МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

КІБЕРБЕЗПЕКА
МЕТОДИЧНІ ВКАЗІВКИ
до виробничої практики

за спеціальністю 125 «Кібербезпека»
(освітньо-кваліфікаційний рівень - бакалавр)

Обговорено і рекомендовано на
засіданні кафедри кібербезпеки та
математичного моделювання
Протокол №8
Від 19 лютого 2019 року

ЧЕРНІГІВ – 2020

Кібербезпека. Методичні вказівки до виробничої практики / укладач: Петренко Т.А. – Чернігів: Чернігівський національний технологічний університет, 2020. – 37 с.

Розробник:

Петренко Т.А., доцент кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск:

Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук, доцент

Рецензент:

Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, кандидат педагогічних 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 курсу інформаційної безпеки на факультеті інформаційних та комп'ютерних систем є формування у студентів 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 комп'ютерні технології міцно увійшли практично в усі сфери людської діяльності, дуже важливим є формування у майбутніх фахівців з захисту інформації саме практичних навичок їх використання в своїй майбутній трудовій діяльності. Саме фахова ознайомлювальна практика покликана закріпити в студентів навички з практичного застосування в своїй майбутній діяльності сучасних комп'ютерних технологій.

Практика займає важливе місце в вирішенні завдання підготовки висококваліфікованих спеціалістів, які володіють комплексом професійних знань, практичними навичками роботи напрямом підготовки 6.170103 «Управління інформаційною безпекою» та спеціальністю 125 "Кібербезпека" та необхідними організаторськими якостями.

Практика студентів є невід'ємною складовою процесу підготовки фахівців за вищезазначеним напрямом (спеціальністю) у Чернігівському національному технологічному університеті 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 студентами за час навчання, набуття і удосконалення практичних навичок і умінь за напрямом підготовки 6.170103 «Управління інформаційною безпекою» та спеціальністю 125 «Кібербезпека» для студентів IV курсу денної форми навчання.

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

Виробнича практика проводиться згідно з Законами України „Про освіту", „Про вищу освіту", Положеннями «Про організацію навчального процесу у вищих навчальних закладах» (наказ МОН України від 02.06.93 № 161) та «Про проведення практики студентів вищих навчальних закладів України» затвердженим наказом Міністерства освіти України від 08.04.1993р. № 93, наказами і директивними вказівками Міністерства освіти і науки України та Положенням про проведення практики студентів Чернігівського національного технологічного університету затвердженим наказом ректора ЧНТУ від 15.05.2013р. №67 та вимогами Міжнародного стандарту якості ISO серії 9000.

Зміст виробничої практики визначається діючим навчальним планом підготовки фахівців за напрямом підготовки 6.170103 «Управління інформаційною безпекою» та спеціальністю 125 «Кібербезпека» та відповідними програмами з курсів «Основи технічного захисту інформації», «Основи криптографічного захисту інформації» «Безпека інформації в інформаційно-комунікаційних системах», «Менеджмент інформаційної безпеки» та інших фундаментальних та професійно–орієнтованих дисциплін.

1 МЕТА І ЗАВДАННЯ ВИРОБНИЧОЇ ПРАКТИКИ

Виробнича на практика студентів має за мету закріплення, поглиблення і систематизацію теоретичних знань, отриманих під час навчання за напрямом підготовки 6.170103 «Управління інформаційною безпекою» та спеціальністю 125 «Кібербезпека», в процесі реальної практичної діяльності.

Метою практики є забезпечення єдності теоретичного і практичного навчання студентів з питань організації діяльності підрозділів захисту

інформації, включаючи особливості функціонування підприємств та вирішуваних ними завдань, набуття студентами практичних навичок розробки пропозицій по вдосконаленню та підвищенню ефективності прийнятих технічних мір і організаційних заходів із застосуванням сучасних технологій захисту інформації, підготовка студентів 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.

