

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ



ЗАТВЕРДЖЕНО

Ректор ВНТУ

Віктор БІЛІЧЕНКО

Наказ ВНТУ № 20 від «26» 01 2023 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Управління інформаційною безпекою

Information Security Management

Рівень вищої освіти	перший (бакалаврський)
Спеціальність	125 Кібербезпека та захист інформації
Галузь знань	12 Інформаційні технології
Освітня кваліфікація	бакалавр з кібербезпеки

Розглянуто та схвалено  
на засіданні Вченої Ради ВНТУ  
Протокол № 6 від  
«26» 01 2023 р.

Вінниця, 2023

## ЛИСТ ПОГОДЖЕННЯ

### ОПП Управління інформаційною безпекою

Рівень вищої освіти перший (бакалаврський)

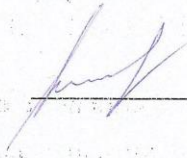
Спеціальність 125 Кібербезпека та захист інформації

Гарант ОПП  
д.ф., ст.викл. каф. МБІС



Ольга САЛІЄВА

Директор Центру  
забезпечення якості освіти  
ВНТУ



Олеся ВОЙТОВИЧ

Освітньо-професійну програму розглянуто та схвалено на засіданні кафедри менеджменту та безпеки інформаційних систем; протокол № 8 від 17 грудня 2022 р.

Завідувач кафедри



Василь КАРПНЕЦЬ

ОПП розглянуто після надходження всіх зауважень та пропозицій та схвалено на:

засіданні Вченої ради факультету менеджменту та інформаційної безпеки; протокол № 5 від 18 січня 2023 р.

Голова



Ірина ЄПФАНОВА

засіданні Методичної ради ВНТУ,  
протокол № 6 від 19 січня 2023 р.

Голова



Олександр ПЕТРОВ

## ПРЕАМБУЛА

**ОПП Управління інформаційною безпекою**  
Рівень вищої освіти перший (бакалаврський)  
Спеціальність 125 Кібербезпека та захист інформації  
Розроблена на основі стандарту вищої освіти (наказ № 1074 від «04» жовтня 2018 р.)

## РОЗРОБНИКИ

Гарант ОПП, к.т.н., доц. кафедри ВМ	Ольга САЛІЄВА
Завідувач кафедри МБІС, к.т.н., доцент	Василь КАРПНЕЦЬ
Голова секції УБ кафедри МБІС, д.т.н., проф.	Юрій ЯРЕМЧУК

Освітньо-професійну програму розглянуто та схвалено на засіданні Студентської ради факультету менеджменту та інформаційної безпеки;

протокол № 1 від 05 січня 2023 р.

Голова



Мирослава ГІРНИК

## РЕЦЕНЗІЇ-ВІДГУКИ РОБОТОДАВЦІВ

На освітньо-професійну програму надіслали рецензії та відгуки:

Грималовський Микола Миколайович, начальник 3-го відділу Управління Державної служби спеціального зв'язку та захисту інформації у Вінницькій області

Прокоф'єв Михайло Іванович, доктор технічних наук, директор Науково-дослідного центру систем технічного захисту інформації "ТЕЗІС" НТУУ «КПІ ім. Ігоря Сікорського», віце-президент Асоціації захисників інформації "АЗІС", Заслужений працівник освіти України .

Волинець Олександр Юрійович, керівник проєктів в ІТ компанії Morebis, випускник кафедри менеджменту та безпеки інформаційних систем ВНТУ за спеціальністю "Управління інформаційною безпекою"

Безпалый Кирило Валерійович, старший інженер розробник в ІТ компанії Exadel, випускник кафедри менеджменту та безпеки інформаційних систем ВНТУ за спеціальністю "Управління інформаційною безпекою"

## Зміст

Вступ.....	5
1. Профіль освітньо-професійної програми.....	5
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність.....	17
3. Форми атестації здобувачів вищої освіти.....	20
4. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти.....	20
5. Перелік нормативних документів, на яких базується освітня програма.....	21
Пояснювальна записка.....	22
Додаток А. Матриці відповідності.....	23
Додаток Б. Зведена таблиця фахових компетентностей та результатів навчання.....	28
Листок реєстрації змін.....	32

## Вступ

Освітньо-професійна програма (далі – ОПП) підготовки бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації» розроблена із врахуванням стандарту вищої освіти (наказ № 1074 від «04» жовтня 2018 р.).

