

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Положення
про автоматизовану систему
«Єдина Державна Електронна База з питань Освіти»
університету

м. Харків - 2013

ЗМІСТ

	ЗАГАЛЬНІ ПОЛОЖЕННЯ	
1	ВИЗНАЧЕННЯ ТЕРМІНІВ	
2	РОБОТА З ЄДЕБО-КЛІЄНТ ВІДПОВІДАЛЬНОЇ ОСОБИ УНІВЕРСИТЕТУ	
2.1	Заява навчального закладу на реєстрацію в Єдиній державній електронній базі з питань освіти	
2.2	Авторизація Університету в ЄДЕБО	
3	ДАНІ	
3.1	Основні дані	
3.2	Попередження	
3.3	Ліцензії Університету	
3.4	Рейтинги	
3.5	Структура	
3.6	Звіти	
4	ДОВІДНИКИ	
4.1	Спеціалізації	
4.2	Квоти	
4.3	Факультет ДП (факультет довузівської підготовки)	
4.4	Довідники ЄДЕБО	
5	АДМІНІСТРУВАННЯ	
5.1	Користувачі	
5.2	Групи користувачів	
6	ВСТУП	
6.1	Пропозиції	
6.2	Заяви	
6.3	Списки рекомендованих	
6.4	Накази	
7	НАВЧАЛЬНИЙ ПРОЦЕС	
7.1	Групи	
7.2	Студенти	
7.3	Накази по студентам	
7.4	Замовлення документів про освіту державного зразка	
7.5	Форма № 2-3 НК	
8	ТЕХНІЧНА ПІДТРИМКА	
9	ФІНАНСУВАННЯ	
10	ВІДПОВІДАЛЬНІСТЬ	
11	ДОДАТКИ	

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Положення про функціонування (далі - Положення) Програмного комплексу «Єдина Державна Електронна База з питань Освіти» (далі – ПК ЄДЕБО) з метою вдосконалення роботи комплексу в умовах Національного технічного Університету «Харківський політехнічний інститут» (далі - Університет)

Єдина Державна Електронна База з питань Освіти (ЄДЕБО) - автоматизована система накопичення, оброблення, зберігання та захисту даних, у тому числі персональних, щодо закладів здійснюючих освітні послуги в Україні.

Для забезпечення функціонування ПК ЄДЕБО створена автоматизована система ЄДЕБО Університету (далі – АС ЄДЕБО). Структура АС ЄДЕБО Університету наведено у Додатку 1.

1) Використання бази

Дані з цієї бази використовуються під час виготовлення:

- документів про освіту державного зразка;
- документів про вчені звання та наукові ступені;
- ліцензій на надання освітніх послуг та сертифікатів про акредитацію;
- учнівських (студентських) квитків;
- для отримання інших відомостей інформаційного характеру та обробки статистичних даних в інтересах навчальних закладів, установ освіти для здійснення контролю та прийняття управлінських рішень.

2) Дотримання законодавства про захист особових даних

Відповідно до чинного законодавства України (Закон України «Про захист персональних даних» від 1 червня 2010 р.) для включення відомостей про людину в електронну базу необхідно отримати її згоду. У навчальному закладі повинен бути забезпечений адміністративно-організаційний механізм збору та зберігання документів - персональні згоди на обробку відповідних даних в ЄДЕБО.

3) Власник та адміністратор

Власником (утримувачем) ЄДЕБО є Міністерство освіти і науки, молоді та спорту України (МОНМСУ), **адміністратором (розпорядником) ЄДЕБО** є державне підприємство «Інфоресурс», що належить до сфери управління МОНМСУ.

4) Організація роботи з ЄДЕБО

Для роботи з програмою необхідні базові навички користувача *Windows* (володіння програмними засобами *Microsoft Word* та *Microsoft Excel*).

Для роботи користувачів найкращі результати досягаються при використанні веб-браузера *Google Chrome*.

Реалізовані наступні елементи для роботи з програмою:

- повідомлення. Отримання службових повідомлень від ЄДЕБО;
- налаштування. Ви маєте можливість провести деякі налаштування, обрати тему, в якій буде комфортніше за все працювати.
- завантаження інформації, розміщеної в ЄДЕБО для користувачів;
- інформація про поточну робочу версію програми;
- допомога. Виклик довідкової програми.