Завдання практики:

- поглиблення, закріплення і поповнення теоретичних знань, придбаних при вивченні теоретичних курсів за напрямом підготовки 6.170103 «Управління інформаційною безпекою» та спеціальністю 125 «Кібербезпека»;
- навчити студентів використовувати в реальних умовах підприємства отримані теоретичні та практичні знання з спеціальності;
- придбання студентами навичок експлуатації інформаційних систем, а також суспільної і організаційної роботи в колективі;
- формувати у студентів практичні навички в роботі з програмним та апаратним забезпеченням, комп'ютерними системами та мережами, базами даних на знань на підприємстві та забезпечення їх безпеки;
- оволодіння студентами 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 студентами на практиці структури інформаційно-аналітичної діяльності та загальнонаукових і спеціальних методів, що застосовуються в управлінні захистом інформації;
- розвинути у студентів професійне вміння приймати самостійні рішення під час виконання конкретної роботи та ін.

До початку практики студент повинен мати базові знання з наступних дисциплін:

1. Архітектура комп'ютерних систем.
2. Операційні системи.
3. Комп'ютерні системи та мережі.
4. Бази даних і знань.
5. Технології програмування.
6. Основи технічного захисту інформації.
7. Основи криптографічного захисту інформації.
8. Безпека інформації в інформаційно-комунікаційних системах.
9. Менеджмент інформаційної безпеки та ін.

Після проходження виробничої практики студент повинен уміти:

1. Вивчати характеристики об'єкту управління і розробляти схему організаційної структури управління об'єктом (підприємством, установою, організацією, що є базою практики);

2. Обстежувати підприємство, вивчати його інформаційну діяльность, визначати об`єкти захисту – інформацію з обмеженим доступом, виявляти загрози, аналізувати їх та будувати моделі загроз.

3. Розробляти рекомендації щодо впровадження комплексної системи захисту інформації на підприємстві;

4. Розробляти рекомендації щодо реалізації організаційних заходів захисту інформації на підприємстві;

5. Розробляти рекомендації щодо реалізації первинних технічних заходів захисту інформації на підприємстві

6. Розробляти рекомендації щодо реалізації основних технічних заходів захисту інформації на підприємстві

7. Формулювати висновки, що розкривають переваги і недоліки в системі захисту АІС, що функціонує на об'єкті управління;

8. Розробляти вимоги до захисту проектованої підсистеми АІС по схемі "як є – як повинно бути";

9. Працювати зі спеціалізованим програмним забезпечення для захисту інформації та ін.

2 ОРГАНІЗАЦІЯ ТЕХНОЛОГІЧНОЇ ПРАКТИКИ

Організація та керівництво технологічною практикою здійснюється відповідно до «Положення про практику», затвердженого ректором ЧДТУ 15.05.2013 року №67. Загальну організацію виробничої практики і контроль за її проведенням в університеті здійснює відділ практики та сприяння працевлаштуванню та кафедра кібербезпеки та математичного моделювання.

Безпосередньо організацію виробничої практики здійснює керівник виробничої практики (співробітник відділу практики та сприяння працевлаштуванню) та керівник практики від кафедри кібербезпеки та математичного моделювання. До керівництва практикою залучаються досвідчені викладачі кафедри.

2.1 Обов’язки керівника практики від ЧНТУ

- контроль підготовленості бази практики та вжиття, за необхідності, потрібних заходів щодо її підготовки;

- ознайомлення керівника від бази практики з програмою виробничої практики та узгодження плану-графіку проходження практики;

- проведення організаційних зборів зі студентами, ознайомлення студентів з програмою практики, охороною праці під особистий підпис, особливостями проходження практики на підприємстві, формою звіту про результати практики;

- надання студентам-практикантам необхідних документів (направлення, програми, щоденника та ін.), перелік яких встановлюється у наскрізній програмі про проведення практики студентів за напрямом підготовки 6.170103 «Управління інформаційною безпекою» та спеціальністю 125 «Кібербезпека»;

- представлення студентів та керівника практики від бази практики і участь у проведенні інструктажу з правил техніки безпеки, протипожежної безпеки та виробничої санітарії на виробництві;

- забезпечення разом з керівником від бази практики виконання програми практики;

