КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

ЗАТВЕРДЖЕНО
Приймальною комісією
Протокол № 1 від «13» 04 2026 р.
Голова Приймальної комісії
_____ Олександр ТУРУНЦЕВ

ПРОГРАМА

вступного випробування (іспиту) до аспірантури
зі спеціальності F5 Кібербезпека та захист інформації

Рівень вищої освіти: третій (освітньо-науковий)

Галузь знань: F Інформаційні технології

Спеціальність: F5 Кібербезпека та захист інформації

Освітньо-наукова програма: «Інформаційна безпека держави»

На основі: освітнього ступеня магістра
(освітньо-кваліфікаційного рівня спеціаліста)

ПОГОДЖЕНО
Проректор з наукової роботи
та міжнародної діяльності
_____ Наталія ВІННІКОВА

РОЗГЛЯНУТО І ЗАТВЕРДЖЕНО
на засіданні Вченої ради
Факультету інформаційних технологій та математики
Протокол № 3 від «18» березня 2026 р.
Голова Вченої ради
_____ Оксана ЛИТВИН

Київ – 2026

1. Пояснювальна записка

Програма вступного випробування для здобувачів третього (освітньо-наукового) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації складена відповідно до програм підготовки фахівців в галузі знань F Інформаційні технології, відповідає вимогам якісної підготовки та атестації здобувачів відповідного рівня вищої освіти та є нормативним документом Київського столичного університету імені Бориса Грінченка.

Головною метою іспиту є визначення рівня осмислення, усвідомлення вступником основ та головних положень спеціальності, стану готовності до дослідницької діяльності у сфері інформаційної та кібербезпеки й захисту інформації.

Програма включає сукупність питань з інформаційних технологій, які окреслюють основні явища та процеси інформаційної і кібербезпеки та захисту інформації, визначають термінологічне поле науки.

Вступник на іспиті має розкрити основний зміст питань білета та додаткових запитань, продемонструвати:

- знання першоджерел, уміння застосовувати їх зміст та основні ідеї;
- володіння змістом принципів захисту інформації та забезпечення безпеки інформаційно-комунікаційних систем, уміння оперувати ними;
- здатність виявити суть проблеми щодо забезпечення інформаційної/кібернетичної безпеки;
- уміння аргументувати власну позицію щодо вирішення завдань забезпечення інформаційної і кібербезпеки та захисту інформації на об'єктах інформаційної діяльності;
- спроможність до проведення самостійних наукових досліджень в обраній галузі.

Прийом вступного іспиту проводиться відповідно до вимог чинного законодавства, нормативних документів Міністерства освіти та науки України.

2. Методичні рекомендації до проведення вступного випробування

Вступне випробування проводиться у формі іспиту та передбачає відповідь вступника за трьома питаннями обраного білету.

Час підготовки відповіді – 30 хв.

3. Типовий перелік питань вступного випробування

Основні положення

Поняття «національна безпека». Види безпеки: державна, економічна, суспільна, військова, екологічна, інформаційна. Види загроз національній безпеці: загрози інформаційній інфраструктурі, загрози безпеці інформації, загрози духовному життю суспільства, загрози правам і свободам громадян. Інформаційна безпека як складова національної безпеки. Взаємозв'язок інформаційної та інших видів безпеки.

Зовнішні і внутрішні загрози інформаційній безпеці: типи і класи загроз, джерела, особливості реалізації загроз та їхні наслідки.

Базові методи запобігання і ліквідації загроз інформаційній безпеці держави (правові, організаційно-технічні, економічні тощо). Поняття політики безпеки. Принципи побудови політики безпеки та її впровадження.

Визначення та загальні властивості інформації. Види та форми представлення інформації.

Поняття інформації, інформаційного ресурсу, інформаційного простору та інформаційного суверенітету. Види інформаційних ресурсів: за правом власності (національні, державні, приватні), за формою подання (текстові, графічні, мультимедійні), за призначенням (наукові, освітні, соціальні, ділові), за технологічною основою (цифрові, аналогові), за режимом доступу (публічні, приватні, з обмеженим доступом). Категорії інформації за режимом доступу.