### 1 Профіль освітньо-професійної програми

<b>1 – Загальна інформація</b>	
<b>Повна назва вищого навчального закладу та структурного підрозділу</b>	Вінницький національний технічний університет, кафедра менеджменту та безпеки інформаційних систем
<b>Ступінь вищої освіти та назва кваліфікації мовою оригіналу</b>	Бакалавр Бакалавр з кібербезпеки
<b>Офіційна назва освітньої програми</b>	Управління інформаційною безпекою
<b>Тип диплому та обсяг освітньої програми</b>	Диплом бакалавра, одиничний На базі ПСЗО - 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців. На базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») перезараховується не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста), термін навчання – 1 рік 10 місяців.
<b>Кваліфікація в дипломі</b>	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Управління інформаційною безпекою
<b>Цикл/рівень</b>	6 рівень НРК України, перший цикл FQ-EHEA, 6 рівень EQF-LLL
<b>Передумови</b>	Повна загальна середня освіта або освітньо-кваліфікаційний рівень «молодший спеціаліст» (ступінь «молодший бакалавр»)
<b>Мова (и) викладання</b>	Українська
<b>Інтернет-адреса постійного розміщення опису освітньої програми</b>	<a href="https://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html">https://vntu.edu.ua/uk/information-for-enrollee/progmagbak.html</a>
<b>2 – Мета освітньої програми</b>	
Формування творчої особистості нового покоління, здатної успішно реалізовувати набуті сучасні професійні компетентності з управління інформаційної безпеки, інтелектуальний потенціал, навички практичного досвіду та інноваційної діяльності в галузі кібербезпеки та захисту інформації, а також соціально-патріотичні та морально-етичні цінності у глобальному суспільно-економічному просторі <sup>1</sup> .	

### 3 – Характеристика освітньої програми

<p><b>Предметна область (галузь знань, спеціальність, спеціалізація)</b></p>	<p>Галузь знань – 12 «Інформаційні технології» Спеціальність – 125 «Кібербезпека та захист інформації»</p>
<p><b>Об’єкти професійної діяльності випускників</b></p>	<ul style="list-style-type: none"> <li>– об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;</li> <li>– технології забезпечення безпеки інформації;</li> <li>– процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту</li> </ul>
<p><b>Цілі навчання</b></p>	<p>підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки</p>
<p><b>Теоретичний зміст предметної області. Знання</b></p>	<ul style="list-style-type: none"> <li>– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;</li> <li>– принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;</li> <li>– теорії, моделей та принципів управління доступом до інформаційних ресурсів;</li> <li>– теорії систем управління інформаційною та/або кібербезпекою;</li> <li>– методів та засобів виявлення, управління та ідентифікації ризиків;</li> <li>– методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;</li> <li>– методів та засобів технічного та криптографічного захисту інформації;</li> <li>– сучасних інформаційно-комунікаційних технологій;</li> <li>– сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій;</li> <li>– автоматизованих систем проектування.</li> </ul>

<b>Орієнтація освітньої програми</b>	Освітньо-професійна програма орієнтована на принципи супроводу систем та комплексів кібербезпеки; теорії, моделі та принципи управління доступом до інформаційних ресурсів; методи та засоби виявлення, управління та ідентифікації ризиків; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації; методи та засоби технічного та криптографічного захисту інформації; сучасні інформаційно-комунікаційні технології; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
<b>Методи, методики та технології</b>	Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення кібербезпеки інформаційних систем.
<b>Інструменти та обладнання</b>	Системи розробки, забезпечення, моніторингу та контролю процесів інформаційної безпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
<b>Основний фокус освітньої програми та спеціалізації</b>	Загальна освіта зі спеціальності кібербезпеки. Акцент робиться на формуванні та розвитку професійних компетентностей спрямованих на розв'язання складних спеціалізованих задач та практичних проблем у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповнотою визначеність умов.
<b>Особливості програми</b>	Формування відповідних компетентностей в умовах нестабільності інформаційного середовища на основі принципів інноваційного розвитку та сучасних інформаційних технологій.
<b>4 – Придатність випускників до працевлаштування та подальшого навчання</b>	
<b>Придатність до працевлаштування</b>	Фахівець із організації інформаційної безпеки може займати такі первинні посади:

	<ul style="list-style-type: none"> <li>– адміністратор інформаційної безпеки;</li> <li>– аудитор/пентестер безпеки інформаційно-комунікаційних систем;</li> <li>– розробник засобів захисту інформації;</li> <li>– провідний спеціаліст/керівник служби технічного захисту інформації;</li> <li>– фахівець з розроблення комп'ютерних програм;</li> <li>– технік із конфігурованої комп'ютерної системи;</li> <li>– фахівець з організації захисту інформації з обмеженим доступом;</li> <li>– фахівець з режиму секретності;</li> <li>– інспектор з організації захисту секретної інформації;</li> <li>– технік обчислювального (інформаційно-обчислювального) центру;</li> <li>– технік із системного адміністрування;</li> <li>– технік-програміст;</li> <li>– фахівець з інформаційних технологій;</li> <li>– фахівець з комп'ютерної графіки (дизайну);</li> <li>– фахівець з розробки та тестування програмного забезпечення.</li> </ul> <p>Права випускників на працевлаштування не обмежуються.</p>
<b>Подальше навчання</b>	Можливість продовжити навчання на другому (магістерському) рівні вищої освіти.
<b>5 – Викладання та оцінювання</b>	
<b>Викладання та навчання</b>	Лекції, практичні заняття, виконання курсових робіт, дослідницькі лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації із викладачами, наукові семінари, демонстраційні класи, елементи дистанційного (онлайн, електронного) навчання проходження практики на підприємствах та в науково-дослідних установах, підготовка кваліфікаційної роботи.
<b>Оцінювання</b>	Методи оцінювання – екзамени, тести, практика, контрольні, курсові роботи, есе, презентації. Формативні (вхідне тестування та поточний контроль): тестування знань або умінь; усні презентації; звіти про лабораторні роботи; аналіз текстів або даних; звіти про практику; огляд літератури тощо). Сумативні (підсумковий контроль): екзамен

	(письмовий з подальшим усним опитуванням); залік (за результатами формативного контролю).
<b>6 – Програмні компетентності</b>	
<b>Інтегральна компетентність</b>	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
<b>Загальні компетентності (ЗК)</b>	<p>ЗК 1. Здатність застосовувати знання у практичних ситуаціях.</p> <p>ЗК 2. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.</p> <p>ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.</p> <p>ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>
<b>Спеціальні (фахові) компетентності (СК)</b>	<p>СК 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.</p> <p>СК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.</p> <p>СК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів</p>

захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

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

СК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та пошкодження.

СК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

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

СК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

СК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

СК 13. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки.

СК 14. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою.

## 7 – Програмні результати навчання

РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

РН 2. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 5. Адаптуватися в умовах частоті зміни технологій професійної діяльності, прогнозувати кінцевий результат.

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

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

РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

РН 12. Розробляти моделі загроз та порушника.

РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється у інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

РН 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.

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

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

РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в

	<p>інформаційних та інформаційно-телекомунікаційних систем (автоматизованих) системах.</p> <p>РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).</p> <p>РН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.</p> <p>РН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.</p> <p>РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.</p> <p>РН 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 та/або кібербезпеки.</p> <p>РН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.</p> <p>РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.</p> <p>РН 31. Застосувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.</p> <p>РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно</p>
--	---

	<p>встановленої політики безпеки.</p> <p>РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.</p> <p>РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.</p> <p>РН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.</p> <p>РН 36. Виявляти небезпечні сигнали технічних засобів.</p> <p>РН 37. Вимірювати параметри небезпечних та заводових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.</p> <p>РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.</p> <p>РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.</p> <p>РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.</p> <p>РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.</p> <p>РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.</p> <p>РН 43. Застосовувати національні та міжнародні</p>
--	---