- надання студентам допомоги в доборі матеріалу для виконання індивідуального завдання і контроль за його виконанням;

- контроль проходження практики студентами та надання необхідних консультацій з питань проходження практики;

- визначення часу і місця підведення підсумків роботи студентів та виставлення підсумкової оцінки за результатами практики;

- перевірка звітної документації і оцінка результатів виконання програми практики;

- приймання захисту практики;

2.2 Обов'язки студентів при проходженні практики

- до початку 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 програмою практики і вказівками її керівників;

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

- нести відповідальність за виконану роботу;

- вести записи у своїх щоденниках про характер виконуваної роботи;

- своєчасно подати необхідні звітні документи та захистити результати практики.

Студент, котрий не виконав програму практики, а також в разі отримання «не зараховано» при захисті звіту про проходження практики, відраховується з університету на загальних підставах.

3 ЗМІСТ ПРАКТИКИ

Зміст виробничої практики визначається вимогами освітньо-кваліфікаційної характеристики та освітньо-професійної програми підготовки

бакалаврів за напрямом (спеціальністю) 6.170103 «Управління інформаційною безпекою».

Практиканти виконують завдання з кожної теми, використовуючи знання набуті під час підготовки за спеціальність, формують практичні навички щодо порядку проведення робіт з технічного захисту інформації відповідно до державних стандартів України.

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

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 первинних технічних заходів захисту інформації на підприємстві
6.	Розробка рекомендацій щодо реалізація основних технічних заходів захисту інформації на підприємстві
7.	Підведення підсумків. Узагальнення матеріалів з практики, оформлення звіту, складання диференційного заліку
	Разом:

3.2 Методичні рекомендації

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

Практиканти повинні ознайомитися з програмою практики, її основними тематичними розділами. Отримати 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;

Керівник установи призначає студенту 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 студент 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 та побудова окремої моделі загроз.

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 студенти складають акт в довільній формі, який додають до звіту про проходження практики.

Матеріали обстеження використовуються під час розроблення окремої моделі загроз, яка повинна включати:

- генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення інформаційної діяльності, а також інженерних комунікацій, які виходять за межі контрольованої території;

- схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкціонованого доступу до інформації з обмеженим доступом;

- оцінку шкоди, яка передбачається від реалізації загроз.

Модель загроз для підприємства включається до звіту про проходження практики.

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

На підставі матеріалів обстеження та окремої моделі загроз студенти повинні визначити головні задачі захисту інформації і скласти технічне завдання на розроблення системи захисту інформації на підприємстві. Технічне завдання повинно включати основні розділи:

- вимоги до системи захисту інформації;

- вимоги до складу проектної та експлуатаційної документації;

- етапи виконання робіт;

- порядок внесення змін і доповнень до розділів ТЗ;

- вимоги до порядку проведення випробування системи захисту.

Технічне завдання на розроблення системи захисту інформації на підприємстві додається до звіту про проходження практики.

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.

Студентам 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;
- розробити правила реалізації заходів технічного 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;
- установити порядок контролю функціонування системи захисту інформації та її якісних характеристик;
- визначити зони безпеки інформації;

Оперативне вирішення задач технічного захисту інформації досягається організацією керування системою захисту інформації, для чого практиканти повинні:

- вивчити й проаналізувати технологію проходження інформації з обмеженим доступом у процесі інформаційної діяльності;
- оцінити схильність інформації з обмеженим доступом до впливу загроз у конкретний момент часу;

- оцінити очікувану ефективність застосування засобів забезпечення технічного захисту інформації;

- визначати (за необхідності) додаткову потребу в засобах забезпечення технічного захисту інформації;

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

5. Розробка рекомендацій щодо реалізації первинних 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).

6. Розробка рекомендацій щодо реалізація основних технічних заходів захисту інформації на підприємстві

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.

Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) інформації з обмеженим доступом про витік інформації чи порушення її цілісності.

Засоби технічного захисту інформації застосовуються автономно або спільно з технічними засобами забезпечення інформаційної діяльності для пасивного або активного приховування інформації з обмеженим доступом.

