МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

МЕТОДИЧНІ ВКАЗІВКИ
з виробничої практики
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Кібербезпека та захист інформації. Методичні вказівки з виробничої практики для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 19 с.

Укладачі: ПЕТРЕНКО ТАРАС АНАТОЛІЙОВИЧ, доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук;
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор;
ШЕЛЕСТ МИХАЙЛО ЄВГЕНОВИЧ, професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор;
СЕМЕНДЯЙ СЕРГІЙ МАТВІЙОВИЧ, старший викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – СИНЕНКО МАРИНА АНАТОЛІЇВНА,
доцент кафедри кібербезпеки та математичного моделювання, кандидат фізико-математичних наук, доцент

ЗМІСТ

ВСТУП

У процесі підготовки кваліфікованих фахівців з кібербезпеки та захисту інформації доводиться постійно вирішувати проблему: якими знаннями, уміннями і навичками в галузі комп'ютерних технологій та захисту інформації повинен оволодіти майбутній спеціаліст, аби його професійна діяльність мала найвищу продуктивність. Модель майбутнього спеціаліста у тій частині, яка зв'язана з інформаційно-комунікаційними технологіями та захистом інформації, повинна визначатися тими задачами, які цей спеціаліст має розв'язувати під час своєї професійної діяльності незалежно від конкретної галузі його праці.

При цьому одним з основних практично-корисних завдань спеціальності 125 - Кібербезпека та захист інформації в ННІ електронних та інформаційних технологій є формування у здобувачів вищої освіти чітких уявлень про те, з якою метою, яким чином та якими засобами і технологіями можна забезпечити захист інформації на підприємстві в цілому та в комп'ютерній системі зокрема.

Саме тому в умовах сьогодення, коли високі інформаційно-комунікаційні технології міцно увійшли практично в усі сфери людської діяльності, дуже важливим є формування у майбутніх фахівців з кібербезпеки та захисту інформації саме практичних навичок їх використання в своїй майбутній трудовій діяльності. І саме виробнича практика покликана закріпити у здобувачів вищої освіти (ЗВО) навички з практичного застосування в реальних умовах діяльності підприємств, установ та організацій теоретичних знать на практичних навичок отриманих в ході навчання за спеціальністю.

Виробнича практика є невід'ємною складовою частиною навчального процесу й передбачена навчальним планом спеціальності 125 - Кібербезпека та захист інформації для здобувачів вищої освіти денної форми навчання у Національному університеті «Чернігівська політехніка» і проводиться на підприємствах різних форм власності, в організаціях різних галузей національного господарства, в органах державної влади, наукових установах та на обладнаних відповідним чином навчальних, виробничих й наукових підрозділах університету. Вона спрямована на закріплення теоретичних знань, отриманих ЗВО за час навчання, набуття і удосконалення практичних навичок і умінь в реальних виробничих умовах за спеціальністю 125 – Кібербезпека та захист інформації для здобувачів вищої освіти 2-го курсу денної форми навчання.

Термін проходження практики – протягом 2-х тижнів у VIII семестрі.

Виробнича практика проводиться згідно з Законом України, „Про вищу освіту", Положенням «Про проведення практики студентів вищих навчальних закладів України», Положенням про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка» зі змінами, внесеними згідно з рішенням Вченої ради від 24.04.2023 року протокол № 5, та наказом ректора № 57/ВС від 24.04.2023 та Положенням про організацію освітнього процесу в Національному університеті «Чернігівська політехніка», навчальним планом спеціальності 125 - Кібербезпека та захист інформації, графіком освітнього процесу на відповідний навчальний рік.

Мета цих методичних вказівок – допомога здобувачам вищої освіти за спеціальністю 125 – Кібербезпека та захист інформації НУ «Чернігівська політехніка» у питаннях планування, проведення та підведення підсумків практики. У методичних вказівках наведено інформацію щодо мети, завдань, організації та інформаційного обсягу виробничої практики, форм та методів контролю, рекомендованих нормативно-правових актів, а також додатки з бланками документів практики.