До цього Положення увійшли основні вимоги інструкції WEB-КЛІЄНТУ Програмного комплексу (далі - ПК ЄДЕБО), Договору про надання технічних послуг з державним підприємством (ДП) «Інфоресурс» та керівних документів МОНМСУ.

Примітка:

По мірі розвитку Програмного комплексу (ЄДЕБО) та наповнення його новими функціями і завданнями, це Положення буде доповнюватися та коригуватися.

1. ВИЗНАЧЕННЯ ТЕРМІНІВ

Єдина державна електронна база з питань освіти (далі – ЄДЕБО) - автоматизована система збирання, верифікації, оброблення, зберігання та захисту даних, у тому числі персональних, щодо надавачів та отримувачів освітніх послуг з метою забезпечення потреби фізичних та юридичних осіб.

Програмні засоби доступу до ЄДЕБО (ПЗ ЄДЕБО) — сукупність криптографічного програмного забезпечення та програм (програмних комплексів, автоматизованих систем, інтерфейсів сполучення комп'ютерних програм з базами даних, тощо) що забезпечують можливість роботи з даними ЄДЕБО, а саме: внесення, використання, оновлення, редагування та видалення даних.

Адміністратор ПЗ ЄДЕБО – уповноважений Ректором Університету штатний працівник, відповідальний за створення облікових записів Операторів ПЗ ЄДЕБО, взаємодію з Розпорядником ЄДЕБО щодо організації та підтримання захищеного з'єднання з ЄДЕБО за допомогою криптографічного програмного забезпечення.

Компрометація – будь-який випадок (втрата, розголошення, крадіжка, несанкціоноване копіювання тощо) з ключовими документами (ключовими даними) та засобами комплексного захисту інформації, який призвів (може призвести) до розголошення (витоку) інформації про них, а також інформації, яка обробляється та передається.

Криптографічне програмне забезпечення – комплекс із захисту з'єднань при передачі даних по незахищеним каналам.

Оператор ПЗ ЄДЕБО – уповноважений Ректором Університету штатний працівник, відповідальний за внесення/редагування повних та достовірних даних до/в ЄДЕБО.

Організація доступу до ЄДЕБО – сукупність адміністративно-технічних заходів Розпорядника ЄДЕБО, спрямованих на створення можливості підключення Навчального закладу до ЄДЕБО.

Параметри доступу до ЄДЕБО – IP-адреса для роботи в ЄДЕБО, логін та пароль Адміністратора ПЗ ЄДЕБО або/та Оператора ПЗ ЄДЕБО.

Підтримання доступу до ЄДЕБО – вжиття Розпорядником ЄДЕБО технічних заходів протягом строку дії Договору, спрямованих на надання можливості доступу Університету до ЄДЕБО.

Секретний ключ – елемент криптографічного захисту, який використовується при роботі криптографічного програмного забезпечення та однозначно ідентифікує Адміністратора АС ЄДЕБО або/та Оператора АС ЄДЕБО.

Робоче місце Оператора – комплекс засобів автоматизації, використання яких дозволяє Оператору виконувати функціональні обов'язки.

Інші терміни вживаються у значенні, наведеному в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 та Положенні про Єдину державну електронну базу з питань освіти, затвердженому постановою Кабінету Міністрів України від 13 липня 2011 р. № 752.

2. РОБОТА З ЄДЕБО-КЛІЄНТ ВІДПОВІДАЛЬНОЇ ОСОБИ УНІВЕРСИТЕТУ

2.1. Заява Університету на реєстрацію в ЄДЕБО

Для реєстрації Університету в ЄДЕБО надсилається заява (з відповідними додатками – встановленої форми), яка підписана Ректором та завірена печаткою Університету (відокремленого структурного підрозділу).

2.2. Авторизація Університету в ЄДЕБО

Для Авторизації Університету в ЄДЕБО у відповідне вікно програми вводяться отримані з електронної пошти reg@edbo.gov.ua логін та пароль. У подальшій роботі використовується новий – особистий пароль.

В разі помилкового вводу паролю більше ніж 5 спроб користувача з даним логіном вхід в систему буде автоматично заблоковано!

Розблокування здійснюється технічної підтримки ЄДЕБО.