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.

Програмні засоби застосовуються для забезпечення:

- ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

- розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем;

- цілісності інформації та конфігурації автоматизованих систем;

- реєстрації та обліку дій користувачів;

- маскування оброблюваної інформації;

- реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

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

Практиканти закінчують виконання індивідуальних завдань практики. Оформлюють та підписують звітну документацію (щоденник практики, звіт про проходження практики, звіт про виконання індивідуального науково-дослідного завдання, додатки, відгук керівника практики від підприємства, характеристика, тощо.)

3.3 Індивідуальні завдання

Перед початком проходження виробничої практики студенти 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 студентами під час практики умінь та навичок

самостійного розв'язання завдань, пов’язаних з використанням комп’ютерної техніки в своїй роботі, активізації діяльності студентів, 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.

Індивідуальні завдання розробляються викладачами кафедри кібербезпеки та математичного моделювання факультету життєдіяльності, природокористування та туризму та затверджуються на засіданні цієї кафедри.

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

4 ФОРМИ І МЕТОДИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ СТУДЕНТІВ

Поточний контроль проводиться у вигляді оцінювання виконаного студентом практичного завдання по кожній з тем та захисту студентом кожної теми практики окремо та звіту в цілому. Поточний контроль здійснюється керівником практики від бази практики, з залученням у разі необхідності керівника практики від кафедри.

Підсумковий контроль проводиться керівником практики від кафедри у вигляді захисту практики студентом.

5 ПІДБИТТЯ ПІДСУМКІВ ПРАКТИКИ

Після закінчення строку проходження практики студенти у письмовому вигляді звітують про виконання плану та індивідуального завдання практики. Загальна і характерна форма звітності студента за практику – це подання письмового звіту, підписаного і оціненого безпосередньо керівником від бази практики, а також керівником практики від кафедри.

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

Додатки 1-6 містять зразки договору, повідомлення, листа-направлення на практику та зразки звітних документів: щоденник, титульну сторінку звіту, графік відвідування баз практики відповідальними особами тощо.

У звіті мають бути відомості про виконання студентом 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 робочою програмою практики.

Типова форма щоденника, титульний аркуш та остання сторінка звіту представлені в додатках № 4-6.

Студенти звітують про проходження практики перед комісією, призначеною завідуючим кафедрою, до складу якої входять керівники практики від кафедри. Комісія приймає звіт у студентів на базах практики в останні дні її проходження або в університеті протягом перших трьох днів після закінчення практики. Оцінка за практику вноситься до заліково-екзаменаційної відомості і індивідуального навчального плану студента за підписами членів комісії.

Оцінювання результатів практики здійснюється за національною шкалою та шкалою ECTS. Залікові відомості з практик, що проводяться влітку, викладач підписує та здає особисто в деканат протягом перших трьох днів після закінчення практики.

Оцінка з практики, що проводиться влітку, враховується при нарахуванні

стипендії за результатами літнього семестрового контролю.

Студенту, який не приступив до практики своєчасно з поважних причин призначається проходження практики в інший період (відповідно до індивідуального графіку).

У разі отримання незадовільної оцінки за проходження практики, перескладання допускається не більше двох разів. При повторному перескладанні диференційований залік у студента може приймати комісія, яка створюється деканом. Оцінка комісії є остаточною. Студент, який отримав незадовільну оцінку після другого перескладання, вважається таким, що не виконав навчальний план та може бути відрахований з Університету.

Підсумки проведення кожної практики обговорюються на засіданнях кафедр щорічно.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Андреев В.І. Стратегія управління інформаційною безпекою: підручник / В.І.Андреев, В.Д.Козюра, Л.М.Скачек, В.О.Хорошко. – К.: Вид. ДУІКТ, 2007. – 277 с.
2. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 544 с.
3. Блавацька Н.М. Програмне забезпечення систем захисту інформації: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.
4. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие для студентов высших учебных заведений / Г.А.Бузов, С.В.Калинин, А.В.Кондратьев. – М.: «Горячая линия – Телеком», 2005. – 416 с.
5. Гайворонський М.В. Безпека інформаційно-комунікаційних систем. - К.: Видавнича група BHV, 2009. - 608 с.

