«Затверджую»
Ректор Національного університету
«Львівська політехніка»
проф. Бобало Ю.Я.
_____
«_____2018 р.

Міністерство освіти і науки України

Національний університет «Львівська політехніка»

Політика інформаційної безпеки Національного університету «Львівська політехніка»

Львів - 2018

Зміст

Розділ 1. Вступ

Політика інформаційної безпеки Національного університету «Львівська політехніка» (далі – Політика) – це внутрішній нормативний документ, який відображає позицію Національного університету «Львівська політехніка» (далі – Університет) щодо інформаційної безпеки (далі – ІБ), а також визначає основні принципи та завдання системи управління інформаційною безпекою (далі – СУІБ) Університету. Політику складено відповідно до вимог законодавства України та рекомендацій міжнародних стандартів інформаційної безпеки ISO/IEC 27000.

1.1. Загальні положення

Інформація є ресурсом, який, як і інші матеріальні та нематеріальні ресурси, має певну цінність для Університету а, отже, потребує відповідного захисту.

Інформаційна безпека передбачає захист інформації від різноманітних загроз для підтримки неперервності освітньої та наукової діяльності, зменшення прямої та непрямої шкоди від несанкціонованого використання інформації, збільшення прямої та непрямої користі від наявної інформації та розширення можливостей ведення основної діяльності Університету.

Незалежно від форми інформації та ресурсів, які використовуються для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень захисту інформації.

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

- конфіденційності – забезпечення доступності інформації та її активів тільки для авторизованих осіб, користувачів, процесів у мінімально необхідному обсязі;
- цілісності – захисту точності, коректності та повноти активів і методів обробки інформації;

- доступності – забезпечення неперервного доступу до інформаційних і супутніх активів і сервісів Університету, згідно з наданими користувачам повноваженням і правами у мінімально необхідному обсязі;
- спостережності – забезпечення можливості визначення користувачів, процесів, що працюють з тим чи іншим інформаційним активом Університету, час та дату такої роботи, а також забезпечення принципу неможливості відмови від виконаних дій.

ІБ досягається шляхом упровадження сукупності необхідних засобів захисту, до яких можуть входити політики, регламенти, рекомендації, інструкції, організаційні структури та програмні функції.

У разі невідповідності будь-якої частини Політики чинному законодавству України, нормативно-правовим актам Міністерства освіти і науки України, у т.ч. у зв'язку із внесенням до них змін та доповнень, прийняттям нових законодавчих актів України, підрозділи Університету керуються цією Політикою у частині, що не суперечить чинному законодавству.

Політика інформаційної безпеки Національного університету «Львівська політехніка» є обов'язковою для використання всіма підрозділами Університету. Дія Політики також поширюється на всі треті сторони, які мають доступ до інформаційних активів Університету.

1.2. Ціль документа

Політика передбачає планування розвитку інфраструктури Університету та заходів безпеки, які повинні бути передбачені у СУІБ для зменшення ризиків під час управління інформацією Університету.

Ціллю Політики є впровадження та ефективне функціонування СУІБ, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів Університету від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників Університету, забезпечувати неперервну роботу Університету, сприяти

мінімізації ризиків освітньої та наукової діяльності Університету та створювати позитивну репутацію Університету під час роботи зі студентами та іншими третіми особами.

Основним завданням інформаційної безпеки є захист інформаційних ресурсів Університету від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

1.3. Нормативна база

Політика розроблена відповідно до вимог чинного законодавства України, а саме:

- Законів України «Про вищу освіту», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних»;
- нормативно-правових актів з інформаційної безпеки Кабінету Міністрів України, Міністерства освіти і науки України;
- інших нормативних документів, що регламентують вимоги до інформаційної безпеки.

Розділ 2. Визначення, терміни та скорочення

Визначення, терміни та скорочення вживаються у такому значенні:

- **Аналіз загроз** – це процес вивчення джерел загроз щодо вразливостей в системі, щоб визначити впливи на конкретні системи в конкретній оперативній ситуації.
- **Аналіз інформаційних ризиків** – процес оцінювання потенційного впливу реалізації загроз на бізнес, визначення загроз і вразливостей і вибір відповідних контрзаходів.
- **Бізнес-процес** – структурована послідовність дій щодо виконання певного виду діяльності на всіх етапах діяльності Університету, метою якої є отримання заданого результату, що має цінність для Університету (зокрема, освітня, наукова, видавнича, проектна, консультаційна та інші види діяльності).
- **Власник інформаційної системи/сервісу** (власник ІС) – структурний підрозділ Університету, що використовує систему/сервіс для забезпечення процесів підрозділу та має ухвалену керівництвом Університету відповідальність щодо контролювання впровадження, розвитку, підтримування, використання та забезпечення безпеки цієї системи.
- **Вразливість** – недолік чи вада в системі безпеки, які збільшують імовірність настання загрози порушення конфіденційності, цілісності та доступності інформації.
- **Документ Політики** – додатковий нормативно-розпорядчий документ, який регламентує заходи Політики у межах окремих бізнес-процесів і/або інформаційних систем/сервісів Університету.
- **Доступність** – властивість інформації (або інформаційного активу), яка визначає можливість її використання за призначенням в будь-який момент часу.
- **Загроза** – спосіб, за допомогою якого може бути порушена конфіденційність, цілісність та доступність інформації.

- **Заходи щодо захисту** – сукупність організаційних і/або технічних дій, спрямованих на управління ризиком.
- **Зниження ризиків** – процес проведення заходів у сфері безпеки задля зменшення виявлених ризиків до прийнятного рівня.
- **Інформаційна безпека** (ІБ) – це сукупність організаційно-технічних заходів і засобів, спрямованих на захист інформації від загроз з метою забезпечення безперервності бізнес-процесів, зниження ризиків і оптимізації витрат.
- **Інформаційна система/сервіс** (ІС) – сукупність організаційних і технічних засобів для збору, збереження, пошуку, обробки та пересилання інформації з метою забезпечення інформаційних потреб користувачів.
- **Інформаційна технологія** (ІТ) – цілеспрямована організована сукупність інформаційних процесів з використанням засобів комп'ютерної техніки, що забезпечують високу швидкість збору, збереження, пошуку, обробки та пересилання інформації, доступ до джерел інформації незалежно від місця їх розташування та у будь-який момент часу.
- **Інформаційний актив** – це сукупність інформації (відомостей), що має цінність для Університету, працівників, здобувачів освіти, сторонніх фізичних і юридичних осіб, діяльність яких пов'язана з Університетом, а також будь-яка система обробки, обміну або фізичного місця зберігання інформації.
- **Інформаційний інцидент** – подія або їх послідовність, які ставлять під загрозу конфіденційність, цілісність і доступність інформаційних активів.
- **Конфіденційність** – властивість інформації (або інформаційного активу), яка полягає в тому, що доступ до неї не може бути отриманий неавторизованими особою, об'єктом і/або процесом, внаслідок правових обмежень, накладених її власником.
- **Операційна система** (ОС) – базовий комплекс програм, що виконує управління апаратною складовою комп'ютера або віртуальної машини; забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем.

- **Підрозділ з питань інформаційної безпеки** (Підрозділ ІБ) – підрозділ у структурі Центру інформаційного забезпечення Національного університету «Львівська політехніка», основною функцією якого є вирішення завдань інформаційної безпеки.
- **Політика** – документ, що визначає загальні принципи та напрями, визначені керівництвом Університету.
- **Програмне забезпечення** (ПЗ) – сукупність програм системи обробки інформації і програмних документів, необхідних для їх експлуатації.
- **Ризик** – це ймовірність шкідливого впливу на діяльність Університету у результаті порушення конфіденційності, цілісності та доступності інформації.
- **Система управління інформаційною безпекою** (СУІБ) – частина загальної системи управління Університетом, яка ґрунтується на підході оцінювання ризиків, призначена для створення, впровадження, експлуатації, контролю, аналізу, підтримки і покращення інформаційної безпеки Університету.
- **Третя сторона** – особа або організація, які вважаються незалежними від задіяних сторін, у випадках виникнення будь-яких питань.
- **Управління ризиками** – це процес, метою якого є зменшити ризики до прийнятного рівня, визначивши заходи захисту та мінімізувавши їх вплив на систему захисту від невизначених подій.
- **Цілісність** – властивість інформації (або інформаційного активу), яка полягає в неможливості її модифікації несанкціоновано, тобто без дозволу її власника.

Усі визначення термінів, що застосовані в Політиці, вжиті лише для зручності подання інформації та використовуються виключно для застосування та тлумачення Політики.

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

Розділ 3. Сфера застосування

Політика розповсюджується на весь Університет у цілому та повинна використовуватися для всіх критичних бізнес-процесів, інформаційних систем та сервісів Університету, які можуть негативно впливати на результати діяльності Університету своєю відсутністю або функціонуванням з помилками.

