МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

ЗАТВЕРДЖЕНО
Вченою радою Чернівецького
національного університету
імені Юрія Федьковича
протокол № 16 від «22» грудня 2025 р.
Голова Вченої ради
Руслан БІЛОСКУРСЬКИЙ

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЧЕРНІВЕЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

УВЕДЕНЕ В ДІЮ
наказом ректора Чернівецького
національного університету
імені Юрія Федьковича
№ 423 від «22» грудня 2025 р.

Чернівці – 2025

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки (далі – Політика) Чернівецького національного університету імені Юрія Федьковича (далі – ЧНУ, Університет) є внутрішнім нормативним документом, який відображає позицію ЧНУ щодо інформаційної безпеки, а також визначає основні принципи та засади функціонування системи інформаційної безпеки ЧНУ.

1.2. Політику складено відповідно до рекомендацій міжнародних стандартів з інформаційної безпеки та вимог законодавства України, зокрема Законів України: «Про вищу освіту», «Про інформацію», «Про захист персональних даних», «Про інформацію в інформаційно-телекомунікаційних системах», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про основи національної безпеки України», «Про електронні комунікації», «Про електронну ідентифікацію та електронні довірчі послуги», Постанови КМУ №1531 від 26.11.2025 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», інших нормативно-правових актів з питань інформаційної безпеки, затверджених Кабінетом Міністрів України та Міністерством освіти і науки України, а також нормативних документів, що регламентують вимоги до забезпечення інформаційної безпеки.

1.3. Політика спрямована на забезпечення неперервної роботи Університету, мінімізацію ризиків освітньої та наукової діяльності, а також формування позитивної репутації Університету під час взаємодії зі студентами, партнерами та іншими третіми сторонами.

1.4. Політика є нормативною основою для захисту інформаційних активів Університету з метою забезпечення:

1.4.1. Конфіденційності – забезпечення доступності інформації та її активів лише для авторизованих осіб, користувачів і процесів у мінімально необхідному обсязі;

1.4.2. Цілісності – захисту точності, коректності та повноти активів і методів оброблення інформації;

1.4.3. Доступності – забезпечення безперервного доступу до інформаційних і супутніх активів та сервісів Університету відповідно до наданих користувачам повноважень і прав у мінімально необхідному обсязі;

1.4.4. Спостережності – забезпечення можливості визначення користувачів та процесів, які працюють із певним інформаційним активом Університету, часу та дати такої роботи, а також гарантування неможливості відмови від виконаних дій.

1.5. Політика є обов’язковою для виконання всіма підрозділами Університету.

1.6. Дія Політики поширюється також на всі треті сторони, які мають доступ до інформаційних активів Університету.

2. ВИЗНАЧЕННЯ, ТЕРМІНИ ТА СКОРОЧЕННЯ

2.1.1. Авторизація з безпеки – рішення щодо можливості функціонування (експлуатації) відповідної інформаційної, електронної комунікаційної, інформаційно-комунікаційної, технологічної системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного, криптографічного захисту та кіберзахисту, що приймається у встановленому законодавством порядку;

2.1.2. Авторизована система з безпеки – інформаційна, електронна комунікаційна, інформаційно-комунікаційна, технологічна система або її окремі елементи, об’єкт критичної інформаційної інфраструктури, у яких запроваджено заходи та/або системи з безпеки інформації, що пройшли авторизацію з безпеки;

2.1.3. Аналіз загроз – процес вивчення джерел загроз і вразливостей системи з метою визначення можливих впливів на конкретні інформаційні ресурси або системи в певній операційній ситуації;

2.1.4. Аналіз інформаційних ризиків – процес оцінювання потенційного впливу реалізації загроз, визначення загроз і вразливостей та вибір відповідних контрзаходів;

2.1.5. Адміністратор інформаційної системи – структурний підрозділ Університету, який забезпечує процеси функціонування інформаційної системи або сервісу та має повноваження щодо конфігурування, управління розвитком, підтримки, використання та забезпечення безпеки цієї системи;

2.1.6. Вразливість – недолік чи слабке місце в системі безпеки, що може підвищити ймовірність реалізації загрози та порушення конфіденційності, цілісності або доступності інформації;

2.1.7. Документ Політики – додатковий нормативно-розпорядчий документ, який регламентує заходи Політики у межах окремих процесів та/або інформаційних систем (сервісів) Університету;