1 МЕТА І ЗАВДАННЯ ПРАКТИКИ

Метою практики є забезпечення єдності теоретичного і практичного навчання ЗВО з питань організації діяльності підрозділів захисту інформації, включаючи особливості функціонування підприємств та вирішуваних ними завдань, набуття ЗВО практичних навичок розробки пропозицій по вдосконаленню та підвищенню ефективності прийнятих технічних мір і організаційних заходів із застосуванням сучасних технологій захисту інформації, підготовка ЗВО до ефективного використання отриманих знань в процесі самостійного розв’язання фахових завдань. Отримання навичок проведення аналізу інформаційних систем конкретного об'єкту управління з метою самостійного проектування та розробки елементів захищених автоматизованих інформаційних систем з використанням сучасних інформаційних технологій та розвинутих інструментальних засобів захисту інформації.

Під час проходження виробничої практики здобувачі вищої освіти розширюють на практиці набуті в ході попереднього навчання наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 – Кібербезпека та захист інформації:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Завдання практики:

– поглиблення, закріплення і поповнення теоретичних знань та практичних навичок, отриманих при вивченні навчальних дисциплін ОП спеціальності 125 – Кібербезпека та захист інформації;

– набуття ЗВО навичок експлуатації інформаційних систем, а також суспільної і організаційної роботи в колективі;

– формування у ЗВО практичні навичок в роботі з програмним та апаратним забезпеченням, комп'ютерними системами та мережами, базами даних на знань на підприємстві та забезпечення їх безпеки;

– оволодіння ЗВО сучасними методами, формами організації роботи за спеціальністю (практичними навичками з автоматизації захисту інформації, інформаційних систем та процесів, безпечного функціонування автоматизованих інформаційних систем і мереж тощо);

– засвоєння ЗВО на практиці структури інформаційно-аналітичної діяльності та загальнонаукових і спеціальних методів, що застосовуються в управлінні захистом інформації;

– розвинути у ЗВО професійне вміння приймати самостійні рішення під час виконання конкретної роботи та ін.

До початку практики ЗВО повинні мати базові знання з наступних дисциплін:

1. Операційні системи.
2. Безпека комп'ютерних мереж.
3. Технології програмування.
4. Системи технічного захисту інформації.
5. Програмний захист інформації.
6. Комплексні системи захисту інформації.
7. Безпека інформації в інформаційно-комунікаційних системах.

Після проходження виробничої практики ЗВО повинен уміти:

- вивчати характеристики об'єкту управління і розробляти схему організаційної структури управління об'єктом (підприємством, установою, організацією, що є базою практики);
- обстежувати підприємство, вивчати його інформаційну діяльність, визначати об`єкти захисту – інформацію з обмеженим доступом, виявляти загрози, аналізувати їх та будувати моделі загроз.
- розробляти рекомендації щодо впровадження комплексної системи захисту інформації на підприємстві;
- розробляти рекомендації щодо реалізації організаційних заходів захисту інформації на підприємстві;
- розробляти рекомендації щодо реалізації технічних заходів захисту інформації на підприємстві

– формулювати висновки, що розкривають переваги і недоліки в системі захисту АІС, що функціонує на об’єкті управління;
– розробляти вимоги до захисту проектованої підсистеми АІС по схемі “як є – як повинно бути”;
– працювати зі спеціалізованим програмним забезпечення для захисту інформації та ін.

Виробнича практика надає змогу здобувачам вищої освіти закріпити та поглибити навички передбачені наступними програмними результати навчання:

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, в тому числі міжнародних в галузі інформаційної та/або кібербезпеки;

ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної і/або кібербезпеки;

2 ОРГАНІЗАЦІЯ ВИРОБНИЧОЇ ПРАКТИКИ

2.1 Бази практики

Виробнича практика проводиться на підприємствах різних форм власності, в організаціях різних галузей національного господарства, в органах державної влади, наукових установах і організаціях, діяльність яких безпосередньо пов’язана з інформаційними технологіями або захистом інформації, або в структурі яких є підрозділи що забезпечують інформаційну безпеку або в штаті є посада фахівця в галузі інформаційних технологій.

Підприємства - бази виробничої практики повинні мати можливість забезпечити проходження практики та виконання індивідуальних завдань ЗВО

відповідно до програми практики. На базах практики повинне функціонувати сучасне технічне обладнання, програмне забезпечення та системи зв'язку. Практика здобувачів вищої освіти може проводитися на базі підприємств, установ та організацій, що розташовані за кордоном.