Системні принципи організації інформаційних ресурсів: доступність, цілісність, забезпечення конфіденційності, структурованість, актуальність, узгодженість, точність, вичерпність, підтримка прийняття рішень, уніфікація і стандартизація.

Принципи побудови та функціонування інформаційних, інформаційно-комунікаційних та цифрових комунікаційних систем Вимоги щодо побудови та функціонування аналітичних і пошукових систем, систем підтримки прийняття рішень, автоматизованих систем управління технологічними процесами. Поняття моделі взаємодії відкритих систем OSI. Моделі розмежування доступу до інформації.

Особливості побудови та функціонування мережі Інтернет, потенційні загрози.

Сучасні проблеми та методологічні, технологічні, технічні та організаційні основи побудови та розвитку інфраструктури єдиного інформаційного простору держави.

Поняття надійності, живучості та відмовостійкості (гарантоздатності) інформаційних систем і процесів. Базові методи реалізації цих принципів.

Інформаційні технології в системі державного управління

Поняття інфраструктури, інформаційної інфраструктури. Принципи побудови сучасних інформаційних інфраструктур (технічні аспекти).

Предметна область інформатики. Соціальні аспекти інформатизації суспільства.

Поняття інформаційної технології. Стан, проблеми розвитку і використання інформаційних технологій.

Методи людино-машинного спілкування. Програмні засоби людино-машинного спілкування. Діалогові системи. Інтелектуальний інтерфейс користувача. Мультимедійні системи як засоби людино-машинного інтерфейсу представлення та інтелектуалізації знань.

Методи і засоби розпізнавання і розуміння мовлення. Методи і засоби автоматичного витягування інформації з текстів на природній мові. Методи і засоби автоматичного синтезу мовлення. Методи і засоби розпізнавання образів. Методи і засоби розпізнавання і синтезу зображень. Системи і засоби віртуальної реальності.

Експертні системи. Основні принципи побудови експертних систем. Мови логічного програмування. Інженерія знань. Здобуття, представлення і формування знань. Організація процесів управління і прийняття рішень на основі логіко-лінгвістичних моделей. Експертні системи в задачах планування і управління.

Задачі і функції систем підтримки прийняття рішень (СППР). Базові функціональні підсистеми СППР та їх задачі. Розподілені системи підтримки прийняття рішень у корпоративних системах.

Інформаційні технології та інформаційна безпека у сфері управління, економіки, фінансів, промисловості тощо. Поняття об'єкту критичної інфраструктури та критичної інформаційної інфраструктури (КІІ). Основні загрози КІІ, методи їх виявлення та запобігання.

Стан розвитку та захищеності КІІ провідних країн світу та країн, що розвиваються. Типові політики безпеки та заходи їх забезпечення (огляд).

Питання інформаційної безпеки при створенні систем інформаційно-аналітичної підтримки державних органів.

Загальні відомості щодо методів дослідження складних систем

Сутність системного підходу у дослідженні складних систем. Основи експертного аналізу. Методологія, сутність, вимоги, сфери застосування експертного аналізу та прогнозування.

Основи технічного аналізу. Методологія, сутність, вимоги, сфери застосування технічного аналізу та прогнозування.

Побудова інформаційних моделей об'єктів, визначення критичних місць в інформаційних системах.

Аналіз і оцінка рівня захищеності інформації у СЗІ. Методологія, сутність, вимоги до проведення аналізу ризиків.

Математичні методи аналізу проблем інформаційної безпеки. Доказовий метод в теорії ЗІ.

Елементи теорії прийняття рішень. Формалізація процесу прийняття рішень. Прийняття рішень в умовах визначеності. Прийняття рішень в умовах ризику і невизначеності.

Елементи теорії систем масового обслуговування (СМО). Основні компоненти і характеристики СМО. Вихідний потік вимог. Процеси загибелі і розмноження. Основні типи СМО, які описуються процесами загибелі і розмноження. Мережі масового обслуговування.

Елементи лінійного програмування. Постановка задачі. Графічні методи рішень. Симплекс-метод. Транспортна задача. Подвійна задача. Задачі оптимізації на мережах.

