УКРАЇНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»

Н А К А З

20.02.2025 м. Чернігів № 36/ВС

Про затвердження плану дій
на випадок несанкціонованого
доступу до персональних даних,
пошкодження технічного обладнання,
виникнення надзвичайних ситуацій

Відповідно до пункту 3.1., абзацу четвертого пункту 3.4. Типового порядку обробки персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини 08 січня 2014 року № 1/02-14

НАКАЗУЮ:

1. Затвердити план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій (далі – План дій), що додається.

2.Керівникам структурних підрозділів забезпечити виконання Плану дій.

3. Контроль за виконанням цього наказу залишаю за собою.

Ректор О.О.Новомлинець

Проєкт наказу вносить
Начальник відділу кадрів
_____В.В.Музика

ЗАТВЕРДЖЕНО
Наказом ректора
від «____»_____ р. № _____

П Л А Н
дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій

Національний університет «Чернігівська політехніка» вживає заходи щодо забезпечення захисту персональних даних на всіх етапах їхньої обробки, за допомогою організаційних та технічних заходів, спрямованих на запобігання втрати, знищення, витоку, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Загроза	**Дії працівника**
Несанкціонований доступ до персональних даних	Користувач автоматизованої системи (АС), у якій обробляються персональні дані, при виявленні спроби або факту несанкціонованого доступу повинен виконати такі дії: – припинити роботу з АС та не виконувати жодних додаткових операцій, які можуть призвести до змін у системі; – зробити скріншоти або зафіксувати підозрілу активність (якщо можливо) для подальшого аналізу; – негайно повідомити адміністратора безпеки АС та передати йому детальну інформацію про час та дату виявлення інциденту, описати підозрілі дії або зміни у системі, власні дії до моменту виявлення загрози та вказати на потенційного зловмисника (якщо є підозри); – дотримуватися вказівок адміністратора АС, який проводить розслідування; – не розголошувати інформацію про інцидент стороннім особам, окрім уповноважених осіб. Дії працівників при роботі з паперовими базами персональних даних (картотеки) у випадку виявлення несанкціонованого доступу до картотек: – негайно припинити будь-яку роботу з документами; – повідомити відповідального за захист персональних даних або адміністрацію університету; – зафіксувати обставини інциденту (час, місце, можливих свідків); – якщо є підозра на викрадення або пошкодження документів, викликати охорону або правоохоронні органи; – якщо документ знайдено у сторонніх осіб, зафіксувати факт та передати інформацію керівництву; – провести аудит втрачених даних;

	– обмежити доступ до картотеки до завершення розслідування; – дочекатися інструкцій від відповідальних осіб щодо подальших дій. Після завершення внутрішнього розслідування причин та наслідків інциденту: – визначаються необхідні заходи для усунення наслідків та запобігання повторенню порушень; – здійснюється оновлення політик безпеки та інструктаж персоналу.
Пошкодження технічного обладнання	Якщо користувач виявив несправність обладнання АС (комп'ютера, сервера, принтера тощо), необхідно: – припинити роботу з пристроєм; – не намагатися самостійно ремонтувати або змінювати конфігурацію обладнання; – якщо пристрій працює нестабільно, не відкривати персональні дані; – повідомити адміністратора АС про характер проблеми та дочекатися від нього інструкцій щодо подальших дій. Після ремонту слід перевірити цілісність персональних даних й коректність роботи обладнання та повідомити адміністратора АС про будь-які відхилення.
Природні катастрофи або техногенні аварії	У випадку настання природних катастроф або техногенних аварій: – негайно припинити роботу з персональними даними та вимкнути комп'ютери, зачинити картотеки у сховища; – покинути приміщення згідно з планом евакуації; – унеможливити неконтрольований доступ до приміщень, де зберігаються носії персональних даних; – повідомити керівництво або відповідальних за безпеку. Дії у випадку пошкодження паперових документів: – за можливості зробити копії пошкоджених документів; – якщо пошкоджені дані критично важливі, негайно повідомити адміністрацію для вжиття заходів із відновлення; – при необхідності провести додатковий аудит картотеки.

Відповідальна особа за організацію роботи,
пов'язаною із захистом персональних даних,

начальник юридичного відділу О.Г. Вершняк

Керівник служби захисту інформації в АС університету С.М. Семендяй