«ЗАТВЕРДЖУЮ»
в.о. ректора Прикарпатського національного
університету імені Василя Стефаника
Ігор ЦЕПЕНДА
«24» грудня 2024 року

ПЛАН ДІЙ
працівників Прикарпатського національного університету імені Василя Стефаника на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій

1. План дій працівників Прикарпатського національного університету імені Василя Стефаника на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій (далі – План) розроблено для регламентування організаційно-технічних заходів у разі виникнення позаштатних ситуацій при обробці персональних даних в Прикарпатському національному університеті імені Василя Стефаника (далі – Університет).

2. План є обов'язковим до виконання працівниками Університету, які мають доступ до персональних даних, та обробляють їх у межах виконання ними своїх посадових обов'язків, у тому числі в інформаційних системах Університету.

3. У разі виникнення позаштатних ситуацій при обробці персональних даних в Університеті працівники Університету зобов'язані неухильно дотримуватися алгоритму дій, наведеного у таблиці:

№ з/п	Подія	Дії працівників / відповідальних осіб / структурних підрозділів
1.	Спроба несанкціонованого доступу або виявлення ознак несанкціонованого доступу до персональних даних на паперових носіях	**Працівники** зобов'язані: 1. негайно припинити обробку персональних даних; 2. повідомити безпосереднього керівника; 3. необхідно зберегти всі документи та матеріали, які можуть бути використані як докази; 4. до місця, де виявлено ознаки несанкціонованого доступу, необхідно обмежити доступ сторонніх осіб;

		5. необхідно визначити, які саме персональні дані могли бути розголошені або пошкоджені; 6. необхідно провести внутрішнє розслідування для встановлення причин інциденту та розробки заходів для усунення його наслідків.
1.	Спроба несанкціонованого доступу або виявлення ознак несанкціонованого доступу до персональних даних в інформаційних системах, підозра на компрометацію доступу до інформаційних систем, кваліфікованих електронних підписів працівників Університету або їх компрометація, підозра на витік інформації або її витік з технічних причин (злом облікового запису працівника Університету, виявлення сторонніх пристроїв в інформаційній системі тощо)	**Працівники** зобов'язані: 1. негайно припинити обробку персональних даних; 2. повідомити безпосереднього керівника; 3. повідомити інформаційно-обчислювальний центр та інших суб'єктів надавачів відповідних послуг **Інформаційно-обчислювальний центр** зобов'язаний: 1. провести попередній аналіз ситуації, з'ясувати причини виникнення позаштатної ситуації; 2. провести перевірку вірогідності проникнення несанкціонованого програмного забезпечення в інформаційну систему; 3. здійснити блокування та/або скасування сертифікатів відкритих ключів відповідно до встановленого порядку (за потреби); 4. довести до відома керівництва Університету та відповідальної особи за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних; 5. здійснити заходи щодо усунення виявлених недоліків.
2.	Зараження програмного забезпечення та носіїв інформації, за допомогою яких здійснюється	**Працівники** зобов'язані: 1. негайно припинити обробку персональних даних; 2. вимкнути робочу станцію від електроживлення;

	обробка персональних даних комп'ютерними вірусами	3. повідомити безпосереднього керівника; 4. повідомити інформаційно-обчислювальний центр. **Інформаційно-обчислювальний центр** зобов'язаний: 1. провести попередній аналіз ситуації, з'ясувати причини виникнення позаштатної ситуації; 2. відключити уражені комп'ютери від сегментів інформаційної системи; 3. організувати перевірку складових інформаційних систем засобами антивірусного захисту та відновлення ушкоджених / заражених комп'ютерним вірусом складових інформаційної системи; 4. довести до відома керівництва Університету та відповідальної особи за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних; 5. розробити план реагування на позаштатну ситуацію в інформаційних системах (за потреби); 6. організувати проведення заходів щодо відновлення працездатності інформаційної системи; 7. провести роз'яснювальну роботу (інструктаж, навчання тощо) з відповідними працівниками Університету. 8. у разі необхідності повідомити про позаштатну ситуації Департамент кіберполіції Національної поліції України в Івано-Франківській області.

3.	Вчинення працівниками випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних тощо	**Працівники** зобов'язані: 1. припинити обробку персональних даних; 2. повідомити безпосереднього керівника; 3. довести до відома керівництва Університету та відповідальної особи за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних.
4.	Збій в роботі інформаційних систем, комп'ютерного та мережевого обладнання, за допомогою яких здійснюється обробка персональних даних.	**Працівники** зобов'язані: 1. негайно припинити обробку персональних даних; 2. повідомити безпосереднього керівника; 3. повідомити інформаційно-обчислювальний центр. **Інформаційно-обчислювальний центр** зобов'язаний: 1. провести попередній аналіз ситуації, з'ясувати причини виникнення позаштатної ситуації; 2. довести до відома керівництво Університету та відповідальної особи за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних; 3. розробити план реагування на позаштатну ситуацію (за потреби); 4. організувати проведення заходів щодо відновлення працездатності інформаційної системи; 5. провести технічне обслуговування та/або ремонт складових відповідно до заявки на проведення додаткових робіт з технічними засобами (за потреби);

		6. провести роз'яснювальну роботу (інструктаж, навчання тощо) з відповідними працівниками Університету.
5.	Виявлення пошкодження, втрати, викрадення, фактів незаконної обробки або знищення документа чи іншого носія персональних даних або спроби несанкціонованого доступу до персональних даних	**Працівники** зобов'язані: 1. припинити обробку персональних даних; 2. повідомити безпосереднього керівника; 3. довести до відома керівництва Університету та відповідальної особи за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних
6.	Настання надзвичайної ситуації (пожежа, вибух в адміністративній будівлі або на території Університету, підтоплення в період паводку або проливних дощів, прориву системи теплопостачання, водопостачання, водовідведення, осідання ґрунту з частковим обваленням адміністративної будівлі, удар блискавки, сильні морози тощо)	**Працівники** зобов'язані: 1. негайно припинити обробку персональних даних; 2. вимкнути робочу станцію, комп'ютерне обладнання від електроживлення; 3. повідомити безпосереднього керівника та/або відповідального з питань цивільного захисту в Університеті; 4. вжити заходів для збереження носіїв персональних даних осіб від втрати та пошкодження (за наявної можливості та у спосіб, що не загрожує життю та здоров'ю працівників); 5. діяти згідно з Планом реагування на надзвичайні ситуації Університету та Внутрішньою інструкцією щодо дій працівників Університету в умовах надзвичайних ситуацій. **Відповідальна особа з питань цивільного захисту та надзвичайних ситуацій в Університеті** зобов'язана: 1. організувати оповіщення відповідних служб реагування;

		2. довести до відома керівництва Університету та відповідальної особи за організації роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних.

4. Про всі випадки позаштатних ситуацій при обробці персональних даних, що наведені у пункті 3 цього Плану, та/або інші випадки, що призвели до пошкодження, псування, несанкціонованого доступу, знищення, поширення тощо персональних даних, працівник, який виявив даний факт, та його безпосередній керівник невідкладно письмово повідомляють про подію керівництво Університету та Відповідальну особу за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних.
5. Після отримання повідомлення Відповідальна особа за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних, за необхідності, за фактами порушень режиму захисту персональних даних звертається до керівництва Університету про проведення службового розслідування.
6. Вимоги Відповідальної особи за організацію роботи з обробки персональних даних та дотримання законодавства у сфері захисту персональних даних є обов'язковими для всіх працівників Університету, які здійснюють обробку персональних даних.

Начальник відділу кадрів Орест СМІШКО

«20» грудня 2024 року