Комп'ютерні системи та їх вплив на інформаційну безпеку держави

Методи організації безпечної взаємодії інформації в комп'ютерних системах.

Роль та місце комп'ютерних систем в державному управлінні та управлінні роботою критично важливих об'єктів держави.

Види інформаційно-технічного впливу в контексті єдиного інформаційного простору та сучасних інформаційних війн. Основні методи, засоби та технології його здійснення.

Основні загрози комп'ютерним системам.

Кібертероризм та сучасні загрози в цій сфері.

Загальний огляд проблем комп'ютерної злочинності. Класифікація комп'ютерних злочинів.

Методи штучного інтелекту у кібербезпеці.

Інформаційна війна та інформаційний вплив

Інформаційні технології як засіб інформаційного впливу. Поняття інформаційної війни, інформаційного впливу, інформаційної зброї, психотронної зброї.

Типи інформаційних війн, основи їх ведення. Типові тактики та стратегії.

Інформаційні війни у сучасному соціально-політичному контексті. Інформаційні операції та технології їхнього здійснення. Захист інформаційного простору держави, суспільства та особистості від негативних впливів. Інформаційна війна, кібероперація, кіберзброя, кібертероризм і кібервійни.

Інформаційна протидія. Роль геополітичного стратегічного аналізу. Основні принципи, завдання, цілі та методи стратегічного прогнозування.

Інформаційно-психологічний вплив. Його цілі та завдання. Особливості формування і функціонування суспільної думки.

Глобальні мережі: феномен Інтернет. Особливості інформаційно-психологічного впливу через Інтернет. Інтернет та сучасна політика.

Можливості і проблеми законодавчого регулювання Інтернет.

Принципи соціального інжинірингу.

Стандарти захисту інформації

Сутність та цілі стандартизації в сфері захисту інформації (ЗІ).

Критерії та класи захищеності засобів обчислювальної техніки та автоматизованих інформаційних систем. Міжнародні та національні стандарти з безпеки комп'ютерних систем, критерії та методи оцінки захищеності цих систем. Процесний підхід щодо побудови системи управління інформаційною безпекою. Поняття Загальних критеріїв (Common criteria) оцінки захищеності комп'ютерних систем .

Нормативно-правова база кібербезпеки.

Захист інформації у комп'ютерних системах

Основні принципи та стратегії ЗІ у комп'ютерних системах.

Методи та види несанкціонованого доступу (НСД). Моделі загроз і порушника. Основні причини порушень безпеки.

Принципи побудови систем захисту інформації. Розмежування доступу користувачів до інформації. Методи ідентифікації та автентифікації (ІА) (парольні схеми ІА, біометричні системи ІА тощо).

Криптографічні засоби захисту інформації. Огляд і класифікація методів шифрування інформації.

Принципи побудови методів та засобів стеганографічного захисту інформації.

Фрагментарний та комплексний і підходи до забезпечення інформаційної безпеки. Безпека периметра.

Моделі та методи забезпечення безпеки програмного забезпечення. Захист програм і даних від «вірусів», «хробаків» і «логічних бомб». Загальні моделі систем і процесів захисту інформації. Антивірусні програми.

Поняття: технічний захист інформації, технічні канали впливу та витоку інформації, комплекс засобів технічного захисту інформації, спеціальні дослідження. Архітектура безпеки та контроль доступу. Безпека мереж та інфраструктури.

Технології забезпечення безпеки мережевої інфраструктури

Забезпечення безпеки на відповідних рівнях моделі OSI: фізичному, канальному, мережному, транспортному, сеансовому. Сучасні системи виявлення вторгнень. Політики виявлення вторгнень. Засоби аналізу безпеки програмного забезпечення. Списки управління доступом (ACL). Передача потоку даних. Багатоадресна розсилка. Технології побудови віртуальних локальних мереж (VLAN). Моніторинг, аналіз та реагування на інциденти.