За згодою сторін практика може проводитися в онлайн-режимі. Організація і порядок проведення практики в онлайн-режимі передбачаються в Угоді на проведення онлайн-практики, яка укладається між Університетом і базою практики.

Здобувачі вищої освіти можуть самостійно запропонувати підприємство – базу проходження практики, з яким в Університету не заключений договір про проходження практики. Кафедра дає згоду про проходження практики на таких базах лише за умови, що вони відповідають вищезазначеним вимогам. В такому випадку ЗВО повинні самостійно забезпечити підписання угоди про проходження практики з підприємством-базою практики.

Залежно від виду практики бази можуть використовуватися здобувачами вищої освіти як колективно, так і індивідуально.

Із базами практики Університет завчасно укладає угоди на її проведення за встановленою формою (додаток №1). Повний список підприємств – баз практик, з якими в НУ «Чернігівська політехніка» укладений договір про проходження практик розміщений за посиланням: http://surl.li/mhetk

Бланки документів необхідні для проходження практики (угода, направлення на практику, титульна сторінка та зміст звіту про проходження практики, відгук і оцінка роботи здобувача вищої освіти) можна знайти в додатках до Положення про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка».

2.2 Обов'язки керівників практики

Відповідно до Положення про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка» загальну організацію практики та контроль за її проведенням в Університеті здійснює відділ з питань працевлаштування, практики та зв'язків з громадськістю. Навчально-методичне забезпечення і виконання програми виробничої практики забезпечує кафедра кібербезпеки та математичного моделювання.

Безпосереднє керівництво виробничою практикою здобувачів вищої освіти покладається на керівника практики за місцем проходження виробничої практики та керівника практики від кафедри кібербезпеки та математичного моделювання. До керівництва практикою залучаються досвідчені, висококваліфіковані фахівці.

Безпосередній керівник практики від бази практики здійснює постійний контроль за роботою практикантів, веде облік виходу їх на роботу. Про всі недотримання правил трудової дисципліни, внутрішнього розпорядку та інші порушення повідомляє керівника практики від кафедри.

Обов'язки керівника практики від кафедри:

– організація проходження виробничої практики й проведення

організаційних заходів перед направленням здобувачів вищої освіти на практику, зокрема:

1) інструктаж про порядок проходження виробничої практики та з техніки безпеки(інструктаж також проводиться при прибутті на місце проходження практики),

2) надання здобувачам вищої освіти-практикантам необхідних документів (угода, програма, індивідуальне завдання, відгук тощо), перелік яких встановлюється у наскрізній програмі про проведення практики здобувачів вищої освіти,

3) ознайомлення здобувачів вищої освіти із системою звітності з практики, прийнятою на кафедрі кібербезпеки та математичного моделювання, а саме: звіту, прикладу оформлення виконаного індивідуального завдання тощо;

4) проведення із здобувачами вищої освіти попереднього обговорення змісту й результатів практики, потреб уточнення програми тощо;

– координація роботи керівників виробничої практики від бази практики;

– контроль умов праці здобувачів вищої освіти під час проходження практики;

– надання ЗВО допомоги в доборі матеріалу для виконання індивідуального завдання і контроль за його виконанням;

– оцінка якості роботи ЗВО.

– подання завідувачу кафедри та працівнику відділу з питань працевлаштування письмового звіту про проведення практики із зауваженнями й пропозиціями щодо поліпшення практики здобувачів вищої освіти

Керівником виробничої практики від бази практики може бути: керівник підприємства-бази практики, керівник ІТ-відділу або інший висококваліфікований спеціаліст сфері інформаційних технологій та/або кібербезпеки підприємства-бази практики.

Обов’язки керівника практики від бази практики:

– затвердження календарного плану проходження практики;

– забезпечення умови для виконання здобувачами вищої освіти програми практики;

– проведення інструктажу на робочому місці в процесі виконання конкретних видів робіт;

– здійснення контролю за виконанням термінів та процесом проходження практики здобувачами вищої освіти;

– закріплення за практикантами безпосередніх керівників із числа висококваліфікованих спеціалістів ІТ-відділу;

– надання характеристику на кожного здобувача вищої освіти після закінчення практики;

– підтримка постійного зв’язку із закладом вищої освіти.