	<p>регулюючі акти в сфері кібербезпеки для розслідування інцидентів.</p> <p>РН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.</p> <p>РН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.</p> <p>РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.</p> <p>РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.</p> <p>РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.</p> <p>РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах .</p> <p>РН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).</p> <p>РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.</p> <p>РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.</p> <p>РН 53. Вирішувати задачі аналізу програмного коду та наявності можливих загроз.</p> <p>РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в</p>
--	---

	<p>Україні.</p> <p>РН 55. Забезпечити належне застосування алгоритмічних математичних аспектів криптографічного захисту інформації.</p> <p>РН 56. Виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС.</p> <p>РН 57. Проектувати системи для здійснення політики безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем.</p>
<b>8 – Ресурсне забезпечення реалізації програми</b>	
<b>Кадрове забезпечення</b>	Кадрове забезпечення ОПІ формується, в основному за рахунок кафедри менеджменту та безпеки інформаційних систем. До викладання дисциплін залучаються також інші кафедри факультету менеджменту та безпеки інформаційних систем, і університету. Керівник проектної групи освітньої програми та викладацький склад, який забезпечує її реалізацію, відповідають вимогам, визначеним Ліцензійними умовами провадження освітньої діяльності.
<b>Матеріально-технічне забезпечення</b>	Матеріально-технічне забезпечення відповідає вимогам Ліцензійних умов провадження освітньої діяльності, в тому числі включає в себе сучасні лабораторії Центру інформаційних технологій та захисту інформації, зокрема комп'ютерні класи мережевої академії Cisco та ІТ Академії Microsoft, Науково-дослідну лабораторію технічного захисту інформації.
<b>Інформаційне та навчально-методичне забезпечення</b>	Відповідно до вимог Ліцензійних умов провадження освітньої діяльності включає в себе бібліотечні ресурси, електронні навчальні ресурси, сайт ВНТУ та сайт кафедри, на яких розміщена основна інформація щодо освітньої діяльності за ОП.
<b>9 – Академічна мобільність</b>	
<b>Національна кредитна мобільність</b>	Здійснюється на підставі укладення угод про співробітництво між Університетом та закладами вищої освіти України.
<b>Міжнародна кредитна мобільність</b>	Здійснюється на підставі укладення угод між Університетом та групою закладів вищої освіти різних країн за узгодженими та

	затвердженими у встановленому порядку індивідуальними навчальними планами студентів та програмами навчальних дисциплін, а також в рамках міжурядових угод про співробітництво в галузі освіти, міжнародних проектів, в яких Університет приймає участь, грантів та ін.
<b>Навчання іноземних здобувачів вищої освіти</b>	За даною освітньою програмою передбачено навчання іноземних здобувачів вищої освіти

## 2 Перелік компонент освітньо-професійної програми та їх логічна послідовність

### 2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
<b>ОБОВ'ЯЗКОВІ КОМПОНЕНТИ</b>			
Загальні			
1.1.	Історія та культура України	3,0	залік
1.2.	Філософія	3,0	залік
1.3.	Політологія	3,0	залік
1.4.	Українська мова за професійним спрямуванням	3,0	залік
1.5.	Іноземна мова за професійним спрямуванням	8,0	залік
1.6.	Вища математика	12,0	іспит
1.7.	Фізика	10,0	іспит
Професійні			
1.8.	Основи комп'ютерної техніки	3,0	іспит
1.9.	Інформаційні технології	3,0	залік
1.10.	Internet-технології та кібергігієна	4,0	іспит
1.11.	Теоретичні основи процесів у кібербезпеці	11,0	іспит
1.12.	Схемотехніка	8,0	залік, іспит
1.13.	Математичні основи криптографії	4,0	іспит
1.14.	Спеціальні вимірювання у сфері захисту інформації	3,0	залік
1.15.	Основи наукових досліджень, аналізу та синтезу інформації	4,0	іспит
1.16.	Управління ризиками та оцінювання захищеності інформації	6,0	іспит
1.17.	Інформаційно-телекомунікаційні системи	3,0	іспит
1.18.	Основи технічного захисту інформації	5,0	іспит
1.19.	Економіка, організація та управління бізнес процесами	3,0	залік
1.20.	Управління інцидентами інформаційної безпеки	4,0	іспит
1.21.	Основи інформаційної безпеки (вступ до фаху)	3,0	залік
1.22.	Основи програмування захищених інформаційних систем (в т.ч. курсова робота)	11,0	залік, іспит
1.23.	Програмний захист в системах управління інформаційною безпекою	4,0	іспит
1.24.	Бази даних і знань (в т.ч. курсова робота)	6,0	іспит
1.25.	Основи криптографічного захисту інформації (вт.ч. курсова робота)	8,0	залік, іспит