2.1.8. Доступність – властивість інформації (або інформаційного активу), що визначає можливість її використання за призначенням у будь-який момент часу;

2.1.9. Загроза – спосіб або подія, за допомогою яких може бути порушено конфіденційність, цілісність або доступність інформації;

2.1.10. Заходи щодо захисту – сукупність організаційних та/або технічних дій, спрямованих на управління ризиком;

2.1.11. Зниження ризиків – процес проведення заходів у сфері безпеки з метою зменшення виявлених ризиків до прийнятного рівня;

2.1.12. Інформаційна безпека (ІБ) – сукупність організаційно-технічних заходів і засобів, спрямованих на захист інформації від загроз з метою забезпечення безперервності процесів, зменшення ризиків і оптимізації витрат;

2.1.13. Інформаційна система/сервіс (ІС) – сукупність організаційних і технічних засобів для збору, зберігання, пошуку, оброблення та передавання інформації з метою забезпечення інформаційних потреб користувачів;

2.1.14. Інформаційна технологія (ІТ) – цілеспрямована організована сукупність інформаційних процесів із використанням засобів комп'ютерної техніки, що забезпечують високу швидкість збору, зберігання, пошуку, оброблення та пересилання інформації, доступ до якої здійснюється незалежно від місця її розташування та в будь-який момент часу;

2.1.15. Інформаційний актив – сукупність інформації (відомостей), яка має цінність для Університету, працівників, здобувачів освіти, інших зацікавлених фізичних та юридичних осіб, а також будь-яка система оброблення, обміну або фізичного зберігання цієї інформації;

2.1.16. Інформаційний інцидент – подія або послідовність подій, що створює загрозу конфіденційності, цілісності або доступності інформаційних активів;

2.1.17. Кібербезпека - це сукупність технологій, процесів та практик, спрямованих на захист комп'ютерних систем, мереж, програм та даних у кіберпросторі від крадіжки, пошкодження, несанкціонованого доступу чи інших цифрових загроз, забезпечуючи конфіденційність, цілісність та доступність інформації;

2.1.18. Конфіденційність – властивість інформації (або інформаційного активу), що полягає в тому, що доступ до неї не може бути отриманий неавторизованими особами, об'єктами або процесами відповідно до обмежень, накладених Адміністратором ІС;

2.1.19. Оброблення інформації в системі – виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, що здійснюються в системі за допомогою технічних і програмних засобів або автономно (без підключення до інших засобів оброблення інформації, ліній зв'язку чи мереж передачі даних) пристроями оброблення інформації;

2.1.20. Операційна система (ОС) – базовий комплекс програм, який здійснює управління апаратним забезпеченням комп'ютера або віртуальної машини, забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем;

2.1.21. Оцінювання стану кіберзахисту – процес перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації або кіберзахисту з метою визначення поточного та/або цільового стану захищеності чи перевірки їхньої відповідності вимогам законодавства щодо повноти запроваджених заходів захисту інформації або кіберзахисту, а також відповідності національним стандартам у цій сфері, або стандартам, настановам, рекомендаціям, аналітичним оглядам та іншим документам, розробленим і прийнятим іноземними та міжнародними організаціями у сфері кібербезпеки;

2.1.22. Перелік авторизованих систем з безпеки – єдина електронна база даних, що містить відомості про авторизовані системи з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, у яких обробляються державні інформаційні ресурси або службова інформація, а також інформація, що становить державну таємницю, об’єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, підприємства, установи та організації, органи місцевого самоврядування. Порядок ведення, внесення даних до цього переліку, а також порядок доступу й надання інформації визначаються спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації. Інформація про авторизовані системи з безпеки, що міститься в переліку, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом та інформації, доступ до якої обмежено відповідно до законодавства на період дії воєнного стану;

2.1.23. Політика інформаційної безпеки – документ, що визначає загальні принципи та напрями забезпечення інформаційної безпеки;

2.1.24. Пристрої оброблення інформації – технічні пристрої (засоби) оброблення інформації, у яких технічно неможливо реалізувати програмні процедури розмежування доступу користувачів та інші функціональні послуги безпеки;

2.1.25. Програмне забезпечення (ПЗ) – сукупність програм оброблення інформації та програмних документів, необхідних для їх експлуатації;

2.1.26. Ризик – можливість негативного впливу на діяльність Університету внаслідок порушення конфіденційності, цілісності або доступності інформації;

