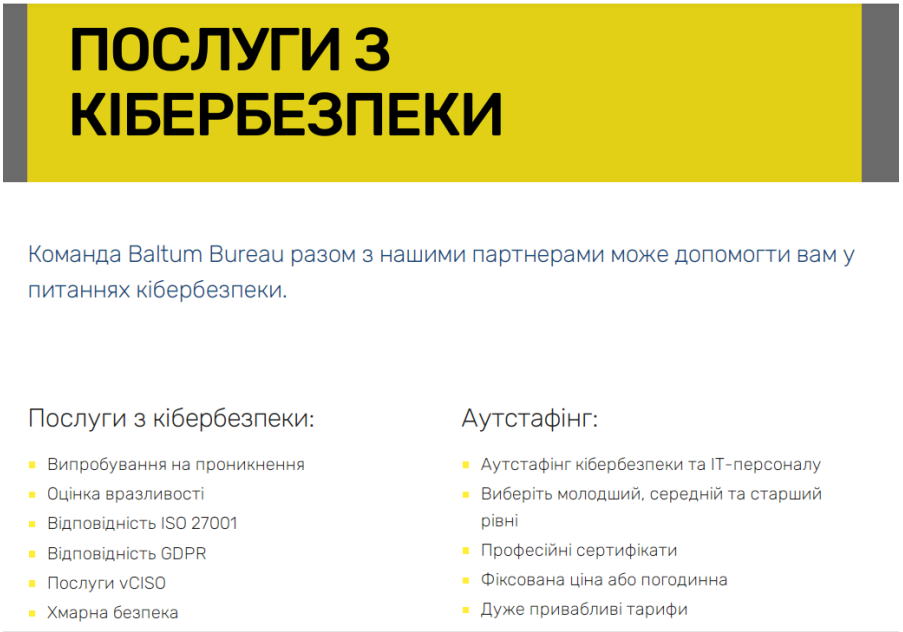


Рис. 16 Послуги з кібербезпеки BALTUM BUREAU.

Занести те, що зацікавило з дослідженого вище до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

3.9 Заняття 9.

Дослідження деяких важливих Інтернет-ресурсів основних гравців на ринку захисту інформації (частина 2).

Перш ніж продовжити нашу роботу з дослідження Інтернет-ресурсів основних гравців на ринку захисту інформації розглянемо ще одну чудову можливість, яка допоможе професійному зростанню студентів.

Про популярність у молоді різноманітних соціальних мереж годі й говорити. Але, як показує практика, поза їх увагою проходе така поважна як LinkedIn [https://ua.linkedin.com/] — соціальна мережа для пошуку і встановлення ділових контактів. У LinkedIn зареєстровано понад 850 мільйонів користувачів, що представляють 150 галузей бізнесу з 200 країн (див. рис. 17).

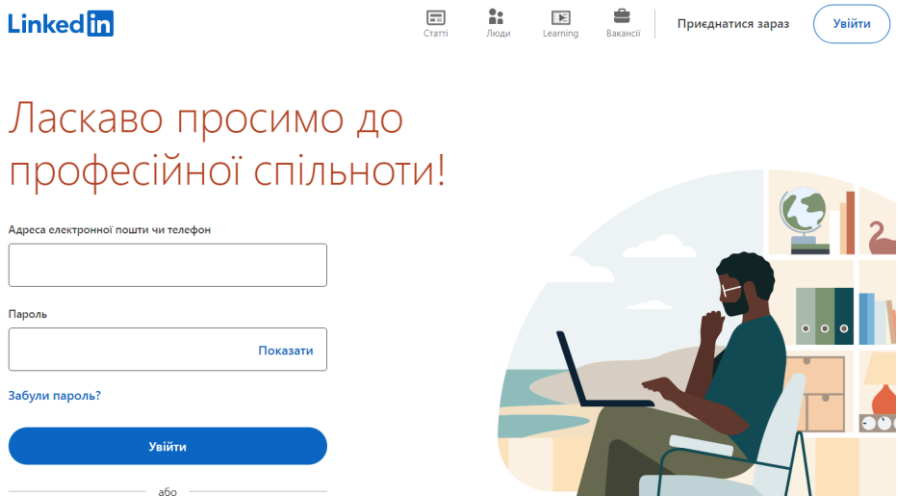


Рис. 17 LinkedIn.

Перед реєстрацією можливо спочатку ознайомитися з довідкою "Що таке LinkedIn і як я можу його використовувати?" [https://www.linkedin.com/help/linkedin/answer/a791920/-linkedin-?lang=uk].