2.3 Обов’язки здобувачів вищої освіти

– до початку виробничої практики одержати від керівника практики

кафедри інструктаж про порядок проходження практики та з техніки безпеки і консультації щодо оформлення усіх необхідних документів;

– своєчасно прибути на базу практики;

– забезпечити збір необхідного фактичного матеріалу для написання звіту про практику;

– у повному обсязі виконувати всі завдання, передбачені цією програмою виробничої практики;

– вивчити і суворо дотримуватися правил охорони праці та техніки безпеки і виробничої санітарії;

– нести відповідальність за виконану роботу;

– своєчасно подати необхідні звітні документи та захистити результати практики.

Під час проходження виробничої практики здобувачі вищої освіти повинні дотримуватися правил внутрішнього розпорядку які встановлені на підприємстві – базі практики.

Здобувач вищої освіти, який офіційно працевлаштований на підприємстві, в установі чи організації на посаді, що відповідає спеціальності 125 – Кібербезпека та захист інформації, має право на зарахування практики на підставі відповідної заяви здобувача вищої освіти з візою керівника практики від кафедри, до якої додається довідка з місця роботи за фахом.

У даному випадку угода на проведення практики між Університетом та підприємством, або установою чи організацією не укладається, направлення на практику здобувачеві вищої освіти не видається. Проте за здобувачем вищої освіти залишається обов'язок підготовки звітної документації та її захисту.

3 ЗМІСТ ВИРОБИЧОЇ ПРАКТИКИ

Зміст виробничої практики визначається вимогами освітньо-кваліфікаційної характеристики та освітньо-професійної програми підготовки бакалаврів за спеціальністю 125 – Кібербезпека та захист інформації.

Алгоритм проходження практики визначається специфікою бази практики, індивідуальним завданням, цими методичними вказівками.

Практиканти, крок за кроком, працюють над завданнями наведеними в індивідуальній програмі практики, використовуючи знання набуті під час підготовки за спеціальністю, формують практичні навички щодо порядку проведення робіт з захисту інформації відповідно до встановленої політики інформаційної безпеки на базі практики, стандартів на інших нормативно-правових документів.

Для досягнення поставлених цілей та задач виробничої практики практиканти працюють на місцях, що відповідають спеціальності 125 - Кібербезпека та захист інформації а також рівню їх освітньо-професійної підготовки з урахуванням особливостей баз практики.

Оскільки під час виробничої практики ЗВО отримують нові знання та практичні навички в основному при виконанні конкретних практичних завдань,

то найбільш доцільною є їх робота поряд з фахівцями які працюють на штатних посадах.

Під час практики потрібно більш детально розглянути положення основних стандартів в галузі захисту інформації. Також, для формування вмінь та навичок, у цей час особливу увагу потрібно приділити нормативним документам розроблених державною службою спеціального зв'язку та захисту інформації України. Це дасть змогу виконати завдання практики у повному обсязі.

Важливою складовою змісту практики виступають також індивідуальні завдання, які обираються здобувачами вищої освіти відповідно до їхніх нахилів, наукових інтересів, можливостей бази практики та попередньо обговорюються з керівниками практики.

В процесі проходження практики увага акцентується на набутті та удосконаленні вищезазначених загальних та фахових компетентностей, досягненню прогнозованих результатів навчання, розвитку творчих здібностей ЗВО та його самостійності, умінні приймати рішення і нести відповідальність за них, розвитку комунікативних якостей та здатності працювати в колективі.

3.1 Орієнтовний тематичний план

№	Тема програми
1.	Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки
2.	Обстеження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.
3.	Розробка рекомендацій щодо впровадження комплексної системи захисту інформації на підприємстві
4.	Розробка рекомендацій щодо реалізації організаційних заходів захисту інформації на підприємстві
5.	Розробка рекомендацій щодо реалізації технічних заходів захисту інформації на підприємстві
6.	Виконання індивідуального завдання
7.	Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку
Всього – 90 годин практики	

3.2 Методичні рекомендації

1. Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки

Практиканти знайомляться з програмою практики, її основними тематичними розділами. Отримують від керівника практики індивідуальні завдання та документи які потрібно оформити під час проходження практики.

