Міністерство освіти і науки України
Вінницький національний технічний університет

ЗАТВЕРДЖУЮ
Ректор Вінницького національного технічного університету
_____ В. В. Грабко
(підпис)
«29» 01 2018 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

за спеціальністю 125 – Кібербезпека
І (бакалаврський) рівень вищої освіти

Назва освітньо-професійної програми «Управління інформаційною безпекою»

(освітньо-професійна програма затверджена Вченою радою
Вінницького національного технічного університету
25.01.2018 протокол № 6)

Галузь науки – 12 «Інформаційні технології»
спеціальність – Кібербезпека
Кваліфікація 3439 «фахівець із організації інформаційної безпеки»
Термін навчання – 3 роки 10 місяців
Форма навчання – денна та заочна

Освітньо-професійна програма «Управління інформаційною безпекою» підготовки бакалаврів

Галузь науки – 12 «Інформаційні технології»

Спеціальність 125 Кібербезпека

2018. — 9 с.

Розробники: Яремчук Ю.Є. , професор, д.т.н., професор

Карпінець В.В., доцент, к.т.н., доцент

Освітньо-професійна програма затверджена на засіданні кафедри менеджменту та безпеки інформаційних систем

Протокол від «26» грудня 2017 року № 8

Голова секції УБ _____ (проф. Яремчук Ю.Є.)

(підпис) (прізвище та ініціали)

Схвалено Методичною комісією Факультету менеджменту та інформаційної безпеки

Протокол від «12» січня 2018 року № 5

Голова Методичної комісії ФМІБ _____ (проф. Небава М.І.)

(підпис) (прізвище та ініціали)

Схвалено Вченою радою Факультету менеджменту та інформаційної безпеки

Протокол від «15» січня 2018 року № 5

Голова _____ (проф. Небава М. І.)

(підпис) (прізвище та ініціали)

Схвалено Методичною радою ВНТУ

Протокол від «18» 01 2018 року № 5

Голова _____ (проф. Романюк О. Н.)

(підпис) (прізвище та ініціали)

Васілевський О.М.

Передмова

1. РОЗРОБЛЕНО у Вінницькому національному технічному університеті кафедрою менеджменту та безпеки інформаційних систем (МБІС)

2. ВНЕСЕНО Вінницьким національним технічним університетом

3. ВВЕДЕНО вперше

4. РОЗРОБНИКИ

1. Яремчук Юрій Євгенович, ВНТУ, д.т.н., професор, професор кафедри менеджменту та безпеки інформаційних систем.

2. Карпінець Василь Васильович, к.т.н., доцент, доцент кафедри менеджменту та безпеки інформаційних систем

Зміст

Вступ

Освітня програма (далі – ОП) «Управління інформаційною безпекою» підготовки бакалаврів за спеціальністю 125 «Кібербезпека» розроблена з врахуванням пропозицій Науково-методичної ради Міністерства освіти і науки України, галузевих об'єднань роботодавців.

1 Загальна характеристика

Рівень вищої освіти – Перший (бакалаврський).

Ступінь вищої освіти – Бакалавр.

Галузь знань – Інформаційні технології, шифр галузі 12.

Спеціальність – Кібербезпека, код спеціальності 125.

Термін навчання – 3 роки 10 місяців

Форма навчання – Денна та заочна.

Освітня кваліфікація – 3439 «фахівець із організації інформаційної безпеки»

Кваліфікація в дипломі – 3439 «фахівець із організації інформаційної безпеки».

Опис предметної області.

Об'єктами вивчення та діяльності бакалавра з управління інформаційною безпекою є:

–об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;

–технології забезпечення безпеки інформації;

–процеси управління інформаційною безпекою об'єктів, що підлягають захисту.

Метою навчання та діяльності є: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки , розв'язувати нестандартні завдання, приймати оптимальні рішення в нетипових умовах, генерувати оригінальні й ефективні для суспільства ідеї, креативно мислити та діяти.

Академічні права випускників: можливість продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістра.

Працевлаштування випускників:

Фахівець з організації інформаційної безпеки може займати первинні посади:

Фахівець з організації захисту інформації з обмеженим доступом;

Фахівець з режиму секретності;

Інспектор з організації захисту секретної інформації;.

2 Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Обсяг освітньо-професійної програми підготовки бакалавра становить 240 кредитів ЄКТС.