Примітка:

Особам, працюючим з ЄДЕБО слід розуміти, що всі введені дані є відомостями, які підлягають спеціальному зберіганню відповідно до Закону України «Про захист персональних даних» від 1 червня 2010 р. Їх створення та несанкціоноване розповсюдження тягнуть за собою відповідальність згідно з чинним законодавством України. Допуск осіб, працюючих з ЄДЕБО (операторів), повинен бути суворо регламентованим адміністративними заходами навчального закладу. Паролі операторів повинні бути строго персоналізовані (ОДИН ОПЕРАТОР – ОДИН ПАРОЛЬ). Розголошення паролів іншим особам є неприпустимим. Паролі повинні періодично змінюватись. Якщо Ви забули свій пароль, виконайте необхідні дії по його відновленню, після чого на Ваш e-mail прийде повідомлення з новим паролем.

3. ДАНІ

3.1. Основні дані

Дані, необхідні для роботи Університету в ЄДЕБО, вводяться на вкладці «Навчальний заклад».

3.1.1. Верифікація документів, що підтверджують освітню діяльність Університету

Верифікація документів - перевірка (підтвердження) даних щодо Університету.

Верифікація проводиться у вигляді надання документів, що підтверджують освітню діяльність Університету, повноваження його керівництва та відповідальних осіб. Документи повинні бути оформлені належним чином, відповідно до вимог діловодства.

Примітка:

Після верифікації документу внести зміни буде неможливим, тому перед відправленням на верифікацію необхідно перевірити правильність внесених даних. У разі виникнення необхідності щодо внесення змін – зверніться з запитом до технічної підтримки.

3.1.2. Редагування даних Університету

Після проходження верифікації та заповнення всіх зазначених параметрів достовірними, правдивими та перевіреними даними вікно «Основні дані» має вигляд:

The screenshot shows a web interface for editing university data. The title is '(00104) Національний технічний університет "Харківський політехнічний інститут"'. There are three tabs: 'Редагувати дані' (selected), 'Акредитація', and 'Підпорядковані'. The left sidebar contains a navigation menu with categories: 'Дані' (Basic Data), 'Довідники' (Reference), 'Адміністрування' (Administration), and 'Вступ' (Admission). The main content area displays the following information:

Повна назва закладу	Національний технічний університет "Харківський політехнічний інститут"
Скорочена назва закладу	НТУ "ХПІ"
Підпорядкування	Міністерство освіти і науки, молоді та спорту України
Форма власності	Державний
Тип навчального закладу	вищий навчальний заклад III-IV рівня акредитації
Код ЕДРПОУ	02071180
Дата заснування	1 янвря 1885 г.
Фактична адреса:	Поштовий індекс: 61002 ХАРКІВСЬКА ОБЛАСТЬ, ХАРКІВ, вулиця Фрунзе, 21
Юридична адреса:	Поштовий індекс: 61002 ХАРКІВСЬКА ОБЛАСТЬ, ХАРКІВ, вулиця Фрунзе, 21
Телефон	+3 (057)700-15-64
Адреса електронної пошти	cmsroot@kpi.kharkov.ua
Адреса інтернет-сайту закладу	http://www.kpi.kharkov.ua/
ПІБ керівника закладу	Товалюкянський Лесюнд Леонідович
Телефон керівника закладу	+3 (057)700-15-64
Адреса електронної пошти керівника закладу	cmsroot@kpi.kharkov.ua
Рівень акредитації	III-IV
Доступ до навчального закладу	
Якому навчальному закладу підпорядкований (00000)	

Примітка:

Навчальним закладом нижчого рівня обов'язково заповнюється поле щодо підпорядкування навчального закладу головному ВНЗ.

3.2. Попередження

Дана вкладка показує всі попередження, що виникають в процесі роботи з ЄДЕБО. Наприклад, таке попередження виникає на етапі, коли документи Університету ще не пройшли верифікацію.

3.3. Ліцензії

Вкладка «Ліцензії» складається з трьох таблиць:

- ліцензії навчального закладу;
- дані ліцензії;
- дані верифікації ліцензії.

3.3.1. Ліцензії Університету

Після заповнення даних, визначених у таблиці, буде відображено інформацію по даному документу – «Параметри ліцензії».

Примітка:

Якщо ліцензія однакова для головного та підпорядкованих навчальних закладів, вона вноситься кожним навчальним закладом з відповідними додатками (обмеження, що були встановлені раніше, зняті).

Примітка:

На робочій панелі «Копіювати», є можливість копіювати ліцензію, що вже була занесена до системи. Це необхідно у випадку, коли навчальний заклад отримав таку ж ліцензію, але з незначними змінами. Копіювання дає можливість не заносити всі дані заново, а лише внести корективи.