6. Галатенко В.А. Стандарты информационной безопасности: курс лекций: учебное пособие. Второе издание / В.А.Галатенко; под ред. академика РАН В.Б.Бетелина. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. – 264 с.
7. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений / В.Г.Грибунин, В.В.Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
8. Гришина Н.В. Организация комплексной системы защиты информации / Н.В.Гришина. – М.: Гелиос АРВ, 2007. – 256 с.
9. Довгань О.Д. Методологія захисту інформації: навч.-метод. посіб. / О.Д.Довгань, Г.М.Гулак, А.К.Гринь, С.В.Мельник. – К.: Наук.-вид. центр НА СБ України, 2012. – 184 с.
10. Емельянова Н.З. Защита информации в персональном компьютере: учебное пособие / Н.З.Емельянова, Т.Л.Партыка, И.И.Попов. – М.: ФОРУМ, 2009. – 368 с.
11. Железняк В.К. Защита информации от утечки по техническим каналам: учебное пособие / В.К.Железняк. – СПб.: ГУАП., 2006. – 188 с.
12. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие / В.И.Завгородний. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001. – 264 с.
13. Зайцев А.П. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Изд. 2-е испр. и доп. / А.П.Зайцев, И.В.Голубятников, Р.В.Мещеряков, А.А.Шелупанов. – М.: Машиностроение-1, 2006. − 260 с.
14. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П.Зайцева, А.А.Шелупанов, Р.В.Мещеряков и др.; под ред. А.П.Зайцева и А.А.Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

15. Коженевский С.Р. Термінологічний довідник з питань технічного захисту інформації / С.Р.Коженевский, Г.В.Кузнецов, В.О.Хорошко, Д.В.Чирков; за ред. проф. В.О.Хорошка. – К.: Вид. ДУІКТ, 2007. – 365 с.
16. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф.Конахович, В.П.Климчук, С.М.Паук, В.Г.Потапов. – К.: «МК-Пресс», 2005. – 288 с.
17. Конеев И.Р. Информационная безопасность предприятия / И.Р.Конеев, А.В.Беляев. – СПб.: БХВ-Петербург, 2003. – 752 с.
18. Кормич Б.А. Інформаційна безпека: організаційно-правові основи К.: Кондор, 2004. - 384 с.
19. Кубрак А.І. Комп'ютерне моделювання та ідентифікація автоматичних систем : навч. посібник К. : Політехніка, 2004
20. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш.учеб. заведений / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. – М.: Изд. центр «Академия», 2006. – 256 с.
21. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений / В.П.Мельников, С.А.Клейменов, А.М.Петраков; под. ред. С.А.Клейменова. – 3-е изд., стер. – М.: Изд. центр «Академия», 2008. – 336 с.
22. Организация и современные методы защиты информации / под общ. ред. С.А.Диева, А.Г.Шаваева. – М.: Концерн «Банковский Деловой Центр», 1998. – 472 с.
23. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие для студентов высших учебных заведений / А.А.Торокин. – М.: «Гелиос АРВ», 2005. – 960 с.
24. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф.Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
25. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов, 2 -е изд. / В.И.Ярочкин. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

НОРМАТИВНІ ДОКУМЕНТИ

1. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
2. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
5. НД ТЗІ 1.5-002-2012 Класифікатор засобів технічного захисту інформації.
6. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
7. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
8. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”, затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215
9. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.
10. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
11. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною № 1).

12. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”.
13. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
14. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
15. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
16. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
17. НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.
18. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.
19. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
20. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
21. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1).
22. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ДОДАТКИ

Додаток 1.