3 Перелік компетентностей випускника

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні задачі у галузі управління та адміністрування інформаційною безпекою, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	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.
Фахові компетентності	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 безпеки.
	КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної безпеки.
	КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної безпеки.
	КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

	КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку
	КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.
	КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
	КФ 11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної безпеки.

4 Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

Результати навчання за загальними компетентностями:

• знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;

• принципів забезпечення та супроводу систем та комплексів інформаційної безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики безпеки;

• теорії та процедури розподілу прав управління доступом, моделей та принципів управління доступом до інформаційних ресурсів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної безпеки;

• процесів функціонування системи управління інформаційною безпекою та основ теорії ризиків;

• методів та засобів виявлення та ідентифікації вразливостей і загроз інформаційній безпеці на об’єктах інформаційної діяльності;

• методів та засобів оцінювання та забезпечення відповідного рівня захищеності інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

• методів та засобів технічного та криптографічного захисту інформації із забезпечення інформаційної безпеки.

Результати навчання за фаховими компетентностями:

Фахові компетентності	Результати навчання
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 безпеки.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; -розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; -виконувати аналіз реалізації прийнятої політики інформаційної безпеки.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; -застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; -здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної безпеки в інформаційно-телекомунікаційних системах.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах	-забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної безпеки.	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); - вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної безпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог

	нормативних документів системи технічного захисту інформації; -вирішувати задачі захисту потоків даних в інформаційних,інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	-вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; -вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів. -створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;
КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; -здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації

	в інформаційних та інформаційно-телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки ; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; -забезпечувати функціонування системи управління інформаційною безпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

	- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; – обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; – впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
КФ 11. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної безпеки.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

5 Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється екзаменаційною комісією відповідно до вимог цього стандарту після виконання студентом навчального плану. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом. Термін проведення атестації визначається навчальним планом та графіком навчального процесу. Атестація здійснюється у формі публічного захисту кваліфікаційного проекту / роботи (та за рішенням ВНЗ кваліфікаційного екзамену) До атестації допускаються студенти, які виконали всі вимоги програми підготовки. Результати атестації визначаються оцінками за національною шкалою.
Вимоги до кваліфікаційної	Кваліфікаційний проект / робота має передбачати розв'язання спеціалізованої задачі в галузі

роботи/проекту	інформаційної та/або кібербезпеки. Кваліфікаційний проект/ робота має бути перевірений на плагіат.
Вимоги до кваліфікаційного екзамену	Кваліфікаційний екзамен має передбачати оцінювання сукупності знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом (*за рішенням ВНЗ)

6 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У ВНЗ функціонує система забезпечення якості освітньої діяльності (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;

9) інших процедур і заходів.

7 Перелік нормативних документів, на яких базується стандарт вищої освіти

1. Закон України «Про вищу освіту» 01.07.2014 №1556-VII - Режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18.
2. «Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року № 47/2017.
3. Постанова Кабінету Міністрів № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р.
4. Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 року, уведеного в дію Указом Президента України від 15 березня 2016 року № 96).

5. «Біла книга Держспецзв'язку». Електронний ресурс. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941.

6. Методичні рекомендації щодо розроблення стандартів вищої освіти / Схвалено сектором вищої освіти Науково-методичної Ради Міністерства освіти і науки України протокол № 3 від 29.03.2016.

7. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0–96. – К. : Держстандарт України, 1996. – 20 с.

8. Захист інформації. Технічний захист інформації. Порядок проведення робіт : ДСТУ 3396.1–96. – К. : Держстандарт України, 1997. – 32 с.

9. Постанова Кабінету Міністрів №1187 «Про затвердження ліцензійних умов провадження освітньої діяльності закладів освіти» від 30.12.2015 р.

10. Наказ МОН України №166 «Деякі питання оприлюднення інформації про діяльність вищих навчальних закладів» від 19.02.2015 р.

11. Наказ МОН України №1151 «Про особливості запровадження переліку галузей знань, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України № 266 від 29.04. 2015 р.» від 06.11.2015 р.

12. Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // Видавництво "Соцінформ". - К.: 2010

13. Наказ Міністерства економічного розвитку і торгівлі України від 18.11. 2014 р. № 1361 «Про затвердження зміни до національного класифікатора України ДК 003:2010» (зміна № 2)

14. Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд, Національна академія педагогічних наук України, Інститут вищої освіти НАПН України, Режим доступу: http://ihed.org.ua/images/biblioteka/Rozvitok_sisitemi_zabesp_yakosti_VO_UA_2015.pdf