3.3.2. Дані ліцензії

До таблиці «Дані ліцензії» вноситься інформація з додатків до ліцензії (з урахуванням підрозділу, який відповідає за напрям (О.К.Р. *бакалавр*) та спеціальність (О.К.Р. *молодший спеціаліст, спеціаліст, магістр*).

У Довідниках інформацію щодо кодів напрямів та спеціальностей внесено згідно діючих керівних документів, а саме:

Переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра, затвердженого постановою Кабінету Міністрів України від 27 серпня 2010 р. № 787 (останні зміни – ПКМУ № 227 від 21.03.2012); / <http://zakon1.rada.gov.ua/laws/show/787-2010-%D0%BF/>

Переліку напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра, затвердженого постановою Кабінету Міністрів України від 13 грудня 2006 р. № 1719 (останні зміни – ПКМУ № 576 від 01.06.2011); / <http://zakon1.rada.gov.ua/laws/show/1719-2006-%D0%BF/print1343207203966705/>

Переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем молодшого спеціаліста, затвердженого постановою Кабінету Міністрів України від 20 червня 2007 р. № 839 (останні зміни – ПКМУ № 365 від 26.05.2010); / <http://zakon1.rada.gov.ua/laws/show/839-2007-%D0%BF/>

наказу Міністерства освіти і науки, молоді та спорту України від 9 листопада 2010 року № 1067 «Про введення в дію переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра, затвердженого постановою Кабінету Міністрів України від 27 серпня 2010 р. № 787» / <http://document.ua/pro-vvedennja-v-diyu-pereliku-specialnostei-za-jakimi-zdiisn-doc38057.html> /, у якому затверджено:

таблицю відповідності спеціальностей переліку 2010 напрямам підготовки переліку 2006 (згідно з додатком 1);

таблицю зіставлення спеціальностей освітньо-кваліфікаційних рівнів спеціаліста і магістра за переліком 1997 і переліком 2010 (згідно з додатком 2);

даних Додатків № 1 та 2 до Умов прийому до вищих навчальних закладів України, затверджених наказом Міністерства освіти і науки, молоді та спорту України від 12 жовтня 2011 р. №1179. / <http://zakon1.rada.gov.ua/laws/show/z1221-11/>

керівних документів інших міністерств та відомств.

Постанови Кабінету Міністрів України та накази Міністерства освіти і науки, молоді та спорту України також розміщено на сайті ДП «Інфоресурс» в розділі «Правове поле» (infosurs.gov.ua/prav_pol.html).

У вікно «**Кількість місць**» внесіть ліцензований обсяг за даним напрямом (спеціальністю). Прийом студентів до Університету за одним напрямом (спеціальністю) здійснюється кількома підрозділами, включеними до його структури, керівництво Університету розподіляє ліцензований обсяг між цими підрозділами (розподіл, за необхідності, можна буде корегувати під час вступної кампанії).

3.4.Рейтинги

У вкладці «**Рейтинги**» заповнюється інформація з метою виконання наказу МОНМСУ від 20.12.2011 р. № 1475 щодо національного рейтингового оцінювання діяльності вищих навчальних закладів

Вкладка «**Рейтинг**» складається з «**Таблиці рейтингів**» та «**Даних для верифікації**».

3.5.Структура

Дана вкладка необхідна для додання Університетом всіх підпорядкованих йому елементів, для структурних підрозділів. Інформація щодо **структури** автоматизованої системи ЄДЕБО (далі – АС ЄДБО) Університету використовується під час занесення **даних ліцензій** та подання **пропозицій на вступ** до Університету (мають значення надані підрозділу права щодо прийому заяв абітурієнтів, обліку студентів та співробітників).

До структури додаються всі структурні підрозділи (факультети, коледжі, центри, кафедри), які приймають участь у організації та проведенні навчального процесу зі студентами і є у підпорядкуванні Університету.

Структура робочих місць Операторів АС ЄДБО наведена у **Додатку 2**

3.6. Звіти

До вказаної вкладки завантажується необхідна звітна та статистична інформація, доступна до скачування.

На даний час формуються наступні звіти:

- **Журнал реєстрації осіб, які вступають до навчального закладу** (форма № Н-1.02), затверджений наказом Міністерства освіти і науки, молоді та спорту України від 29 березня 2012 р. № 384;
- **оперативні дані** за наступними формами, встановленими Міністерством освіти і науки, молоді та спорту України:

Зведені дані про результати прийому (форма № 1);

Інформація про результати прийому за напрямами підготовки і спеціальностями (форма № 2).