2.1.27. Система інформаційної безпеки (СІБ) – частина загальної системи управління Університетом, що ґрунтується на методах оцінювання ризиків і призначена для створення, впровадження, експлуатації, контролю, аналізу та постійного вдосконалення інформаційної безпеки;

2.1.28. Спеціальна інформаційно-комунікаційна система –

інформаційно-комунікаційна система, що забезпечує оброблення інформації, яка становить державну таємницю або іншу інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом, із застосуванням технічних засобів електронних комунікацій і засобів криптографічного захисту інформації;

2.1.29. Третя сторона – особа або організація, що не є безпосередньо залученими сторонами, але може взаємодіяти з Університетом у разі виникнення відповідних питань;

2.1.30. Управління ризиками – процес, метою якого є зменшення ризиків до прийнятного рівня шляхом визначення заходів захисту та мінімізації їхнього впливу на систему захисту від несанкціонованих дій;

2.1.31. Цілісність – властивість інформації (або інформаційного активу), що полягає в неможливості її модифікації несанкціонованим чином, тобто без дозволу Адміністратора ІС;

2.2. Усі визначення термінів, що застосовуються в Політиці, подано для зручності та використовуються виключно для її застосування та тлумачення.

2.3. Усі інші терміни, ужиті в Політиці, застосовуються у значеннях, визначених законодавчими та нормативно-правовими актами України.

3. СФЕРА ЗАСТОСУВАННЯ

3.1. Забезпечення ІБ та СІБ Університету ґрунтується на таких фундаментальних принципах:

3.1.1. Принцип законності – СІБ Університету базується на нормах чинного законодавства України та застосуванні міжнародних норм у сфері ІБ;

3.1.2. Принцип узгодженості – цілі та завдання ІБ відповідають стратегічним цілям і завданням Університету;

3.1.3. Принцип єдності – управління ІБ є невід’ємною частиною управління Університетом;

3.1.4. Принцип ефективності – засоби захисту інформаційних активів впроваджуються відповідно до їхньої критичності, тобто категорії класифікації та рівня ризику інформаційного активу;

3.1.5. Принцип практичності – засоби захисту інформаційних активів повинні бути практичними та забезпечувати баланс між працездатністю системи і її захищеністю;

3.1.6. Принцип неперервності – ІБ є постійним процесом протидії загрозам і управління ризиками, характерними для сфери діяльності Університету;

3.1.7. Принцип відповідальності – керівництво Університету всіх рівнів, працівники, здобувачі освіти та інші треті сторони, які мають доступ до інформаційних активів Університету, повинні дотримуватися вимог

нормативних документів Університету у сфері ІБ та нести персональну відповідальність за їх невиконання;

3.1.8. Принцип комплексності та системності – інформаційна безпека забезпечується на правовому, адміністративному, організаційному та програмно-технічному рівнях, а також на підставі комплексного застосування засобів захисту інформації та взаємодії всіх підрозділів Університету.

3.2. Основними завданнями ІБ Університету є:

3.2.1. Забезпечення інформаційної безпеки працівників та здобувачів освіти Університету;

3.2.2. Управління ІБ, у тому числі визначення ролей та обов'язків у сфері ІБ, створення та підтримання СІБ Університету;

3.2.3. Класифікація інформаційних активів;

3.2.4. Здійснення оцінки ризиків ІБ;

3.2.5. Забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків;

3.2.6. Моніторинг подій ІБ, реагування на них та управління інцидентами ІБ;

3.2.7. Забезпечення безперервності інформаційної діяльності Університету;

3.2.8. Безпечне управління життєвим циклом ІС.

3.2.9. Забезпечити мінімальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем;

3.2.10 Забезпечення застосування специфічних заходів безпеки (контроль доступу сторонніх осіб, захист обладнання) для технологічних систем.