1.26.	Проектування систем управління інформаційною безпекою (в т.ч. курсовий проект)	10,0	залік, іспит
1.27.	Менеджмент інформаційної безпеки	7,0	залік, іспит
1.28.	Нормативно-розпорядчі засади управління інформаційною безпекою	4,0	іспит
1.29.	Виробнича практика	9,0	залік
1.30.	Переддипломна практика	4,5	залік
1.31.	Бакалаврська кваліфікаційна робота	10,5	
<b>Загальний обсяг обов'язкових компонент</b>		<b>180</b>	
<b>ВИБІРКОВІ КОМПОНЕНТИ ЗА ВІЛЬНИМ ВИБОРОМ СТУДЕНТА</b>			
Загальні			
2.1.	Освітній компонент з гуманітарної та філософської підготовки з БДВВ	3,0	залік
2.2.	Освітній компонент з суспільно-політичної підготовки з БДВВ	3,0	залік
2.3.	Освітній компонент з економічної підготовки з БДВВ	3,0	залік
2.4.	Освітній компонент підготовки з іноземної мови з БДВВ	3,0	залік
Професійні			
2.5.	Освітній компонент 1 з БДВВ	5,0	залік
2.6.	Освітній компонент 2 з БДВВ	5,0	залік
2.7.	Освітній компонент 3 з БДВВ	5,0	залік
2.8.	Освітній компонент 4 з БДВВ	5,0	залік
2.9.	Освітній компонент 5 з БДВВ	5,0	залік
2.10.	Освітній компонент 6 з БДВВ	5,0	залік
2.11.	Освітній компонент 7 з БДВВ	6,0	залік
2.12.	Освітній компонент 8 з БДВВ	5,0	залік
2.13.	Освітній компонент 9 з БДВВ	3,0	залік
2.14.	Освітній компонент 10 з БДВВ	4,0	залік
		<b>60</b>	
<b>ЗАГАЛЬНИЙ ОБСЯГ ЗА ПЛАНОМ</b>		<b>240</b>	

## 2.2. Структурно-логічна схема освітньо-професійної програми

1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр
OK 1	OK 4	OK 2	OK 5	OK 3	OK 18	OK 19	OK 20
OK 5	OK 5	OK 5	OK 11	OK 16	OK 25	OK 26	OK 26
OK 6	OK 6	OK 11	OK 12	OK 17	OK 29	OK 27	OK 27
OK 7	OK 7	OK 12	OK 14	OK 24	BK 3	OK 28	OK 30
OK 8	OK 11	OK 13	OK 15	OK 25	BK 9	BK 4	OK 31
OK 9	OK 21	BK 1	OK 16	BK 7	BK 10	BK 11	BK 4
OK 10	OK 22	BK 5	BK 2	BK 8		BK 12	BK 9
OK 22	OK 23	BK 14	BK 6				
			BK 14				

### **3 Форми атестації здобувачів вищої освіти**

#### **Форми атестації здобувачів вищої освіти**

Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.

До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом та освітньою програмою.

Вимоги до кваліфікаційної роботи/проєкту

Кваліфікаційний проєкт/робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної та/або кібербезпеки.

Кваліфікаційний проєкт/робота має бути перевірений на плагіат.

Кваліфікаційна робота повинна бути опублікована на сайті Вінницького національного технічного університету.