4. ДОВІДНИКИ

4.1. Спеціалізації

Вкладка служить для створення Університетом необхідних **спеціалізацій** до спеціальностей.

Внесення спеціалізацій не є обов'язковим та здійснюється за необхідності.

Всі спеціалізації, створені Університетом, включаються до загальної бази.

*Для напрямів **освітньо-кваліфікаційний рівень**.(далі - **О.К.Р.**) **бакалавр спеціалізації не створюються.** У разі необхідності їх введення створить потрібну спеціалізацію для спеціальності (**О.К.Р. спеціаліст, магістр**), спорідненої з напрямом*

Для внесення спеціалізації, у даному вікні зазначаються:

- № створеної спеціалізації;
- статус документу;
- дата створення/зміни.

Примітка:

Назва спеціалізації не може співпадати з назвою спеціальності.

Для кожної спеціальності одну й ту ж спеціалізацію можна внести лише один раз

4.2. Квоти

Вкладка служить для занесення Університетом, типів **квот цільового прийому**, встановлених у ньому на вступ для визначених категорій абітурієнтів (наприклад, сільська молодь). **Обсяги квот цільового прийому** за кожним видом вносяться при створенні **пропозицій на вступ** (розділ 6).

Перелік квот визначений відповідно до *листа Міністерства освіти і науки, молоді та спорту України від 01.08.2011 р. № 1/9 – 582 «Про типову форму наказу про зарахування».*

Дані щодо **пільгових категорій** абітурієнтів в цій вкладці **не заносяться.**

ЄДБО передбачає наступні типи квот:

- 1) іноземні громадяни;
- 2) особи з сільської місцевості;

- 3) особи з прикордонної місцевості;
- 4) особи з обмеженими можливостями (вадами слуху);
- 5) інша квота.

4.3. Факультет ДП (факультет довузівської підготовки)

Цей розділ ЄДЕБО в умовах Університету реалізує Центр дистанційної та доуніверситетської підготовки (ЦДДП)

4.4. Довідники ЄДЕБО

В даному розділі знаходяться існуючі **довідники** «Єдиної державної електронної бази з питань освіти». Довідники регулярно оновлюються, за необхідності здійснюється корегування даних.

4.4.1. Вступні кампанії

Даний довідник відображає **вступні кампанії** за роками, формами навчання (денна, заочна, вечірня, екстернат, дистанційна) та термінами їх проведення.

4.4.2. Кваліфікаційні рівні

Даний довідник показує **освітньо-кваліфікаційні рівні (О.К.Р.)**, за якими здійснюється набір.

4.4.3. Напрями

Даний довідник показує всі **напрями** за **О.К.Р. «Бакалавр»**.

4.4.4. Олімпіади

Даний довідник показує додаткові бали для абітурієнтів за досягнення у Всеукраїнських учнівських олімпіадах та конкурсах.

4.4.5. Пільги

Даний довідник показує встановлені законодавством пільги для окремих категорій абітурієнтів.

4.4.6. Спеціалізації

В цьому довіднику відображені всі спеціалізації, що введені навчальними закладами та пройшли перевірку (у довіднику **«Спеціальності (загальний)»** представлені спеціальності разом з своїми спеціалізаціями).

4.4.7. Спеціальності

В даному довіднику розміщені всі спеціальності за **О.К.Р. «Спеціаліст»**, **«Магістр»** та **«Молодший спеціаліст»**.

4.4.8. Спеціальності (загальний)

В даному довіднику розміщені **всі існуючі** спеціальності (з відповідними кодом та назвою **галузі**, кодом та назвою **напрямку**, назвою **спеціалізації** (за наявності)).

4.4.9. Типи документів персон

В даному довіднику вказано **перелік документів**, які повинен надати **абітурієнт** при подачі **заяви на вступ** до навчального закладу (залежно від рівня освіти абітурієнта, напрямку (спеціальності) та умов вступу). В останній колонці статус **«1»** мають документи, на основі яких можливо подавати заяви на вступ.

4.4.10. Типи контактів персон

В даному розділі довідника вказані всі типи контактів, які можливо використовувати, при реєстрації абітурієнтів.

4.4.11. Форми навчання

В даному розділі довідника відображено форми навчання, за якими здійснюється занесення даних абітурієнтів.