3.3. Серед основних об'єктів, на які поширюється дія системи ІБ Університету, розглядаються такі види ресурсів:

3.3.1. Інформаційні ресурси – інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються або оприлюднюються, у тому числі відомості працівників, партнерів Університету, бази даних і файли, документація, інструкції користувача, навчальні матеріали, описи процедур, архівована інформація тощо;

3.3.2. Програмне забезпечення – прикладне, системне, сервісне та будь-яке інше програмне забезпечення, незалежно від способу отримання (придбання, власна розробка чи ліцензоване використання), яке використовується в Університеті працівниками, системами для роботи та здобувачами освіти, сторонніми фізичними і юридичними особами, а також іншими внутрішніми та зовнішніми системами;

3.3.3. Фізичні ресурси – працівники, апаратні засоби інфраструктури (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати,

телекомунікаційне обладнання, обладнання зв’язку, маршрутизатори, факси, модеми тощо), носії даних (диски, флеш-накопичувачі тощо), приміщення, виробниче обладнання та інші технічні засоби;

3.3.4. Сервісні ресурси – обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв’язку тощо), інші технологічні системи (опалення, освітлення, енергозбереження, енергозабезпечення, кондиціонування повітря, системи сигналізації та моніторингу), усі послуги, пов’язані з отриманням, налаштуванням, використанням, передачею та знищенням ресурсів, а також юридичні та фізичні суб’єкти, організації, установи та підприємства, чиїми сервісами користується Університет для отримання, використання, передачі та знищення ресурсів.

3.4. Університет дотримується таких правил ІБ:

3.4.1. Працівники Університету беруть участь у підтримці належного рівня ІБ у межах своїх обов’язків і повноважень та несуть відповідальність за її порушення відповідно до чинного законодавства України, внутрішніх нормативних документів Університету та положень цієї Політики;

3.4.2. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги ІБ;

3.4.3. Публічні сервіси Університету та внутрішні мережі повинні відповідати вимогам стандартів ІБ;

3.4.4. Університет забезпечує виконання всіх вимог, передбачених у договорах із третіми сторонами щодо використання інформаційних активів;

3.4.5. Для зменшення ризику виникнення інцидентів ІБ в Університеті створюються умови для систематичного навчання працівників та здобувачів освіти із метою дотримання норм та застосування заходів ІБ;

3.4.6. Про кожен інцидент ІБ працівники Університету негайно інформують безпосереднього керівника. Документами з ІБ Університету передбачаються процедури аналізу та реагування на інциденти ІБ; за результатами аналізу вживаються заходи для запобігання повторенню подібних інцидентів;

3.4.7. В Університеті розробляються, систематично тестуються та оновлюються плани безперервного функціонування на випадок непередбачуваних критичних ситуацій;

3.4.8. В університеті на постійній основі здійснюється моніторинг подій кібербезпеки.

3.5. Університет використовує такі підходи щодо забезпечення ІБ:

3.5.1. Створення та затвердження переліку відомостей, що містять інформацію з обмеженим доступом, службову інформацію, інформацію з грифом «ДСК»;

3.5.2. Встановлення правил доступу до інформаційних ресурсів і програмно-технічних комплексів;

3.5.3. Забезпечення контролю фізичного та логічного доступу до всіх визначених ресурсів;

3.5.4. Забезпечення парольного захисту програмних і сервісних ресурсів;

3.5.5. Забезпечення антивірусного захисту програмних і сервісних ресурсів;

3.5.6. Забезпечення захисту мережі;

3.5.7. Забезпечення контрольованого доступу до ресурсів у мережі та на всіх рівнях (локальна мережа, мережа Інтернет, мережі інших організацій);

3.5.8. Забезпечення ідентифікації та автентифікації всіх наявних інформаційних ресурсів Університету;

3.5.9. Забезпечення криптографічного захисту інформації.

4. ДОДАТКОВІ ДОКУМЕНТИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Додаткові документи Політики інформаційної безпеки (Документи Політики) – це нормативно-розпорядчі документи Університету, які регламентують заходи інформаційної безпеки під час функціонування окремих інформаційних систем і сервісів та забезпечать виконання мінімальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем для потреб Університету.

4.2. Документи Політики розробляються для ІС і є невід'ємною частиною документації, необхідної для їхнього функціонування. Вони можуть мати постійний або тимчасовий характер.

4.3. Кожен Документ Політики може містити такі відомості щодо вимог ІБ, необхідних для функціонування відповідних ІС:

- загальні вимоги безпеки ІС;
- вимоги до рівня захищеності ІС;
- вимоги до організації мережної безпеки;
- вимоги до виявлення інформаційних ризиків та інцидентів;
- вимоги до керування доступом до інформаційних активів;
- вимоги до керування моніторингом та сповіщеннями;
- вимоги до захисту від шкідливого коду;
- вимоги до віддаленого доступу до інформаційних активів;
- вимоги до забезпечення продуктивності ІС;
- вимоги до функціонування служби підтримки користувачів;
- вимоги до забезпечення криптографічного захисту інформації.