Після цього студенту потрібно зареєструватися у мережі і у вільному режимі дослідити її можливості враховуючи свій фах. Для спеціальності 125 Кібербезпека та захист інформації можна скористатися матеріалами додатку З

Надамо ще декілька ресурсів для самостійного дослідження.

SoftServe [20] — найбільша глобальна IT-компанія з українським корінням, що працює у галузі розробки програмного забезпечення та надання консультаційних послуг.

SoftServe є однією з найбільших компаній-розробників програмного забезпечення у Центральній та Східній Європі та входить до переліку найбільших сервісних IT-компаній України. Близько 13 500 співробітників працюють у 40 офісах, що розміщені від Сан-Франциско до Сінгапуру. Головні офіси компанії розташовані у Львові та Остіні (штат Техас, США). Компанія має центри розробки у Львові, Києві, Дніпрі, Харкові, Рівному, Івано-Франківську, Чернівцях, Ужгороді, Тернополі, Одесі, Вінниці, Луцьку, Ужгороді, Тернополі та Хмельницькому, а також в Польщі, Болгарії, Румунії та в країнах Латинської Америки.

У блозі на AIN.UA компанія ділиться своєю експертизою, глобальним досвідом роботи та розповідає про найцікавіші задачі, з якими розробники стикаються під час роботи.

Information Security Stack Exchange (Обмін стеками інформаційної безпеки, [https://security.stackexchange.com]) – це сайт із запитаннями та відповідями для професіоналів із інформаційної безпеки. Реєстрація займає лише хвилину.

Практики корпоративної безпеки Oracle [https://www.oracle.com/corporate/security-practices/].

EC-Council Cybersecurity Exchange. [https://www.eccouncil.org/cybersecurity-exchange/].

Imperva. [https://www.imperva.com/].

Асоціація фахівців з безпеки інформації «Захист.ЮЕЙ». Комплексні послуги в сфері інформаційної безпеки [https://zahyst-ua.com/].

Компанія H-X. Сервіси безпеки IT і Web3. [https://www.h-x.technology/ua/] Оцінюють, розробляють, впроваджують, сертифікують й підтримують безпечні системи. Викладають безпеку. Додайте у ваші проекти нашу глибоку компетенцію в IT та кібербезпеці.

NordVPN [https://nordvpn.com/uk/pricing/] – поза конкуренцією серед сервісів VPN. NordVPN пропонує широкий вибір різноманітних серверів і ефективних функцій, надійні методи забезпечення конфіденційності й захисту, а також зручні додатки для всіх популярних платформ.

Klik Ukraine Support. [https://www.kliksolutions.com.ua/].

Авторський сайт Валерія Домарєва. Синтезатор системних знань з питань інформаційної безпеки. [https://security.ukrnet.net].

HashDork — це блог, орієнтований на штучний інтелект і технології майбутнього, де ми ділимося думками та висвітлюємо досягнення у сфері штучного інтелекту, машинного навчання та глибокого навчання. Багато важливого по кібербезпеці. [https://hashdork.com/uk/].

Головною метою Наукової асоціації кібербезпеки України [https://scsa.org.ua/] є підвищення загального рівня кібербезпеки українського суспільства за рахунок здійснення наукової, науково-технічної та освітньої діяльності в галузі кібербезпеки і суміжних галузях, спрямованої на розвиток зазначеної галузі та задоволення фахових інтересів своїх членів.

Занести те, що зацікавило з дослідженого вище до розділу щоденника Робочі записи під час практики. (додаток 5 [1]).

3.10 Заняття 10.

Підведення підсумків. Узагальнення та систематизація матеріалу щодо проходження начальної практики. Оформлення проміжного звіту з практики. Остаточне заповнення щоденника практики по першим двом тижням навчання. Отримання проміжного відгуку керівника практики від підприємства.** Отримання проміжного відгуку керівника практики від університету. Оголошення та посилання стосовно проходження практики в наступні два тижня.

Підведення підсумків

- Практиканти закінчують виконання індивідуальних завдань практики.
- Оформляють та підписують звітну документацію.

4. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ.