5. АДМІНІСТРУВАННЯ

Відповідно до «ІНСТРУКЦІЇ WEB-КЛІЄНТУ Програмний комплекс «Єдина Державна Електронна База з питань Освіти» (ЄДЕБО) в Університеті визначена особа відповідальною за внесення відомостей та даних від Університету до Єдиної державної електронній бази з питань освіти (далі - Адміністратор), яка призначена наказом Ректора Університету від 29 грудня 2012 року № 632-І відповідно до якого вона здійснює обробку даних, зокрема персональних даних (далі – ПД), в веб-сервісі ЄДЕБО-клієнт.

Права та обов'язки Адміністратора визначені у «Інструкції Адміністратору АС ЄДЕБО Університету (Додаток - 3), по забезпеченню безпеки експлуатації програмного комплексу ЄДЕБО – клієнт».

У разі необхідності, Адміністратору надається можливість створення нового користувача ЄДЕБО.

5.1. Користувачі

В цьому розділі термін «Користувач» означає людину (відповідальну особу), яка отримує відповідні права для роботи з ЄДЕБО. Всі призначення осіб, які мають право безпосередньо працювати з ЄДЕБО, оформлені відповідними наказами по Університету (накази Ректора Університету від 21 травня 2012 року № 257-І, від 29 травня 2012 року № 266-І). У Університеті видані відповідні документи, де визначені структура системи ЄДЕБО Університету, перелік робочих місць, склад, права та обов'язки користувачів ЄДЕБО, керівників та відповідальних осіб, яким надано право призначати і усувати від роботи «Операторів».

Передача паролів стороннім особам (у тому числі і безпосереднім начальникам) категорично заборонена. Особа («користувач»), що вносить дані в ЄДЕБО, несе персональну відповідальність за свої дії і коректність внесених даних.

Будь-яка інформація що буде внесено до системи, повинна мати документальне підтвердження, відповідати прийнятим у ЄДЕБО форматам та бути узгодженою з Адміністратором

ВСІ ДІЇ користувача щодо введення та редагуванню даних в ЄДЕБО автоматично фіксуються.

Примітка:

Навіть при тимчасовому припиненні роботи з ЄДЕБО (користувач відходить від комп'ютера, з якого здійснено вхід в програму) слід припиняти сеанс роботи (вихід з програми) або виконувати блокування комп'ютера для недопущення несанкціонованого зчитування або редагування даних ЄДЕБО.

5.1.1. Користувачі (Оператори)

Права та обов'язки користувачів (операторів) визначені у «Інструкції Користувачу (Оператору) АС ЄДЕБО Університету по забезпеченню безпеки експлуатації програмного комплексу ЄДЕБО-клієнт» (Додаток - 4)

Вибір «Сертифікату» для користувача здійснюється, виходячи з способу його підключення:

- з **сертифікатом (підключення через клієнт криптозахисту)** – звичайне підключення додаткового **робочого місця** користувача (без шлюзу);
- **без сертифікату (підключення через шлюз)** - підключення додаткового **робочого місця** користувача у разі організації доступу Університету до ЄДЕБО за допомогою апаратно-програмного комплексу «ІТ Захист з'єднань-2. Проксі захисту»);
- **без сертифікату (підключення через SOAP шлюз)** - підключення **власної системи (програмного засобу)** Університету через програмний інтерфейс доступу до ЄДЕБО.

Ключова фраза голосової ідентифікації - слово, вираз, набір символів та цифр, що визначені користувачем в додатку до заяви на генерацію ключів та які будуть використовуватись при телефонному зв'язку в екстрених випадках.

«Роль» нового користувача можуть бути обраними із запропонованого списку відповідальною особою навчального закладу (рівень прав, що будуть надані користувачу).

Передбачено два типи показників «Ролі» – **Адміністратор** та **Оператор**.

Адміністратор - відповідальна особа навчального закладу, яка має права Оператора щодо внесення та редагування даних. Крім того, Адміністратор встановлює права доступу для Операторів та Користувачів.

Оператор - особа, яка має права щодо внесення та редагування даних.

За умовчанням передбачено три типи показників «Групи» – **Адміністратор, Оператор, Користувач**. У вкладці «Групи користувачів» Адміністратор навчального закладу має можливість створювати та змінювати групи, визначати їх права щодо доступу до інформації.

Всі користувачі несуть персональну відповідальність за результати своєї роботи з ЄДЕБО.