4.4. Загальні вимоги ІБ ІС у Документах Політики стосуються таких питань:

- предмет захисту в межах процесу, який передбачає функціонування ІС;

- вимоги щодо захисту інформації, заходів ІБ та шляхи їхнього застосування;

- рівні ІБ;

- засоби ІБ.

4.5. Вимоги ІБ до рівня захищеності ІС у Документах Політики стосуються таких питань:

- безпека облікових записів користувачів;

- сумісність ІС із програмними платформами та супутніми ІТ-засобами;

- вимоги до встановлення та видалення ІТ-засобів авторизованими фахівцями;

- вимоги до файлової системи та компонентів операційної системи;

- вимоги до конфігурації апаратних засобів.

4.6. Вимоги ІБ до організації мережної безпеки у Документах Політики стосуються таких питань:

- рівні захисту локальної мережі від незахищених та ненадійних зовнішніх мереж;

- вимоги до мережних екранів (файрволів);

- вимоги до виявлення вторгнень у мережі.

4.7. Вимоги ІБ до виявлення інформаційних ризиків та загроз у Документах Політики стосуються таких питань:

- перелік ризиків та загроз;

- фактори, внаслідок яких може бути отримана інформація через несанкціоновані канали;

- фактори, внаслідок прояву яких може бути порушена цілісність або доступність інформації;

- моделі потенційних порушників;

- заходи щодо зменшення вразливості інформаційних активів.

4.8. Вимоги ІБ щодо керування доступом до інформаційних активів у Документах Політики стосуються таких питань:

- надання прав доступу користувачам та їх скасування;

- вимоги до аутентифікації користувачів;

- вимоги до ідентифікації користувачів;

- вимоги щодо авторизації користувачів на основі ролевої системи доступу.

4.9. Вимоги ІБ до керування моніторингом та сповіщеннями у Документах Політики стосуються таких питань:

- вимоги щодо реєстрації подій та їх ідентифікації;

- захист від несанкціонованого впливу на процес реєстрації подій;

- вимоги до забезпечення сповіщень у критичних ситуаціях.

4.10. Вимоги ІБ щодо захисту від шкідливого коду у Документах Політики стосуються таких питань:

- виявлення шкідливих програм на основі бази сигнатур вірусів та евристичного аналізу;

- вимоги до своєчасного оновлення антивірусного ПЗ та баз сигнатур вірусів.

4.11. Вимоги ІБ до віддаленого доступу користувачів до інформаційних активів Університету у Документах Політики стосуються таких питань:

- загальні вимоги до віддаленого доступу до інформаційних активів;

- вимоги до організації доступу на основі стеку протоколів TCP/IP;

- вимоги до віддаленого доступу засобами вебтехнологій;

- вимоги до віддаленого доступу з використанням захищених мереж.

4.12. Вимоги ІБ до забезпечення продуктивності ІС у Документах Політики стосуються таких питань:

- доступність інформаційних активів;

- надійність функціонування апаратного забезпечення та ПЗ;

- неперервність і своєчасність виконання бізнес-процесів;

- резервне копіювання інформаційних активів та плани відновлення у випадку критичних ситуацій.

4.13. Вимоги ІБ до функціонування служби підтримки користувачів у Документах Політики стосуються таких питань:

- визначення підрозділів або робочих груп працівників, відповідальних за підтримку ІС;

- технічні засоби підтримки користувачів;

- вимоги до оперативності підтримки користувачів.

5. РОЛІ ТА ОБОВ’ЯЗКИ У ПОЛІТИЦІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Ролі та обов’язки під час керування Політикою:

5.1.1. Центр цифрової трансформації ЧНУ (ЦЦТ) забезпечує процес розроблення, впровадження, функціонування, моніторингу, контролю, підтримки та вдосконалення СІБ;

5.1.2. На ЦЦТ покладаються завдання щодо виконання заходів ІБ, їхньої відповідності вимогам чинного законодавства України, у тому числі нормативно-правових актів Міністерства освіти і науки України, нормативних документів Університету, а також інтегрованості ІБ в інформаційні системи та сервіси;

5.1.3. ЦЦТ контролює виконання Політики, систематично аналізує ефективність її реалізації та вносить пропозиції щодо оновлення;

5.1.4. ЦЦТ веде реєстр ІС, які підлягають документуванню, а також розробляє відповідні документи Політики;

5.1.5. ЦЦТ здійснює контроль за діяльністю будь-якого структурного підрозділу Університету щодо виконання нормативних документів з питань ІБ шляхом ініціювання внутрішнього моніторингу;

5.1.6. ЦЦТ здійснює контроль за відповідністю стану інформаційної безпеки Університету мінімальним вимогам до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем.