Засоби забезпечення інформаційної безпеки та їх проектування

Принципи побудови технічних систем. Методологія побудови захищених інформаційних систем (ІС). Поняття архітектури систем. Особливості архітектури систем забезпечення інформаційної безпеки держави.

Особливості використовування засобів забезпечення інформаційної безпеки під час захисту об'єктів критичної інфраструктури.

Параметри функціонування ІС. Поняття критичних параметрів.

Особливості створення систем забезпечення інформаційної безпеки в державній сфері. Захист інформації державного призначення.

Характеристика основних засобів та інструментів забезпечення технічного та криптографічного захисту інформації, кібербезпеки та принципи їх створення.

Методи криптографічного захисту інформації: шифрування та цифровий підпис, вимоги що управління безпекою криптографічних ключів на етапах їх життєвого циклу (генерація, тестування, розподіл). Забезпечення безпеки криптографічних модулів. Поняття про електронну ідентифікацію та електронні довірчі послуги.

Функції та завдання державних органів що регулювання питань кібербезпеки, криптографічного та технічного захисту інформації.

Організаційно-технічні заходи щодо забезпечення захисту інформації. Організація і підрозділи служби безпеки (режиму, охорони, протипожежна, детективна, інформаційно-аналітична тощо).

Особливості захисту інформації в комп'ютерних системах і мережах. Особливості ЗІ у розподілених базах даних і телекомунікаціях. Проблема безпеки при підключенні автоматизованого робочого місця.

4. Критерії оцінювання

Оцінювання випробування відбувається у 200-бальній системі (прохідний бал – 100 б.).

Кількість балів (max – 200)	**Критерії**
180 – 200	Виставляється за глибокі знання програмного матеріалу; вміння аналізувати явища, які вивчаються, у їхньому взаємозв'язку і розвитку, чітко і лаконічно; логічно і послідовно відповідати на поставлені запитання; вміння застосовувати теоретичні положення під час розв'язання практичних задач; вияв креативності у розумінні і творчому використанні набутих знань та умінь.
160 – 179	Виставляється за ґрунтовні знання програмного матеріалу, аргументовані відповіді на поставлені запитання; вміння застосовувати теоретичні положення під час розв'язування практичних задач.
140 – 159	Виставляється за міцні знання програмного матеріалу, аргументовані відповіді на поставлені запитання, які, однак, містять певні (несуттєві) неточності; вміння застосовувати теоретичні положення під час розв'язання практичних задач.
120 – 139	Виставляється за посередні знання програмного матеріалу, мало аргументовані відповіді, слабке застосування теоретичних положень при розв'язанні практичних задач.
100 – 119	Виставляється за слабкі знання програмного матеріалу, неточні або мало аргументовані відповіді, з порушенням послідовності його викладання, за слабке застосування теоретичних положень при розв'язанні практичних задач.
1 – 99	Виставляється за незнання значної частини програмного матеріалу, істотні помилки у відповідях на запитання, невміння орієнтуватися під час розв'язання практичних задач, незнання основних фундаментальних положень.

5. Список рекомендованої літератури

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.
2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці. – К.: ДУТ, 2015. – 345 с.
3. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – К.: ТОВ «СІК ГРУП Україна», 2015. – 449 с.
4. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
5. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
6. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, М.В. Ворохоб. – Київ: Київський столичний університет імені Бориса Грінченка, 2025. – 1016 с.
7. Системи захисту інформації: підручник / Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва. – Київ: Київський столичний університет імені Бориса Грінченка, 2025. – 887 с.
8. Buriachok V.L. Methods of information protection in telecommunication systems: [manual]. / V.L. Buriachok, Ie.V. Duravkin, N.V. Lukova-Chuyko, P.M. Skladanniy / – K.:KUBG, 2019. – 74 с.
9. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – 2023. – 370 с.
10. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. Навчальний посібник для студентів галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека – Київ: Вид-во КУБГ. 2021. 160 с.
11. Соколов, В. Ю. Безпека безпроводових і мобільних мереж: Навчальний посібник / В. Ю. Соколов, В. Л. Бурячок, М. М. Таджділні / ред. перекл. О. П. Райтер. — 2 вид., доп. — К. : КУБГ, 2019. — 130 с.
12. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.
13. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. - В.: ВНТУ, 2011. -198 с.
14. Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л., Складанний П.М., Гайдур Г.І. Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку. Навчальний посібник. – Львів: Магнолія, 2023. – 221 с.
15. Пасічник В.В., Виклюк Я.І., Камінський Р.М. Моделювання складних систем. - Львів: Новий світ-2000, 2021. - 404 с.
16. Горбань І.І. Теорія ймовірностей та математична статистика для наукових працівників та інженерів. - К.: НАН України, 2003. - 239 с.