Договір
на проведення практики студентів
Чернігівського національного технологічного університету
№ ___

м. Чернігів ***“___” _____ 201__ р.***

Чернігівський національний технологічний університет (надалі - навчальний заклад), в особі ректора Шкарлета Сергія Миколайовича , який діє на підставі статуту, з однієї сторони і _____ (надалі – база практики) в особі_____ _____, який діє на підставі _____ _____ з другої сторони, уклали цей договір на проведення практики студентів Чернігівського національного технологічного університету (надалі - Договір), разом іменовані – Сторони, а кожна окремо – Сторона, про наступне:

І. ПРЕДМЕТ ДОГОВОРУ

1. Забезпечення на умовах взаємовигідного співробітництва Сторін організації проходження практики студентами університету відповідно до умов цього Договору.

ІІ. ОБОВ’ЯЗКИ І ВІДПОВІДАЛЬНІСТЬ СТОРІН

2. База практики зобов’язується:

2.1. Належним чином виконувати умови цього Договору.

2.2. Відмовляти в організації проходження практики тим студентам, відповідно до яких не виконуються умови п. 3 р.2 Договору.

2.3. Коригувати чисельність студентів в залежності від можливостей.

2.4. Прийняти студентів на практику згідно з календарним планом.

2.5. Надіслати до вищого навчального закладу повідомлення встановленого зразка про прибуття на практику студента(ів).

2.6. Призначити наказом кваліфікованих спеціалістів для безпосереднього керівництва практикою.

2.7. Створити необхідні умови для виконання студентами програм практики, не допускати їх використання на посадах та роботах, що не відповідають програмі практики та майбутній спеціальності.

2.8. Забезпечити студентам умови безпечної роботи на кожному робочому місці. Проводити обов’язкові інструктажі з охорони праці, ввідний та на робочому місці. У разі потреби навчати студентів-практикантів безпечним методам праці.

2.9. Надати студентам-практикантам і керівникам практики від навчального закладу можливість користуватись документацією, необхідною для виконання програми практики.

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

2.11. Після закінчення практики дати характеристику на кожного студента-практиканта, у якій відобразити якість підготовленого ним звіту.

3. Вищий навчальний заклад зобов’язується:

3.1. Ознайомити базу практики з програмою практики через студента-практиканта, не пізніше ніж за тиждень – надати базі практики список студентів, які направляються на практику.

3.2. Призначити керівниками практики кваліфікованих викладачів.

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

4. Відповідальність сторін за невиконання угоди

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

4.2. Всі суперечки, що виникають між сторонами за цим Договором вирішуються в установленому порядку.

5. Прикінцеві положення:

5.1. Договір набирає чинності з дня його підписання Сторонами і діє до _____.

5.2. У разі відсутності заяви однієї зі Сторін про припинення або зміну цього Договору після закінчення строку його чинності протягом одного місяця, Договір вважається продовженим на той самий строк і на тих самих умовах.

5.3. Зміни та доповнення до цього Договору можуть бути внесені за взаємною згодою Сторін, що оформляється додатковим договором до цього Договору.

5.4. Договір складений у двох примірниках – по одному для кожної Сторони.

6. Юридичні адреси сторін:

Навчального закладу: 14027, м. Чернігів, вул. Шевченка, 95, Тел.: (04622)31651, Факс: (04622) 3 42 44, E-mail: cstu@stu.cn.ua;

Бази практики:

_____

_____

_____

Підписи та печатки:

Ректор
Чернігівського національного
технологічного університету

_____ проф. С.М. Шкарлет

«____» _____ 20__ р.

М.П.

_____
(посада)

_____

_____ / _____ /
(підпис) (прізвище, ініціали)

«____» _____ 20__ р.

М.П.

Додаток 2. Направлення на практику

КЕРІВНИКУ

_____
_____
_____
_____
_____

НАПРАВЛЕННЯ НА ПРАКТИКУ

/є підставою для зарахування на практику/

Згідно з угодою від „___” _____ 20__ року № ___, яку укладено з

_____
_____

(повне найменування підприємства, організації, установи)

направляємо на практику студентів ____ курсу, які навчаються за напрямом підготовки (спеціальністю) _____
_____

Назва практики _____

Строки практики з „___” _____ 20___ року

по „___” _____ 20 ___ року

Керівник практики від кафедри_____
_____

(посада, прізвище, ім’я, по батькові)

ПРІЗВИЩА, ІМЕНА ТА ПО БАТЬКОВІ СТУДЕНТІВ

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

М.П.