Після прибуття на підприємство практикант повинен ознайомитися:

- з відомчим підпорядкуванням бази практики, основними нормативно-правовими документами, що лежать в основі її діяльності;

- з режимом роботи і правилами внутрішнього розпорядку;

- з вимогами, які пред'являються до працівників бази практики, їх професійних компетентностей в сфері інформаційних технологій та захисту інформації;

- з основними обов'язками працівників та посадових осіб бази практики які відповідають за інформаційну безпеку;

Керівник установи призначає ЗВО керівника практики від бази практики, ознайомлює з порядком проходження, розпорядком роботи установи. На основі запропонованого орієнтовного тематичного плану, враховуючи конкретні умови роботи установи та його підрозділів, складається календарний графік проходження практики. Цей графік підписується керівником практики від бази практики. У разі потреби при виконанні індивідуальних завдань ЗВО складає і затверджує особистий план.

Практиканти проходять інструктаж з техніки безпеки під час проходження практики.

2. Обстеження підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту – інформації з обмеженим доступом, виявлення загроз, їхній аналіз.

Практикантам в ході обстеження бази практики необхідно:

- провести аналіз умов функціонування підприємства, його розташування на місцевості для визначення можливих джерел загроз;

- дослідити засоби забезпечення інформаційної діяльності, які мають вихід за межі контрольованої території;

- вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізацій), а також інженерних комунікацій та металоконструкцій;

- дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання інформації;

- визначити наявність та технічний стан засобів забезпечення технічного захисту інформації;

- перевірити наявність на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог технічного захисту інформації, а також нормативної та експлуатаційної документації, яка забезпечує інформаційної діяльності;

- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню;

- визначити технічні засоби, що потребують переобладнання та встановлення засобів технічного захисту інформації.

За результатами обстеження ЗВО складають акт в довільній формі, який додають до звіту про проходження практики.

3. Розробка рекомендацій щодо впровадження комплексної системи захисту інформації на підприємстві

На підставі матеріалів обстеження ***підприємства, вивчення його інформаційної діяльності, визначення об`єктів захисту ЗВО*** повинні визначити головні задачі захисту інформації і скласти технічне завдання на розроблення системи захисту інформації на підприємстві.

Наступним кроком практиканти повинні дослідити:

- розпорядчі, організаційно-методичні, нормативні документів з технічного захисту інформації що застосовуються на підприємстві, а також вказівки щодо їхнього застосування;
- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;
- інструкції, що встановлюють обов`язки, права та відповідальність персоналу;

4. Розробка рекомендацій щодо реалізації організаційних заходів захисту інформації на підприємстві

Організаційні заходи захисту інформації - комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення технічного захисту інформації.

ЗВО у процесі розроблення рекомендацій щодо реалізації організаційних заходів потрібно:

- визначити окремі задачі захисту інформації з обмеженим доступом;
- обґрунтувати структуру і технологію функціонування системи захисту інформації;
- визначити права та обов`язки підрозділів та осіб, що беруть участь в обробленні інформації з обмеженим доступом;
- запропонувати засоби забезпечення технічного захисту інформації та нормативні документи для забезпечення ними підприємства-бази практики;
- встановити порядок впровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю технічного захисту інформації;
- - визначити зони безпеки інформації, тощо;

Практиканти повинні розробити пропозиції щодо коригування плану технічного захисту інформації в цілому або окремих його елементів.

5. Розробка рекомендацій щодо реалізації технічних заходів щодо захисту інформації на підприємстві

У процесі розробки рекомендацій щодо реалізації первинних технічних заходів щодо захисту інформації на підприємстві практиканти повинні передбачити:

- блокування каналів витоку інформації;
- блокування несанкціонованого доступу до інформації чи її носіїв;
- перевірку справності та працездатності технічних засобів забезпечення інформаційної діяльності.