1. Чим повинна визначатися модель майбутнього спеціаліста у тій частині, яка зв’язана з інформаційно-комунікаційними технологіями та захистом інформації?
2. Які виробничі функції, типові завдання діяльності та уміння, якими повинен володіти випускник вищого навчального закладу з кваліфікацією бакалавра у галузі сучасних ІТ та особливо кібербезпеки?
3. Яку роль грає практика у процесі формування у здобувачів вищої освіти професійних компетентностей, необхідних для успішної роботи в обраній галузі?
4. Яка основна мета проведення навчальної (комп'ютерно-ознайомчої) практики для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 125 Кібербезпека та захист інформації на першому курсі?
5. Які основні завдання навчальної практики?
6. Якими загальними професійними компетентностями буде володіти студент після завершення практики?
7. Згідно з якими основними документами проводиться навчальна практика?
8. Основні складові опису навчальної практики.
9. На формування яких компетентностей, визначених стандартом вищої освіти зі спеціальності 125 Кібербезпека та захист інформації, направлений зміст навчальної практики (комп'ютерно-ознайомчої)?
10. На формування яких програмних результатів навчання, визначених стандартом вищої освіти зі спеціальності 125 Кібербезпека та захист інформації, направлений зміст навчальної практики (комп'ютерно-ознайомчої)?
11. Навчальна практика поглиблює знання перш за все яких дисциплін першого курсу?
12. Структуру та загальний зміст комп'ютерно-ознайомчої практики.
13. База комп'ютерно-ознайомчої практики.
14. Структуру та загальний зміст організації практики.

15. Обов’язки викладачів-керівників практики від кафедри.

16. Обов’язки здобувачів вищої освіти при проходженні практики.

17. Критерії оцінювання практики для здобувачів вищої освіти.

18. Структуру та загальний зміст техніки безпеки, охорони праці та пожежної безпеки при проведенні практики.

19. Які основні правила техніки безпеки та поведінки при роботі у лабораторії обчислювальної техніки Ви знаєте?

20. До чого можуть привести багаторазові порушенні студентом правил техніки безпеки та охорони праці?

21. Що враховується при оцінюванні проходження практики?

22. Що очікує студента, який не виконав програму практики і одержав незадовільну оцінку при захисті звіту?

23. Критерії виставлення оцінок при захисті звітів з практики.

24. З якою метою передбачені індивідуальні завдання?

25. Узагальнений календарний план практики.

26. Порядок контролю проходження практики.

27. Орієнтовний тематичний план частина 1 навчальної (комп'ютерно-ознайомчої) практики.

28. Що входе до додатків до цих методичних вказівок?

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Навчальна практика: метод. рекомендації до проходження навчальної (комп’ютерної) практики для здобувачів першого (бакалаврського) рівня вищої освіти денної (заочної) форми навчання спеціальності 125 Кібербезпека та захист інформації / Держ. біотехнол. ун-т; уклад.: І. В. Чалий, Т. А. Бутенко, Ю.В. Синявіна, Ю. Є. Мегель (Хнуре), А. В. Левкін, О. Д. Міхнова. – Харків : [б.-в.], 2024 – 34 с.

2. Освіта України в умовах воєнного стану. Інформаційно-аналітичний збірник. [Електронний ресурс] – Режим доступу:

[https://mon.gov.ua/storage/app/media/zagalna%20serednya/serpneva-konferencia/2022/Mizhn.serpn.ped.nauk-prakt.konferentsiya/Inform-analityc.zbirn-Osvita.Ukrayiny.v.umovakh.voyennoho.stanu.22.08.2022.pdf].

3. Робоча програма навчальної (ознайомчої) практики здобувачів вищої освіти СО «Бакалавр» спеціальності 125 Кібербезпека освітньої програми «Кібербезпека». Донецький національний університет імені Василя Стуса. URL: [https://www.donnu.edu.ua/wp-content/uploads/sites/8/2020/05/01-rp-z-oznajomchoyi-praktychnoyi-pidgotovky.pdf].

4. Техніка безпеки при роботі на ПК та основи його устрою: метод. вказ. до виконання лабораторних робіт з «Інформатика», «Інформатика та комп'ютерна техніка» для студ. перш. (бакалавр.) рівня вищ. освіти ден., заоч., та дист. форм навчання всіх спеціальностей ФЕЦКТ / Державний біотехнологічний університет; уклад.: Ю.Є. Мегель, О.Д. Міхнова, А.В. Левкін, І.В. Чалий, Д.М. Яковенко – Харків: [б.-в.], ДБТУ, 2022. –46 с.