5.1.7. Ініціативи ЦЦТ щодо функціонування СІБ узгоджуються з комісією Вченої ради Університету з питань інформаційної та медійної діяльності, рішення якої з питань ІБ є обов'язковими для виконання всіма працівниками Університету;

5.1.8. Документи Політики розробляються адміністраторами ІС (ЦЦТ, режимно-секретним відділом та іншими структурними підрозділами Університету) і затверджуються ректором;

5.1.9. Підтримка актуального стану Політики здійснюється адміністраторами ІС, які забезпечують її контроль, впровадження, виконання та вдосконалення;

5.1.10. Стратегія розвитку ІТ Університету та всі проєкти, пов'язані з ІТ, узгоджуються з цією Політикою.

5.2. Ролі та обов'язки під час застосування Політики:

5.2.1. Університет управляє ризиками ІБ через адміністраторів ІС, постійного моніторингу подій кібербезпеки та ЦЦТ шляхом складання, впровадження, тестування та оновлення планів забезпечення безперервного функціонування ІС на випадок непередбачуваних критичних ситуацій;

5.2.2. Аналіз ризиків та загроз здійснюють адміністратори ІС;

5.2.3. Кожен працівник Університету забезпечує підтримку належного рівня ІБ у межах своїх службових обов'язків і повноважень. Працівники повинні виконувати вимоги Політики, законодавчих, регуляторних та внутрішньоуніверситетських норм і несуть відповідальність за їх порушення відповідно до чинного законодавства України та нормативних документів Університету;

5.2.4. Для зниження ризиків виникнення інцидентів ІБ керівництво Університету створює умови для систематичного навчання працівників нормам та заходам ІБ;

5.2.5. Усі розроблені документи з питань доступу працівників Університету в межах їхніх повноважень мають використовуватися для забезпечення виконання вимог Політики ІБ.

5.3. Обов'язки здобувачів освіти та представників третіх сторін:

5.3.1. Здобувачі освіти та представники третіх сторін несуть відповідальність за дотримання вимог Політики інформаційної безпеки

Університету та чинного законодавства України;

5.3.2. Представники третіх сторін, за необхідності, проходять належне навчання для підвищення поінформованості та регулярно отримують оновлені відомості щодо політик і процедур Університету, ознайомлення з якими є обов'язковим для виконання покладених на них зобов'язань відповідно до укладених договорів;

5.3.3. Працівники та представники третіх сторін ознайомлюються з документами Університету, що встановлюють їхню відповідальність щодо ІБ, та підтверджують це підписом;

5.3.4. Після завершення співпраці або контракту всі отримані від Університету ресурси, що перебували у використанні, мають бути повернені у робочому стані відповідно до встановленого рівня ІБ.

6. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

6.1. Політика набирає чинності з моменту введення її в дію наказом ректора Університету.

6.2. ЦЦТ проводить роботи щодо підтримки Політики в актуальному стані. Перегляд Політики здійснюється за необхідності, але не рідше ніж один раз на рік.

6.3. Внесення змін до Політики здійснюється у таких випадках:

- зміни у законодавчих, регуляторних або інших нормах;
- зміни в документах, на підставі яких розроблялася Політика;
- впровадження нових документів, що впливають на процеси, описані в Політиці;
- зміна ролей, відповідальності та процесів, установлених Політикою;
- зміни в інформаційній інфраструктурі та/або впровадження нових ІТ.

6.4. Зміни та доповнення до цього документа набирають чинності з першого робочого дня з дати введення їх у дію, якщо інше не передбачено рішенням Вченої ради Університету або її комісії з питань інформаційної та медійної діяльності, та поширюються лише на ті частини документа, що підлягають змінам.

Підготовлено

Директор ННІФТКН — Петро ШПАТАР — "12" грудня 2025 р.

Завідувач кафедри РТ та ІБ — Андрій САМЛА — "12" грудня 2025 р.

Погоджено

Проректор з науково-педагогічної роботи та цифрової трансформації — Андрій ВЕРСТЯК

Керівник центру цифрової трансформації — Юрій АНТОЩУК

Юридичний відділ — Анжела ЛЯТНІЙ