Блокування каналів витоку інформації може здійснюватися:

- демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням підприємства та обробленням інформації з обмеженим доступом;
- видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює інформації з обмеженим доступом;
- тимчасовим відключенням технічних засобів, які не беруть участі в обробленні інформації з обмеженим доступом, від ліній зв'язку, сигналізації, керування та енергетичних мереж;
- застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення інформаційної діяльності.

Блокування несанкціонованого доступу до інформації або її носіїв може здійснюватися:

- створенням умов роботи в межах установленого регламенту;
- унеможливленням використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

У процесі розробки рекомендацій щодо реалізації основних технічних заходів захисту практикантам потрібно:

- запропонувати встановити засоби виявлення та індикації загроз і перевірити їхню працездатність;
- запропонувати встановити захищені засоби оброблення інформації, засоби технічного захисту інформації та перевірити їхню працездатність;
- запропонувати застосування конкретних програмних засобів захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє функціональне тестування і тестування на відповідність вимогам захищеності;

Вибір засобів забезпечення технічного захисту інформації зумовлюється фрагментарним або комплексним способом захисту інформації.

Фрагментарний захист забезпечує протидію певній загрозі.

Комплексний захист забезпечує одночасну протидію безлічі загроз.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

6. Виконання індивідуального завдання

Під час проходження практики практиканти виконують заздалегідь отримане від керівника практики індивідуальне завдання. Порядок отримання завдань та їх орієнтовна тематика наведені в п. 3.3

7. Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку

Практиканти закінчують виконання індивідуальних завдань практики. Оформлюють та підписують звітну документацію (звіт про проходження практики, звіт про виконання індивідуального завдання, додатки, відгук керівника практики від підприємства, характеристику, тощо.) Представляють результати виконаних завдань на заліку.

3.3 Індивідуальні завдання

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

Індивідуальне завдання видається з метою формування у практикантів навичок самостійної роботи, уміння використовувати теоретичні знання в конкретних видах діяльності, аналізувати і оцінювати рівень інформаційної безпеки бази практики на основі теоретичних знань, які вони одержали в навчальному закладі, надбання ЗВО під час практики умінь та навичок самостійного розв'язання завдань, пов’язаних з використанням комп’ютерної техніки в своїй роботі, активізації діяльності ЗВО, розширення їх світогляду.

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

Формами індивідуальної роботи можуть бути:

- написання рефератів на певну тему;
- складання задач;
- проведення досліджень.

Індивідуальні завдання розробляються викладачами кафедри кібербезпеки та математичного моделювання.

Спеціальний час для написання індивідуального завдання не відводиться, воно виконується одночасно з проходженням тем практики.

Безпосередній керівник практики в установі бази практики надає ЗВО допомогу в зборі необхідного матеріалу (бланки, документи, література), контролює виконання завдання.

3.4 Документи та звітність за підсумками практики

Загальна форма звітності здобувача вищої освіти про результати проходження практики – це подання письмового звіту. Звіти про результати проходження практики оформлюються в електронному, друкованому або письмовому вигляді, підлягають оцінці та підписуються безпосередньо керівником від бази практики.

Після цього здобувачі вищої освіти розміщують електронний варіант сканованих копій вищеназваних звітних документів у системі дистанційного навчання Moodle, і керівники практики від кафедри проводять їх перевірку.

У звіті мають бути відомості про виконання здобувачем вищої освіти усіх розділів програми практики та індивідуального завдання, розділи з охорони праці та техніки безпеки, висновки та пропозиції, список використаних джерел.

Оформлюється звіт за вимогами встановленими ДСТУ 3008:2015 "Звіти у сфері науки і техніки. Структура та правила оформлення".

4 ФОРМИ І МЕТОДИ КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Поточний контроль здійснюється керівником практики від бази практики, з залученням у разі необхідності керівника практики від кафедри шляхом оцінювання якості роботи здобувачів вищої освіти на базі практики та виконання індивідуального завдання. При цьому оцінюється рівень теоретичної та практичної підготовки практикантів до вирішення конкретних завдань, їх дисциплінованість, пунктуальність, ініціативність, самостійність а також повнота, своєчасність та правильність виконання завдань, рівень

В ході захисту результатів практики ЗВО надають оформлені відповідно до вимог документи про проходження практики (щоденник, звіт, індивідуальне завдання), звітують про результати своєї роботи під час проходження виробничої практики, представляють результати виконання індивідуального завдання.