5. Інструкція №БЖД-18-75 з охорони праці та безпеки життєдіяльності під час роботи у комп'ютерному класі. [https://it.nmu.org.ua/ua/to_students/files_instructions/Інструкція_№БЖД_18_75_з_охорони_праці_та_безпеки_життєдіяльності.pdf].

6. Інструкція №БЖД-18-76 з охорони праці та безпеки життєдіяльності під час роботи у комп'ютерному класі [https://it.nmu.org.ua/ua/to_students/files_instructions/Правила_безпеки_життєдіяльності_№БЖД_18_76.pdf].

7. Вступ до фаху та академічна доброчесність:методичні вказівки для самостійного вивчення дисципліни для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання спеціальності 125 «Кібербезпека». Короткий тлумачний словник основних термінів / Держ. біотехнологічний ун-т; авт.-уклад.: Ю.Є. Мегель, О.Д. Міхнова, А.В. Левкін, І.В. Чалий, Д.М. Яковенко. – Харків : [б.-в.], 2023 – 50 с.

8. Словник термінів з кібербезпеки / за заг. ред. О. В. Копана, Є. Д. Скулиша– К. : ВБ «Аванпост-Прим», 2012р. – 214с.

9. Воробиенко П.П. Англо-русский словарь по телекоммуникациям и информационной безопасности / [Воробиенко П.П., Кузнецова Г.П.,Веретенникова В.П., Стоянова И.И.]. – Одесса: ОНАС им. А.С. Попова, 2012. –212 с.

10. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки / Харків. нац. ун-т ім. В. Н. Каразіна ; уклад. Віталій Іванович Єсін, Сергій Геннадійович Рассомахін. – Харків : ХНУ ім. В. Н. Каразіна, 2018. – 63 с.

11. Англо-український словник термінів з інформаційних технологій та кібербезпеки / ІСЗЗІ КПІ ім. Ігоря Сікорського ; уклад. А. Я. Гладун, О. О. Пучков, І. Ю. Субач, К. О. Хала. – Електронні текстові дані (1 файл: 4,36 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 380 с. – Назва з екрана.

12. Мінцифри представило "словник термінів з онлайн-безпеки". Джерело: [https://censor.net/ua/p3225693].

13. Withdrawn NIST Technical Series Publication. Glossary of Key Information Security Terms [https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf].

14. Методичні вказівки до виконання лабораторної роботи «Використання on-line ресурсів Інтернет для самостійного вивчення дисциплін за фахом» для здобувачів другого (магістерського) рівня вищої освіти, спеціальності 072 «Фінанси, банківська справа та страхування (напрям ІТ)», денної та заочної форми навчання; уклад.: Ю.Є. Мегель, О.Д. Міхнова, А.В. Левкін, І.В. Чалий, Д.М. Яковенко, – Харків [б.-в.],: Державний біотехнологічний університет 2023 – 32 с.

15. Дія. Цифрова освіта». [Електронний ресурс] – Режим доступу: [https://osvita.diia.gov.ua/].

16. [https://www.microsoft.com].

17. З початку 2022 року урядова команда CERT-UA вжила заходів щодо більш ніж 200 деструктивних кібератак проти України [Електронний ресурс] – Режим доступу: [https://cip.gov.ua/ua/news/z-pochatku-2022-roku-uryadova-komanda-cert-ua-vzhila-zakhodiv-shodo-bilsh-nizh-200-destruktivnikh-kiberatak-proti-ukrayini].

18. Боротьба на кіберфронті: як долучитися до української ІТ-армії. [Електронний ресурс] – Режим доступу: [https://thedigital.gov.ua/news/borotba-na-kiberfronti-yak-doluchitisya-do-ukrainskoi-it-armii].

19. Блог SOC Prime. [Електронний ресурс] – Режим доступу: [https://ain.ua/tag/blog_soc_prime/].

20. SoftServe. [Електронний ресурс] – Режим доступу: [https://career.softserveinc.com/uk-ua/about].

21. Кібербезпека. Методичні вказівки до навчальної практики здобувачів вищої освіти освітнього ступеню «бакалавр», спеціальності 125 - «Кібербезпека»/ укладачі: Зейналова Е.Ф., Мехед Д.Б. – Чернігів: Чернігівський національний технологічний університет, 2020. – 21 с.

22. Платформа Prometheus. URL: [https://prometheus.org.ua/].

23. Coursera. URL: [https://www.coursera.org/].

24. Screencast-O-Matic.[Електронний ресурс]. Режим доступу: [http://www.screencast-o-matic.com].

25. VCASMO. [Електронний ресурс]. Режим доступу: [http://www.vcasmo.com].

Додаткові ресурси

1. Верховна Рада України. Законодавство України: [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/.