3.1. Принципи інформаційної безпеки

Забезпечення ІБ та СУІБ Університету ґрунтуються на таких фундаментальних принципах:

- принцип законності: СУІБ Університету базується на нормах чинного законодавства України, а також застосуванні міжнародних норм в галузі ІБ;
- принцип узгодженості: цілі та завдання ІБ відповідають стратегічним цілям та завданням Університету;
- принцип єдності: управління ІБ є невід'ємною частиною управління Університетом;
- принцип ефективності: засоби захисту інформаційних активів впроваджуються відповідно до їхньої критичності, тобто категорії класифікації та рівня ризику інформаційного активу;
- принцип практичності: засоби захисту інформаційних активів повинні бути практичними та підтримувати баланс між працездатністю і захищеністю ІС;
- принцип неперервності: ІБ є постійним процесом протистояння загрозам та управління ризиками, характерними для сфери діяльності Університету;
- 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 їхнє невиконання;
- принцип комплексності та системності: ІБ Університету забезпечується на правовому, адміністративному, організаційному та програмно-технічному

рівнях, а також на підставі комплексного застосування засобів захисту інформації та взаємодії всіх підрозділів Університету.

Принципи ІБ інтегровані в усі особливості управління процесами та інформаційними технологіями Університету.

3.2. Завдання інформаційної безпеки

Основними завданнями ІБ Університету є:

- забезпечення інформаційної безпеки працівників та здобувачів освіти Університету;
- управління ІБ, у тому числі визначення ролей та обов'язків у галузі ІБ, створення та підтримування СУІБ Університету;
- класифікація інформаційних активів;
- здійснення оцінки ризиків ІБ;
- забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків;
- моніторинг подій ІБ, реагування на них і управління інцидентами ІБ;
- забезпечення неперервності інформаційної діяльності Університету;
- безпечне управління життєвим циклом ІС.

3.3. Об'єкти інформаційної безпеки

Серед основних об'єктів, на які розповсюджується дія ІБ Університету, розглядаються такі види ресурсів:

- інформаційні ресурси – інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання працівників, партнерів Університету, бази даних та файли, документація, інструкції користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
- програмне забезпечення – прикладне, системне, сервісне та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується

в Університеті працівниками та системами для роботи та взаємодії зі здобувачами освіти, сторонніми фізичними та юридичними особами, а також іншими внутрішніми та зовнішніми системами тощо;

- фізичні ресурси – працівники, апаратні засоби інфраструктури (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), приміщення, виробниче обладнання, інші технічні засоби тощо;
- сервісні ресурси - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх співробітники), послугами яких користується Університет для отримання, використання, передачі та знищення ресурсів.

Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їхньої мінімізації, тобто Університет використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків основної діяльності.

3.4. Правила інформаційної безпеки

Університет дотримується таких правил щодо ІБ та безперебійної діяльності:

- працівники Університету беруть участь у підтримці відповідного рівня ІБ в межах своїх обов'язків та повноважень і несуть відповідальність за його порушення в межах, встановлених чинним законодавством України, внутрішніми нормативними документами Університету та цією Політикою;
- під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги ІБ;

- публічні сервіси Університету та внутрішні мережі Університету повинні відповідати вимогам стандартів з ІБ;
- Університет забезпечує зі свого боку виконання усіх вимог ІБ, які наявні в угодах з третіми сторонами стосовно використання інформаційних активів;
- для зменшення ризиків виникнення інцидентів ІБ в Університеті створюються умови для систематичного навчання працівників з метою дотримання норм і вживання заходів ІБ;
- про кожен інцидент ІБ працівники Університету негайно інформують безпосереднього керівника. Документами з ІБ Університету повинні бути передбачені процедури аналізу та реагування на той чи інший інцидент ІБ; за результатами аналізу вживаються заходи щодо недопущення повторення подібних інцидентів;
- в Університеті складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування Університету на випадок непередбачуваних критичних ситуацій.

3.5. Підходи інформаційної безпеки

Університетом використовуються такі підходи щодо забезпечення ІБ:

- створення та затвердження переліку відомостей, що містять інформацію з обмеженим доступом, службову інформацію, інформацію з грифом «ДСК»;
- створення та затвердження переліку критичних бізнес-процесів;
- встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечення контролю фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечення парольного захисту програмних та сервісних ресурсів;
- забезпечення антивірусного захисту програмних та сервісних ресурсів;
- забезпечення захисту мережі;
- забезпечення віддаленого доступу до ресурсів мережі Університету (локальної, мережі Інтернет, мереж інших організацій);

- забезпечення ідентифікації та автентифікації усіх наявних інформаційних ресурсів Університету;
- забезпечення криптографічного захисту інформації.