Примітка:

У такому сенсі «користувач» використовується тільки для показників «Групи», в інших випадках це узагальнене поняття.

В полі «Департамент» визначте структурний підрозділ, у якому працює користувач, в полі «Посада» - відповідно посаду, яку він займає.

В «E-mail» вкажіть адресу електронної пошти, що визначена користувачем в додатку до заяви на генерацію ключів, на яку новому користувачу прийде повідомлення щодо підключення до ЄДЕБО, а також, у разі необхідності, буде використовуватись для альтернативного зв'язку.

Відносно користувачів Адміністратор може виконувати наступні дії:

- 1) Редагувати** - В даних користувача змінювати роль, e-mail, номера телефонів та нотатки (пароль змінюється окремо).
- 2) Знищити** - Видалення облікового запису користувача. Після видалення запису користувач втрачає можливість роботи з ЄДЕБО.
- 3) Блокувати** - Адміністратор має можливість заблокувати створеного користувача. Цей користувач втрачає право роботи з базою (але не буде видалений з неї), в подальшому його можна допустити до роботи.

5.1.2. Верифікація

Верифікація користувачів Університету здійснюється за двома документами:

- заявка на генерацію ключів (**з додатками**);
- наказ про закріплення користувачів. _

5.2. Групи користувачів

У цій вкладці **Адміністратор** має можливість створювати та змінювати групи, визначати їх права щодо доступу до інформації.

Також **Адміністратор** має можливість заблокувати доступ до ЄДЕБО вибраній групі.

Для регулювання доступу до бази позначається, до якої інформації матимуть доступ члени групи:

6. ВСТУП

Розділ використовується, за необхідності коригується під час вступної кампанії та містить наступні складові:

6.1. Пропозиції

У цій вкладці Університет створює **пропозиції на вступ** до нього.

6.2. Заяви

Вкладка передбачена для занесення та обробки заяв абітурієнтів, що вступають до Університету.

6.3. Списки рекомендованих

У цій вкладці Університет створює конкурсні та рейтингові списки вступників за кожною пропозицією на вступ.

6.4. Накази

У цій вкладці Університет створює накази про зарахування до нього, а потім завантажується інформація на верифікацію.

Детальніше зміст цього розділу розкрито у Положенні про приймальну комісію

7. НАВЧАЛЬНИЙ ПРОЦЕС

7.1. Групи

У цій вкладці вноситься інформація щодо навчальних груп, до яких відносяться студенти. Розподіл до *навчальних груп* здійснюється у вкладці «Студенти».

Групи в таблиці розташовані за номером в ЄДЕБО, який надається автоматично. Для сортування груп натисніть на назву відповідного стовпця.

Додано можливість створення навчальних груп без деталізації ОКР (наприклад, для ОКР (загальний) «Молодий спеціаліст» можна об'єднати в групі студентів ОКР (детальний) «Молодий спеціаліст на основі повної ЗСО» та «Молодий спеціаліст на основі диплому кваліфікованого робітника»).

7.2. Студенти

У цій вкладці вноситься інформація щодо студентів навчального закладу, а також здійснюється додання нових студентів. Всі *студенти обов'язково* розподіляються до *навчальних груп*.

Вкладка «Студенти» складається з 3 розділів:

- **Студенти за групами** – включає студентів, які вже розподілені в ЄДЕБО до відповідних навчальних груп;
- **Студенти без груп** – включає студентів, не розподілених до навчальних груп;
- **Пошук студента** – здійснюється пошук студентів за їх ПІБ або номером у базі.

7.2.1. Студенти за групами

На вкладці відкривається таблиця з переліком **навчальних груп**, до яких вже розподілені студенти.

Встановлено наступні можливості внесення змін стану студентів протягом їх навчання (*детально – у розділі 7.3 «Накази по студентам»*):

- **відрахування** (в *особовій картці* студента встановлюється статус «**Відрахування**»);
- зміна джерела **фінансування** (державне замовлення, кошти фізичних (юридичних) осіб) (в *особовій картці* студента встановлюється статус «**Зміна фінансування**»);
- **переведення** у межах навчального закладу (зміна форми навчання, переведення до іншої групи тощо) (в *особовій картці* студента встановлюється статус «**Переведення**»);
- **довнесення** (введення в базу інформації щодо студентів, які вже навчаються у навчальному закладі (перейшли на наступний курс) (в *особовій картці* студента встановлюється статус «**Переведення на курс**»);
- **внесення** (введення в базу інформації щодо студентів, які зараховуються до навчального закладу *поза вступної кампанії*) (в *особовій картці* студента встановлюється статус «**Зарахування**»).