### **4 Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти**

У вищому навчальному закладі функціонує система забезпечення якості освітньої діяльності та якості вищої освіти (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 ефективною системою запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;
- 9) інших процедур і заходів, які забезпечують належний рівень якості вищої освіти.

## **5 Перелік нормативних документів, на яких базується освітня програма**

- Закон України «Про вищу освіту» 01.07.2014 №1556-VII - [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1556-18>];
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Режим доступу: <http://zakon2.rada.gov.ua/laws/show/80/94-вр>];
- Закон України «Про основні засади забезпечення кібербезпеки України» - відомості Верховної Ради (ВВР), 2017, №45, ст.403;
- Постанова Кабінету Міністрів України від 30.12.2015р. №1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» [Режим доступу: <http://zakon4.rada.gov.ua/laws/show/1187-2015-п/page>];
- Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29.04.2015 р.№266. [Режим доступу: <http://zakon.rada.gov.ua/laws/show/266-2015-п>];
- Національний класифікатор України: "Класифікатор професій» ДК 003:2010 [Режим доступу: <http://www.003.com>];
- Наказ МОН України №1074 «Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти» від 04.10.2018 р.;
- «Доктрина інформаційної безпеки України», затверджено Указом Президента України від 25 лютого 2017 року №47/2017. [Режим доступу: <https://www.president.gov.ua/documents/472017-21374>];
- Рішення Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» від 27.01.2016 р., уведеного в дію Указом Президента України від 15.03.2016 р. №96. [Режим доступу: <https://www.president.gov.ua/documents/2422016-20141>];
- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 р. №1229;
- Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 р. №505;
- Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. №373.

### **Пояснювальна записка**

Освітньо-професійна програма містить програмні компетентності, що визначають специфіку підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації» та програмні результати навчання, які виражають те, що студент повинен знати, розуміти та бути здатним виконувати після успішного завершення освітньої програми. В таблицях 1, 2 наведені матриці відповідності визначених освітньою програмою результатів навчання (компетентностей) та освітніх компонентів.

Таблиця 1. Матриця забезпечення програмних результатів навчання обов'язковими освітніми компонентами

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31
PH 1				+	+																								+	+	+
PH 2											+					+				+	+					+			+	+	+
PH 3									+		+				+	+			+		+			+					+	+	+
PH 4		+				+	+				+				+	+		+	+	+	+					+			+	+	+
PH 5						+					+								+							+			+	+	+
PH 6		+				+	+						+								+					+		+	+	+	+
PH 7																		+			+					+		+			
PH 8																											+	+			
PH 9																		+		+							+	+			
PH 10								+				+					+														
PH 11									+	+							+														
PH 12																+				+							+				
PH 13								+	+	+							+														
PH 14																						+	+								
PH 15								+	+			+					+					+		+							
PH 16																	+								+			+			
PH 17												+					+														
PH 18																						+	+								
PH 19													+					+				+			+	+	+				
PH 20																						+	+								
PH 21																										+	+	+			



	OK 1	OK 2	OK 3	OK 4	OK 5	OK 6	OK 7	OK 8	OK 9	OK 10	OK 11	OK 12	OK 13	OK 14	OK 15	OK 16	OK 17	OK 18	OK 19	OK 20	OK 21	OK 22	OK 23	OK 24	OK 25	OK 26	OK 27	OK 28	OK 29	OK 30	OK 31	
PH 41																+					+											
PH 42																						+										
PH 43																					+							+	+			
PH 44																+			+										+			
PH 45																+												+				
PH 46																+	+															
PH 47													+													+						
PH 48													+													+						
PH 49								+										+			+							+				
PH 50																						+	+									
PH 51																		+			+											
PH 52										+								+			+											
PH 53																						+	+									
PH 54	+		+																													
PH 55													+													+						
PH 56																+	+	+														
PH 57																			+								+	+				

