ПОРІВНЯЛЬНА ТАБЛИЦЯ ЗМІН ДО
ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЧЕРНІВЕЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Пункт/Розділ політики	**Чинна редакція (22.12.2025)**	**Пропонована редакція**	**Обґрунтування зміни**
Розділ 2, пункт 2.1.7	2.1.7. Документ Політики - додатковий нормативно-розпорядчий документ, який регламентує заходи Політики у межах окремих процесів та/або інформаційних систем (сервісів) Університету;	*Викласти у такій редакції:* 2.1.7. Документ Політики — спеціальний нормативно-розпорядчий документ Університету, який регламентує комплекс заходів інформаційної безпеки для окремої інформаційної системи у випадках, прямо передбачених законодавством України або за окремим рішенням керівника ЦЦТ;	Уточнення статусу «Документа Політики» як спеціального акта для окремої системи (замість обов'язкового документа під кожну ІС).
Розділ 2, доповнення пунктом 2.1.32	Додати визначення технічного регламенту інформаційної безпеки	*Доповнити розділ 2 пунктом 2.1.32 такого змісту:* 2.1.32. Технічний регламент інформаційної безпеки — нормативно-розпорядчий документ Університету, який встановлює єдині технічні та організаційні правила захисту інформації для ІТ-інфраструктури Університету в цілому або для окремих наскрізних технологічних процесів (резервне копіювання, управління доступом, ізоляція середовищ тощо);	Розмежування понять «Документ Політики» та «Технічний регламент інформаційної безпеки» для узгодження з розділом 4 Політики.
Розділ 3, підрозділ 3.4,	Додати правило щодо заборони передачі облікових даних та особистих ключів КЕП	*Доповнити підрозділ 3.4 пунктом 3.4.9 такого змісту:*	Закріплення персональної відповідальності працівників за дії в інформаційних системах, дотримання

доповнення пунктом 3.4.9		3.4.9. Працівникам Університету Забороняється передавати іншим особам паролі, особисті ключі електронного підпису, коди та інші засоби підтвердження автентифікації, а також надавати можливість виконувати дії від імені іншого користувача.	вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та запобігання несанкціонованому доступу до інформаційних активів Університету.
Розділ 4, пункти 4.1–4.3	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 (перелік із 11 блоків вимог).	*Пункти 4.1–4.2 викласти у такій редакції:* 4.1. Для деталізації положень цієї Політики можуть розроблятися технічні регламенти інформаційної безпеки Університету (щодо управління доступом, резервного копіювання та аварійного відновлення, ізоляції середовищ розробки, криптографічного захисту тощо), дія яких поширюється на всі інформаційні системи, групи систем або окрему систему Університету. 4.2. Розроблення окремого Документа Політики для конкретної інформаційної системи здійснюється виключно у випадках, прямо передбачених законодавством України або за вмотивованим рішенням керівника ЦЦТ. *Пункт 4.3 викласти у такій редакції:* Вимоги інформаційної безпеки можуть установлюватися спільними регламентами для всієї ІТ-інфраструктури, груп інформаційних систем або окремих	Усунення надлишкового бюрократичного навантаження та формальних ризиків під час зовнішніх перевірок, оскільки інформаційні системи Університету працюють на спільній серверній інфраструктурі та захищаються єдиними технічними регламентами.

		технологічних процесів Повторне викладення однакових вимог у документації кожної системи не вимагається. Для кожної системи фіксуються відповідальні особи, застосовні регламенти та спеціальні вимоги, зумовлені законодавством, профілем безпеки і результатами оцінювання ризиків	
Розділ 5, пункт 5.1.4	5.1.4. ЦЦТ веде реєстр ІС, які підлягають документуванню, а також розробляє відповідні документи Політики;	*Викласти у такій редакції:* 5.1.4. ЦЦТ визначає перелік технічних регламентів інформаційної безпеки, необхідних для забезпечення безперервності та захищеності ІТ-інфраструктури Університету, та забезпечує їх актуалізацію;	Скасування обов'язку ведення окремого формального реєстру інформаційних систем на користь управління єдиними технічними регламентами ІБ.
Розділ 5, пункт 5.1.8	5.1.8. Документи Політики розробляються адміністраторами ІС (ЦЦТ, режимно-секретним відділом та іншими структурними підрозділами Університету) і затверджуються ректором;	*Викласти у такій редакції:* 5.1.8. Технічні регламенти інформаційної безпеки розробляються ЦЦТ (а в частині режимно-секретної роботи - режимно-секретним відділом) і затверджуються наказом ректора Університету;	Узгодження порядку розроблення та затвердження обох видів внутрішніх нормативних документів ІБ.