Підсумковий контроль проводиться у вигляді заліку, в ході якого оцінюються теоретичні знання та практичні навички, набуті або вдосконалені в ході проходження виробничої практики. При цьому враховується своєчасність виконанням програми практики та оформлення звітної документації (звіту про проходження практики та індивідуального завдання), відповідність її оформлення встановленим вимогам.

5. ПІДБИТТЯ ПІДСУМКІВ ПРАКТИКИ

Після закінчення строку проходження виробничої практики здобувачі вищої освіти звітують про проходження практики перед комісією, призначеною завідуючою кафедрою, до складу якої входять керівники практики від кафедри. Комісія приймає звіт у здобувачів вищої освіти в останні дні проходження практики на базах практики або в університеті протягом перших трьох днів після закінчення практики.

Оцінювання результатів практики здійснюється за національною шкалою та шкалою ECTS. Результати захисту практики вносяться керівником практики в особистому електронному кабінеті в автоматизованій системі управління Університету (АСУ «ВНЗ») до електронної відомості обліку успішності.

У разі отримання незадовільної оцінки за захист практики, перескладання здійснюється за графіком, установленим дирекцією ННІ електронних та інформаційних технологій і допускається не більше двох разів. Перший раз –

керівнику практики від кафедри, при другому перескладанні – комісії, яка створюється розпорядженням директора ННІ електронних та інформаційних технологій. Для документального оформлення результатів ліквідації академічної заборгованості здобувачів вищої освіти в АСУ «ВНЗ» працівниками дирекції ННІ електронних та інформаційних технологій формується ліквідаційна електронна відомість, яку НПП заповнює у визначений день ліквідації академічної заборгованості.

Оцінка з практики враховується при нарахуванні стипендії за результатами літнього семестрового контролю.

Результати оцінювання практики можуть бути оскаржені здобувачами вищої освіти у порядку, що регламентується «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка».

Здобувачу вищої освіти, який не приступив до виробничої практики своєчасно з поважних причин призначається проходження практики в інший період (відповідно до індивідуального графіку та наказу ректора).

Шкала оцінювання здобувачів вищої освіти

Оцінка за системою ECTS	**Визначення**	**Оцінка за 100-бальною шкалою**	**Оцінка за національною системою**
A	Відмінно	90-100	Відмінно
B	Добре	82-89	Добре
C	Добре	75-81	Добре
D	Задовільно	66-74	Задовільно
E	Задовільно	60-65	Задовільно
FX	Незадовільно – з можливістю повторного складання	0-59	Незадовільно

Критерії оцінювання здобувачів вищої освіти з урахуванням конвертації балів у їх нормовану кількість