**Таблиця 2. Матриця відповідності компетентностей обов'язковим освітнім компонентам**

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	
ЗК1	+			+	+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+		+	+	+	+		
ЗК2						+	+			+	+					+	+	+		+	+	+	+				+	+	+	+		
ЗК3				+	+																								+	+	+	
ЗК4						+	+		+	+	+					+		+		+	+		+		+			+	+	+	+	
ЗК5	+	+				+	+		+	+	+	+			+	+	+	+	+	+		+		+				+	+	+	+	
ЗК6	+	+	+																													
ЗК7	+		+															+					+					+				
СК1											+			+				+		+	+							+				
СК2								+	+	+	+												+				+					
СК3												+					+	+					+			+						
СК4																			+								+					
СК5													+				+	+			+					+		+	+			
СК6								+									+											+				
СК7												+		+				+										+				
СК8																+				+												
СК9																+				+	+							+	+			
СК 10												+	+					+								+						
СК 11								+									+										+					
СК 12															+	+				+	+		+					+				
СК 13																+				+												
СК 14																+				+							+	+	+			

**Таблиця 3. Зведена таблиця фахових компетентностей та результатів навчання**

Фахові компетентності	Результати навчання
<p>СК 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.</p>	<ul style="list-style-type: none"> <li>– готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і/або кібербезпеки;</li> <li>– розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем;</li> <li>– виконувати аналіз реалізації прийнятої політики інформаційної і/або кібербезпеки.</li> </ul>
<p>СК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.</p>	<ul style="list-style-type: none"> <li>– здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій;</li> <li>– розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;</li> <li>– застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;</li> <li>– здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах;</li> <li>– виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і/або кібербезпеки в інформаційно- телекомунікаційних системах.</li> </ul>
<p>СК 3. Здатність до використання програмних та програмно-апаратних комплексів засобу захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.</p>	<ul style="list-style-type: none"> <li>– забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;</li> <li>– забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-</li> </ul>

	<p>телекомунікаційних (автоматизованих) системах;  – виконувати розробку експлуатаційної документації та комплексів засобів захисту.</p>
<p>СК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p>	<p>– вирішувати задачі супроводу ( в т.числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу до 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.</p>
<p>СК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p>	<p>– обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, 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 реалізовувати 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-</p>

	<p>телекомунікаційних (автоматизованих) системах;</p> <ul style="list-style-type: none"> <li>– визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</li> <li>– використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.</li> </ul>
<p>СК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та пошкодження.</p>	<ul style="list-style-type: none"> <li>– вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів;</li> <li>– вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес-процесів після здійснення кібератак, збоїв та відмов різних класів;</li> <li>– створювати і впроваджувати плани процесу забезпечення безперервності бізнесу;</li> <li>– виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.</li> </ul>
<p>СК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін..).</p>	<ul style="list-style-type: none"> <li>– вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</li> <li>– здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах, використовувати інструментальні засоби оцінювання наявності потенційних вразливостей;</li> <li>– вирішувати задачі управління комплексною системою захисту інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</li> <li>– вирішувати задачі експертизи, випробування комплексних систем захисту інформації.</li> </ul>
<p>СК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p>	<ul style="list-style-type: none"> <li>– вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</li> <li>– проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях</li> </ul>

	<p>сфері інформаційної безпеки та/або кібербезпеки;</p> <ul style="list-style-type: none"> <li>– забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації.</li> </ul>
<p>СК 9. Здатність Здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p>	<ul style="list-style-type: none"> <li>– забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів;</li> <li>– забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінювання.</li> </ul>
<p>СК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<ul style="list-style-type: none"> <li>– аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації;</li> <li>– застосовувати алгоритмічні математичні аспекти криптографічного захисту інформації;</li> <li>– аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації;</li> <li>– виявляти небезпечні сигнали технічних засобів;</li> <li>– вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами;</li> <li>– визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;</li> <li>– інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;</li> <li>– обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності;</li> <li>– впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами.</li> </ul>
<p>СК 11. Здатність виконувати моніторинг процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої</p>	<ul style="list-style-type: none"> <li>– забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем;</li> <li>– забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних</li> </ul>

<p>політики інформаційної та/або кібербезпеки.</p>	<p>системах.</p>
<p>СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.</p>	<ul style="list-style-type: none"> <li>– виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</li> <li>– аналізувати ефективність системи виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах;</li> <li>– аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.</li> </ul>