Розділ 4. Додаткові документи політики інформаційної безпеки

Додаткові документи політики інформаційної безпеки (далі – документи Політики) – це нормативно-розпорядчі документи Університету, які регламентують заходи ІБ під час функціонування окремих інформаційних систем і сервісів для потреб Університету.

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

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 загроз;
- 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.

4.1. Загальні вимоги безпеки інформаційних систем/сервісів

Загальні вимоги ІБ ІС у документах Політики стосуються таких питань:

- предмет захисту в межах бізнес-процесу, який передбачає функціонування ІС;
- вимоги до захисту інформації, заходів ІБ та шляхи їхнього застосування;
- рівні ІБ;

- засоби ІБ.

4.2. Вимоги до рівня захищеності інформаційних систем/сервісів

Вимоги ІБ до рівня захищеності ІС у документах Політики стосуються таких питань:

- безпека облікових записів користувачів;
- сумісність ІС з програмними платформами та супутнім ПЗ;
- вимоги до встановлення та видалення ПЗ авторизованими фахівцями;
- вимоги до файлової системи та дозволів ОС;
- вимоги до конфігурації апаратних засобів.

4.3. Вимоги до організації мережної безпеки

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;
- вимоги до виявлення вторгнень до мережі.

4.4. Вимоги до виявлення інформаційних ризиків та загроз

Вимоги ІБ до виявлення інформаційних ризиків та загроз у документах Політики стосуються таких питань:

- перелік ризиків та загроз;
- фактори, наслідком, яких може бути отримання (або небезпека отримання) інформації через несанкціоновані канали;
- фактори, наслідком прояву яких може бути порушення цілісності або доступності інформації;
- моделі порушників;
- заходи щодо зменшення вразливості інформаційних активів.

4.5. Вимоги до керування доступом до інформаційних активів

Вимоги ІБ до керування доступом до інформаційних активів та загроз 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.

4.6. Вимоги до керування моніторингом та сповіщеннями

Вимоги ІБ до керування моніторингом та сповіщеннями у документах Політики стосуються таких питань:

- вимоги щодо реєстрації подій, їх ідентифікації;
- захист від експлуатаційних проблем реєстрації подій;
- вимоги до забезпечення сповіщень щодо критичних ситуацій:

4.7. Вимоги до захисту від шкідливого коду

Вимоги ІБ до захисту від шкідливого коду у документах Політики стосуються таких питань:

- виявлення шкідливих програм на основі баз сигнатур вірусів та евристичного аналізу;
- вимоги до своєчасного оновлення антивірусного ПЗ та баз сигнатур вірусів;
- вимоги до функціонування антивірусного ПЗ у межах бізнес-процесу.

4.8. Вимоги до віддаленого доступу до інформаційних активів

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 з'єднання на основі стека протоколів TCP/IP;
- вимоги до віддаленого доступу засобами веб-технологій;
- вимоги до віддаленого доступу з використанням захищених мереж.

4.9. Вимоги до забезпечення продуктивності інформаційних систем/сервісів

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-процесу;
- резервне копіювання інформаційних активів та плани відновлення на випадок виникнення критичних ситуацій.

4.10. Вимоги до функціонування служби підтримки користувачів

Вимоги ІБ до функціонування служби підтримки користувачів у документах Політики стосуються таких питань:

- визначення підрозділів чи робочих груп працівників, відповідальних за підтримку ІС;
- технічні засоби підтримки користувачів;
- вимоги до оперативності підтримки користувачів.

Розділ 5. Ролі та обов'язки політики інформаційної безпеки

Керівництво Університету чітко розуміє, що ІБ є основою життєдіяльності Університету та сприяє (організаційно та фінансово) впровадженню, контролю та виконанню вимог прийнятої Політики.

5.1. Ролі та обов'язки під час керування політикою

В Університеті створений та постійно працює підрозділ з питань ІБ (далі – Підрозділ ІБ) у структурі Центру інформаційного забезпечення.

Підрозділ ІБ забезпечує процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ.

На Підрозділ ІБ покладені завдання щодо визначення завдань ІБ, їх відповідності вимогам чинного законодавства України, в тому числі, нормативно-правовим актам Міністерства освіти і науки України, нормативним документам Університету, а також їх інтегрованості у бізнес-процеси, інформаційні системи та сервіси.