2. Державна служба спеціального зв’язку та захисту інформації: [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index.

3. CERT-UA: [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.

ДОДАТКИ

Додаток 1[17]

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, з початку 2022 року забезпечила реагування на 200 цільових кібератак деструктивного характеру проти українських установ та компаній. Здебільшого реалізації зловмисного задуму вдалося запобігти. Про це в ході міжнародної конференції «Кіберстійкість у сучасному світі. Досвід України», яка проходить у Варшаві (Польща), сказала керівниця Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA Євгенія Наконечна.

«Кількість кіберінцидентів, які наша команда опрацьовує з початку повномасштабного вторгнення, суттєво збільшилася і зросла майже вдвічі. Ця інтенсивність не зменшується», – зазначила Євгенія Наконечна.

За її словами, об'єктами таких кібератак найчастіше стають міністерства, державні органи, критична інфраструктура, зокрема енергетичний сектор, ІТ-компанії та телекомунікаційні провайдери. Метою зловмисників є розвідувальні операції, довготривале шпигунство, знищення даних та інформаційних систем. Велику роль у протидії кібератаці відіграє виконання рекомендацій CERT-UA об'єктами таких атак.

Керівниця CERT-UA визначила п'ять ключових факторів, які дозволяють урядовій команді успішно боротися з кіберзагрозами:

- плідна та самовіддана праця колективу досвідчених фахівців;
- співпраця з найкращими безпековими компаніями та можливість використання сучасних технологій;
- розробка та експлуатація власних технічних рішень;
- ефективна взаємодія з операторами та провайдерами телекомунікацій та їх співпраця з питань покращення кіберзахисту;

• ефективна взаємодія з ключовими суб'єктами забезпечення кібербезпеки України, зокрема з СБУ, Кіберполіцією, НБУ та ЗСУ.

Нагадаємо, що Урядова команда реагування на комп'ютерні надзвичайні події України підготувала рекомендації з кіберзахисту, виконання яких сприятиме посиленню захищеності систем та мереж і дозволить ефективно протидіяти кіберзагрозам. Ознайомитися з ними можна за посиланням: [https://cert.gov.ua/article/5436463].

Раніше Держспецзв'язку повідомляла про базові заходи з кіберзахисту, які допомагають захистити інформаційні системи організації, вчасно помітити та ліквідувати загрози.

Додаток 2[18]

З початку повномасштабного вторгнення ІТ-фахівці з України та зі всього світу створили ІТ-армію, щоб боротися з ворогом на кіберфронті. Долучитися і підсилити ІТ-армію може кожен охочий залежно від цифрових навичок.

Наразі ІТ-армія об'єднує понад 200 тисяч українських та міжнародних фахівців. Щодня вони відбивають кібератаки та успішно контрнаступають. За 9 місяців повномасштабної війни айті-армія атакувала понад 13 тисяч російських онлайн-ресурсів. Серед них – сайт групи Вагнера, порталу Госуслуги та офіційний сайт кремля. Також відбила понад 1300 кібератак з боку росії. Усе це дало змогу державним та урядовим установам, банкам вистояти і продовжити роботу.

Ви можете використати власні цифрові навички і зробити свій внесок в перемогу.

Чим ви можете бути корисні і як долучитися до ІТ-армії?

• Стати підписником телеграм-каналу ІТ-армії. Ви будете в курсі всіх актуальних завдань та зможете оперативно долучитися до їх виконання.

• Встановити програмне забезпечення (ПЗ) ІТ-армії. Це найпростіший спосіб долучитися до активних дій. Скачуєте та вмикаєте на ноутбуці або на власному сервері ПЗ, розроблене волонтерами ІТ-армії, і допомагаєте щоденним атакам на

економічний, військовий та держсектор рф. Скачати ПЗ можна за посиланням.

- Долучитися до внутрішньої команди. Це фахівці-волонтери, які виконують найскладніші завдання. ІТ-армії потрібні програмісти, пентестери, розвідники. Так, це саме ви будете здійснювати найбільш масштабні атаки, про які потім пишуть в медіа.
- Долучитися до зовнішньої команди. Якщо ви можете надавати обґрунтовані цілі для DDoS-атак, маєте контакт зі спеціальними службами чи якусь корисну інформацію, яку можна використати в кіберпросторі – ІТ-армія чекає на вас. Також айті-фахівці готові співпрацювати з розробниками ПЗ для DDoS та інших атак.