Оцінки				Зміст критеріїв оцінки
відмінно	5	90-100	A	Матеріали про проходження практики оформлені відповідно до вимог. Доповідь здобувача вищої освіти продумана, структурована, містить основні результати проходження практики, відповіді на питання членів комісії повні, розуміння матеріалу глибоке, основні вміння сформовані та засвоєні, виклад логічний, обґрунтований, висновки і узагальнення точні, мають місце практичні рекомендації; використання фахової термінології правильне. Керівники від бази практики та університету оцінили роботу на «відмінно».
добре	4	82-89	B	Мають місце неістотні зауваження щодо змісту та оформлення матеріалів про проходження практики. Доповідь здобувача вищої освіти продумана, обґрунтована, містить основні результати проведеного дослідження, відповіді на питання членів комісії повні, розуміння матеріалу достатньо глибоке, основні вміння сформовані та засвоєні, висновки й узагальнення точні, мають місце практичні рекомендації; використання фахової термінології правильне. Керівники від бази практики та від університету оцінили проходження практики на «добре» або один із керівників практики оцінив її проходження на «відмінно», а інший – на «добре».
добре	4	75-81	C	Мають місце неістотні зауваження щодо змісту та оформлення матеріалів про проходження практики. Доповідь здобувача вищої освіти продумана, обґрунтована, містить основні результати проведеного дослідження, відповіді на питання членів комісії повні, розуміння матеріалу достатньо глибоке, основні вміння сформовані та засвоєні, висновки й узагальнення точні, мають місце практичні рекомендації ,правильно використовує фахову термінологію. Але виклад матеріалу недостатньо систематизовано, у визначенні понять, термінології та узагальненнях мають місце окремі помилки, які виправляються за допомогою додаткових питань членів комісії. Керівники від бази практики та від університету оцінили проходження практики на «добре».
задовільно	3	66-74	D	Недбале оформлення звіту й щоденника про проходження практики. Доповідь здобувача вищої освіти свідчить про розуміння основних питань програми практики, проте мають місце окремі прогалини в знаннях: визначення понять нечіткі, неточні, висновки й узагальнення, практичні рекомендації аргументовані слабо, в них допускаються помилки, знання фрагментарні, неповні, спостерігається невміння працювати з документами, нормативними джерелами, користуватися фаховою термінологією. Керівники від бази практики та від університету оцінили проходження практики на «задовільно» або один із керівників практики оцінив її проходження на «задовільно», а інший – на «добре».
		60-65	E	Недбале оформлення звіту й щоденника про проходження практики. Доповідь здобувача вищої освіти свідчить про розуміння основних питань програми практики, проте мають місце значні прогалини в знаннях: визначення понять нечіткі, неточні, недостатні, висновки й узагальнення, практичні рекомендації аргументовані слабо, у них допускаються помилки, знання практиканта фрагментарні, неповні, спостерігається невміння працювати з документами, нормативними джерелами, фаховою термінологією. Керівники від бази практики та від університету оцінили проходження практики на «задовільно».
незадовіль	2	0-59	FX	Мають місце істотні зауваження щодо змісту й оформлення матеріалів про проходження практики. Доповідь здобувача вищої освіти належним чином не підготовлена, відповіді на питання членів комісії не обґрунтовані або відсутні, розуміння змісту та завдань практики; здобувач вищої освіти недостатньо орієнтується в особливостях захисту інформації, не в змозі на належному рівні використовувати фахову термінологію. Керівники практики від університету та бази практики оцінили роботу на «незадовільно» або один із керівників практики оцінив її проходження на «задовільно», а інший – на «незадовільно».

6 ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Закон України.“Про захист інформації в автоматизованих системах”.// Галицькі контракти. – 1996. - № 47. – С. 54 – 56.
2. Закон України «Про вищу освіту» від 1 липня 2014 року, № 1556-VII// Відомості Верховної Ради України , 2014, № 37-38, ст.2004
3. Положення «Про проведення практики студентів вищих навчальних закладів України»: наказ Міністерства освіти України від 08.04.1993р. № 93
4. Положення «Про проведення практики здобувачів вищої освіти Національного університету «Чернігівська політехніка», затверджено вченою радою Національного університету «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6, введено в дію наказом ректора від 31 серпня 2020 р. № 26
5. Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка», затверджено Вченою радою Національного університету «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 Введено в дію наказом ректора від 31 серпня 2020 р. № 26
6. ДСТУ 3008:2015 "Звіти у сфері науки і техніки. Структура та правила оформлення": наказ ДП «УкрНДНЦ» від 22 червня 2015 р. № 61
7. ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів»: наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 1 липня 2020 р. № 144.
8. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання: ДСТУ 7.1:2006. Чинний від 07.01.2007. - К. : Держспоживстандарт України, 2007. - 47 с.
9. Оформлення наукових джерел відповідно до вимог Вищої атестацій-ної комісії України [Електронний ресурс] // Вища атестаційна комісія України. – 2019. – Режим доступу до ресурсу: https://vak.in.ua.
10. Правила забезпечення захисту інформації в інформаційних телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені поста-новою КМУ від 29 березня 2006. - №373.
11. http://robota-chntu.stu.cn.ua/- веб-портал Центру розвитку кар'єри НУ "Чернігівська політехніка.
12. Система дистанційного навчання НУ «Чернігівська політехніка». [Електронний ресурс]. – Режим доступу: http://eln.stu.cn.ua/
13. Бібліотека та читальний зал НУ «Чернігівська політехніка». – [Електронний ресурс]. – Режим доступу: http://library2.stu.cn.ua
14. Національна бібліотека ім В.І. Вернадського / [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/