Підрозділ ІБ переглядає Політику, систематично аналізує ефективність її реалізації, та затверджує зміни до неї.

Підрозділ ІБ веде реєстр ІС, які підлягають документуванню і для яких розробляються документи Політики.

Підрозділ ІБ здійснює контроль за діяльністю будь-якого структурного підрозділу Університету щодо виконання ним вимог нормативних документів Університету з питань ІБ шляхом ініціювання перед Ректором Університету проведення перевірок підрозділів Університету з питань впровадження та функціонування СУІБ.

Ініціативи Підрозділу ІБ щодо функціонування СУІБ подаються на розгляд комісії Вченої Ради Університету з питань інформатизації, рішення якої щодо питань ІБ є обов'язковими для виконання усіма працівниками Університету.

Документи Політики розробляються власниками ІС (Центром інформаційного забезпечення, Науково-технічним Центром мережних технологій та іншими структурними підрозділами Університету за відповідними напрямами діяльності) і затверджуються ректором або проректором, відповідальним за ІБ.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані здійснює Підрозділ ІБ. Постійний контроль впровадження, виконання, вдосконалення та підтримки документів Політики в актуальному стані здійснюють власники ІС.

Стратегія розвитку ІТ Університету, усі проекти, які пов'язані з ІТ, узгоджуються з цією Політикою.

5.2. Ролі та обов'язки під час застосування політики

В Університеті управління ризиками ІБ здійснюється власниками ІС та Підрозділом ІБ шляхом складання, впровадження, тестування та оновлення планів забезпечення безперебійного функціонування ІС на випадок непередбачених критичних ситуацій. Аналіз ризиків та загроз ІБ проводять власники ІС.

Кожен працівник Університету забезпечує підтримку відповідного рівня ІБ Університету. В межах своїх службових обов'язків та повноважень працівники повинні виконувати та відповідати за виконання вимог Політики, законодавчих, регуляторних і внутрішньо-університетських норм і несуть відповідальність за їх порушення згідно з чинним законодавством України та нормативними документами Університету.

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

Усі розроблені документи з питань ІБ доступні працівникам Університету у межах їх повноважень і призначені надавати допомогу у виконанні вимог ІБ.

Здобувачі освіти та представники третіх сторін несуть відповідальність за порушення вимог ІБ Університету згідно з чинним законодавством України.

Усі підрядники та представники третіх сторін (за необхідності) проходять належне навчання для поінформованості та регулярно отримують оновлені дані щодо політик і процедур Університету, ознайомлення з якими є необхідним для виконання покладених на них зобов'язань відповідно до укладених договорів.

Працівники, підрядники та представники третіх сторін погоджують і підписують документи Університету, які встановлюють взаємну відповідальність щодо ІБ.

Працівники, підрядники та представники третіх сторін повертають усі отримані від Університету ресурси, що перебувають у їх розпорядженні для підтримки належного рівня ІБ, після припинення їхнього найму, контракту чи угоди.

Розділ 6. Перегляд документа

Політика набирає чинності на наступний робочий день з дати затвердження рішенням Вченої Ради Університету.

Підрозділ ІБ проводить роботи щодо підтримки Політики в актуальному стані. Політика переглядається за необхідністю, але не рідше ніж один раз на рік.

Наступна/нова редакція Політики затверджується рішенням Вченої Ради Університету або комісії Вченої Ради Університету з питань інформатизації. Попередня редакція Політики втрачає свою чинність з дати набрання чинності наступної/нової редакції цього документа або на підставі рішення Вченої Ради Університету.

У разі невідповідності будь-якої частини Політики чинному законодавству України або нормативно-правовим актам Міністерства освіти і науки України, Політика діє лише в тій частині, яка їм не суперечить.

Внесення змін/доповнень до Політики ІБ здійснюється у таких випадках:

- при змінах у законодавчих, регуляторних та інших нормах;
- при змінах у документах, на підставі яких розроблено Політику;
- при впровадженні нових документів, що змінюють/впливають на процеси, описані в Політиці;
- при зміні ролей, відповідальності та процесів, що встановлює Політика;
- при змінах в інформаційній інфраструктурі та/або впровадженні нових ІТ.

Зміни та доповнення до цього документу набувають чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Вченої Ради Університету або комісії Вченої Ради Університету з питань інформатизації. Усі зміни та доповнення до цього документу є його невід'ємною частиною.