Зараз Україна отримує унікальний досвід боротьби на кіберфронті, який може бути цікавим всьому світові. І ви можете зробити свій внесок в перемогу. Долучайтеся до ІТ-армії!

Додаток 3

Професійний підхід до LinkedIn для фахівців з кібербезпеки

LinkedIn – потужний інструмент для розвитку кар'єри в сфері кібербезпеки. Цей ресурс не лише допомагає знайти роботу, але й дає можливість:

- Налагодити зв'язки з іншими фахівцями та спільнотами.
- Слідкувати за новинами та трендами в галузі.
- Підтримувати професійну репутацію.
- Продемонструвати свої навички, досвід та освіту потенційним роботодавцям.

Ось кілька порад, як використовувати LinkedIn максимально ефективно, створити профіль, який вигідно представить ваші навички та досвід.

1. Фотографія:

- Виберіть професійне фото, яке відповідає вашому іміджу.
- Уникайте селфі та неформальних зображень.

2. Загальні відомості:

- Сформулюйте чіткий та лаконічний слоган, який описує вашу професійну ідентичність.

• Використовуйте ключові слова, релевантні для кібербезпеки.

• Надайте короткий та чіткий опис вашого досвіду та навичок.

• Перевірте текст на орфографію та граматику.

3. Навички та освіта:

• Перелічіть всі ваші технічні та м'які навички, релевантні для кібербезпеки.

• Вкажіть володіння мовами.

• Зверніть увагу на дипломи бакалавра та магістра, курси та сертифікати, які підкреслюють вашу ініціативу та знання в сфері кібербезпеки.

4. Спілкуання:

• Встановіть зв'язки з іншими фахівцями з кібербезпеки.

• Приєднайтеся до груп, пов'язаних з кібербезпекою, наприклад, Мережева академія Cisco та Learning @Cisco Certifications.

• Надавайте допомогу іншим користувачам та публікуйте цінну інформацію.

5. Підтримка актуальності. Оновлюйте свій профіль:

• Регулярно оновлюйте інформацію про ваш досвід, навички та освіту.

• Змінюйте опис попередніх місць роботи, щоб відобразити їх у минулому часі.

• Регулярно публікуйте статті, блог-пости та інші матеріали, які демонструють вашу експертність.

• Використовуйте ключові слова, релевантні для кібербезпеки, у вашому профілі та публікаціях.

6. Пам'ятайте про етику:

• Будьте чесними у своїй інформації.

• Не публікуйте конфіденційну або чутливу інформацію.

• Поводьтеся з іншими користувачами з повагою.

Використання LinkedIn для пошуку роботи:

• Підпишіться на повідомлення від порталів з працевлаштування.

• Шукайте вакансії на сайтах роботодавців.

- Попросіть знайомих з добрими зв'язками допомогти вам із роботою.

Використання LinkedIn може допомогти вам:

- Збільшити ваші шанси на отримання роботи в сфері кібербезпеки.
- Розширити свою мережу контактів.
- Підтримувати свою кар'єрну конкурентоспроможність.

Завдяки правильному підходу до LinkedIn ви зможете досягти своїх кар'єрних цілей у сфері кібербезпеки. Пам'ятайте, що LinkedIn – це динамічний інструмент, який потребує вашого постійного втручання. Оновлюйте свій профіль, будьте активними та спілкуйтеся з іншими користувачами, щоб максимально використовувати можливості цієї платформи.

Навчальне видання

ВСТУП ДО ФАХУ ТА АКАДЕМІЧНА ДОБРОЧЕСНІСТЬ

Методичні вказівки до проведення навчальної (комп'ютерної) практики

для здобувачів першого (бакалаврського) рівня вищої освіти
денної та заочної форм навчання спеціальності
125 Кібербезпека та захист інформації

Укладачі:
ЧАЛИЙ Ігор Вільович
БУТЕНКО Тетяна Андріївна
СИНЯВІНА Юлія Вікторівна
МЕГЕЛЬ Юрій Євгенович
ЛЕВКІН Артур Володимирович
МІХНОВА Олена Дмитрівна

Формат паперу 60x84/16. Гарнітура Times New Roman
Папір для цифрового друку. Друк ризографічний
Умовн. друк. аркушів – 3,5
Наклад 50 пр.
Державний біотехнологічний університет
м. Харків, 61002, вул. Алчевських 44