Керівник виробничої практики
Чернігівського національного
технологічного університету _____ _____

(підпис) (прізвище та ініціали)

Додаток 3. Повідомлення про прибуття на практику

ПОВІДОМЛЕННЯ

студент Чернігівського національного технологічного університету

_____

(прізвище, ім'я, по батькові)

_____

(курс, інститут, факультет (відділення), напрям підготовки (спеціальність))

прибув „___" _____ 20___ року до _____

(назва підприємства, організації, установи)

_____

і приступив до практики. Наказом по підприємству (організації, установі) від „__" _____20____ року № _____ студент _____ прийнятий на практику_____

(назва структурного підрозділу)

_____

Керівником практики від підприємства (організації, установи) призначено

_____

(посада, прізвище, ім'я, по батькові)

Керівник підприємства (організації, установи)

_____ _____

(підпис) (посада, прізвище, ім'я, по батькові)

Печатка (підприємства, організації, установи)

"_____"_____ 20___ року

Керівник практики від кафедри Чернігівського національного технологічного університету _____

_____

(назва кафедри)

_____ _____

(підпис) (посада, прізвище, ім'я, по батькові)

"_____"_____20____ року

Додаток 4. Щоденник практики

Чернігівський національний технологічний університет

ЩОДЕННИК ПРАКТИКИ

_____

(вид і назва практики)

студента _____

(прізвище, ім’я, по батькові)

Факультет _____

Кафедра _____

освітньо-кваліфікаційний рівень_____

напрям підготовки _____

спеціальність_____

(назва)

_____ курс, група _____

Студент_____
(прізвище, ім’я, по батькові)

прибув на підприємство, організацію, установу _____
_____

Печатка
підприємства, організації, установи ,,____” _____ 20___ року

_____ _____
(підпис) (посада, прізвище та ініціали відповідальної особи)

Вибув з підприємства, організації, установи _____
_____

Печатка
Підприємства, організації, установи “___” _____ 20___ року

_____ _____
(підпис) (посада, прізвище та ініціали відповідальної особи)

Календарний графік проходження практики

№ з/п	Назви робіт	Тижні проходження практики						Відмітки про виконання
		1	2	3	4	5	6	
1	2	3	4	5	6	7	8	9

Керівники практики від кафедри Чернігівського національного технологічного університету ____________ _________________________

(підпис) (прізвище та ініціали)

від підприємства, організації, установи ______________ __________________________

(підпис) (прізвище та ініціали)

Робочі записи під час практики

Відгук і оцінка роботи студента на практиці

_____

(назва підприємства, організації, установи)

Керівник практики від підприємства, організації, установи _____

_____ _____

(підпис) (прізвище та ініціали)

Печатка

«_____» _____ 20 __ року

Відгук осіб, які перевіряли проходження практики

Висновок керівника практики від кафедри Чернігівського національного технологічного університету про проходження практики

Дата складання заліку „____”_____20____ року

Оцінка:
за національною шкалою_____
(словами)

кількість балів _____
(цифрами і словами)

за шкалою ECTS _____

Керівник практики від кафедри Чернігівського
національного технологічного університету _____ _____
(підпис) (прізвище та ініціали)

Додаток 5. Титульна сторінка звіту про виконання програми навальної (виробничої, технологічної) практики

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ЗВІТ

про виконання програми виробничої практики

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

групи _____

напрям підготовки (спеціальність) _____

спеціалізація _____

кваліфікаційний рівень _____

база практики _____
(повна назва)

Керівник практики
від бази практики

_____
(посада, прізвище, ініціали)

Керівник практики від кафедри

_____
(посада, прізвище, ініціали)

Чернігів - ЧНТУ - 20__

Додаток 6.

Відгук і зауваження керівника практики

_____

(текст відгуку)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник практики від підприємства,
установи організації: _____

_____

(посада)

_____ _____

(підпис) (П.І.П.)