17. І.В. Веригіна, О.В. Островська, О.В. Сугакова. Теорія ймовірностей та математична статистика. Лекції і практикум. Навчальний посібник (Електронне мережне навчальне видання). – К.: КПІ ім. Ігоря Сікорського, 2022. – 254 с.
18. Катренко А. В. Дослідження операцій: Підручник – 3-тє вид., стер. –Львів: «Магнолія – 2006», 2024. – 350 с.
19. Бідюк П.І., Тимощук О.Л., Коваленко А.Є., Коршевнюк Л.О. Системи і методи підтримки прийняття рішень. Підручник (Електронне мережне навчальне видання). - К.: КПІ ім. Ігоря Сікорського, 2022. – 610 с.
20. Теорія систем масового обслуговування: навч. посібник / А. Л. Литвинов; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків: ХНУМГ ім. О. М. Бекетова, 2018. – 141 с.
21. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с
22. Бутко М.П. Системний підхід і моделювання в наукових дослідженнях. - К.: ЦУЛ, 2014. - 360 с.
23. Толюпа С.В. Захист об'єктів інформаційної діяльності /Толюпа С.В., Оксіюк О.Г., Бурячок В.Л., Вялкова В.І.// К.: ККБ та ЗІ ФІТ КНУ імені Тараса Шевченка, 2018. – 322 с.
24. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1999.
25. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1999.
26. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1999.
27. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / ДСТСЗІ СБ України. - Введ. 1999.
28. 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 / ДСТСЗІ СБ України. - Введ. 2013.
29. НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи / ДСТСЗІ СБ України. - Введ. 2007.
30. Про державну таємницю: Закон України від 21.01.94 № 3855-XII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text
31. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.94 № 80/94-ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
32. Про інформацію: Закон України від 02.10.92 № 2657 - XII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

33. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
34. Про Концепцію Національної програми інформатизації: Закон України від 04.02.98 №75/98-ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text
35. Про науково-технічну інформацію: Закон України від 25.06.93 № 3322 - XII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/3322-12#Text
36. Про Національну програму інформатизації: Закон України від 01.12.22 №2807-IX - ВР [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2807-20#Text
37. Стратегія кібербезпеки України [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text
38. Про технічні регламенти та оцінку відповідності: Закон України від 15.01.2015 № 124-VIII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/124-19#Text
39. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text
40. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем: Постанова Кабінету міністрів України від 29.03.2006 № 373 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
41. Деякі питання електронної ідентифікації та електронних довірчих послуг: Постанова Кабінету міністрів України від 28.06.2024 № 764 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/764-2024-%D0%BF#Text
42. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету міністрів України від 19.06.2019 №518 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
43. Про затвердження Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 07.05.2021 № 278 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/z0696-21#Text
44. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/z0862-07#Text

45. Про затвердження Положення про державну експертизу у сфері технічного захисту інформації: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/z0820-07#Text
46. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.2023 № 463 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/rada/show/v0463519-23#Text
47. SANS Institute [Електронний ресурс]. - Режим доступу: https://www.sans.org/information-security-policy
48. CSA Security Guidance for Critical Areas of Focus in Cloud Computing [Електронний ресурс]. - Режим доступу: https://cloudsecurityalliance.org/research/guidance
49. NERC CIP [Електронний ресурс]. - Режим доступу: https://www.nerc.com/standards/reliability-standards/cip
50. National Institute of Standards and Technology [Електронний ресурс]. - Режим доступу: https://www.nist.gov/