7.2.2. Студенти без груп

На вкладці відкривається таблиця з переліком *напрямів (спеціальностей)*, за якими є **студенти**, зараховані на навчання, але не розподілені до **навчальних груп**.

Після розподілу студента до навчальної групи він зникає з цього списку та, відповідно, з'являється в обраній групі у вкладці «**Студенти за групами**».

7.2.3. Пошук студента

Встановлено можливість здійснення пошуку студентів за їх **ПІБ** або його **номером** у базі.

7.3. Накази по студентам

У цій вкладці навчальний заклад створює накази щодо зміни стану студентів протягом їх навчання у цьому закладі.

Встановлено наступні **типи наказів по студентам**:

- **зарахування** студентів (*поза вступної кампанії*);
- **зміна джерела фінансування** навчання (державне замовлення, кошти фізичних (юридичних) осіб);
- **переведення** (*зміна ОКР, форми навчання, факультету, групи, спеціальності тощо*);
- **переведення на курс** (щодо студентів, які вже навчаються у навчальному закладі та перейшли на наступний курс);
- **відрахування** студентів та інші.

Взаємодію відділів та служб Університету щодо видання наказів по студентам в Університеті визначає «Методика підготовки, формування та видання наказів по студентам ...».

7.4. Замовлення документів про освіту державного зразка

Замовлення на виготовлення документів про освіту, студентських та учнівських квитків створюється за допомогою спеціалізованого програмного забезпечення ІВС “ОСВІТА”, згідно «Порядку замовлення, видачі та обліку документів про освіту державного зразка» затвердженого Наказом Міністерства освіти і науки України 10.12.2003 № 811

Виготовлення документів про освіту державного зразка, вчені звання та наукові ступені, ліцензій на надання освітніх послуг та сертифікатів про акредитацію, учнівських (студентських) квитків. Під час виготовлення зазначених документів використовуються лише дані, що містяться в ЄДЕБО (Постанова Кабінету Міністрів України від 13 липня 2011р. №752);

Відсутність даних про студентів в ЄДЕБО унеможливить виготовлення вказаних документів. (Лист ДП «Інфоресурс» від 14 грудня 2012р №1109)

7.5. Форма № 2-ЗНК

Форма державного спостереження №2-ЗНК «Звіт Університету на початок навчального року» (далі – Звіт) складається (згідно листа МОНмолодьспорту від 06.09.12 №1/9-633) за станом на *1 жовтня поточного року* за допомогою ЄДЕБО.

Інструкцію щодо заповнення форми № 2-ЗНК, затверджена наказами Держкомстату від 17.08.2004 р. № 483, та від 14.07.2010 р. № 276

Університет подає Звіт до органів статистики. У всіх розділах Звіту крім даних враховуються дані, отримані від *підпорядкованих* структурних підрозділів, що не мають статусу юридичної особи, незалежно від регіону їх розташування та форми навчання.

Інформацію про структурні підрозділи та основні показники їх діяльності (окремо по кожному) Університет наводить у *розділі XII* звіту, виділяючи її «у тому числі» із загальної інформації, наведеної у *розділі I*.

У Звіті не враховуються дані щодо слухачів *підготовчих курсів, підготовчих факультетів*, та студентів, які *відряджені для навчання* в інші країни, а також слухачів відділень (факультетів) *післядипломної освіти, перепідготовки та підвищення кваліфікації*.

До Звіту включаються дані про тих осіб, які здобувають *другу вищу освіту* на загальних засадах.

Інформація стосовно студентів з числа *іноземних громадян* та громадян країн колишнього СРСР наводиться у звіті тільки у *розділі XI*, а у *розділах I – X, XII* не враховується.

Дані щодо осіб, які навчаються за *дистанційною* та *екстернатною* формами, наводяться у Звіті, який складається за *заочною* формою навчання.

Студенти, які навчаються *другий рік на одному й тому ж курсі та не переведені*, незалежно від причин (неуспішність, академічна відпустка тощо), на початок навчального року на наступний курс, ураховуються у загальній кількості студентів.

Заповнення форми №2-ЗНК в Університеті здійснюють Адміністратор Університету або користувач навчального відділу.

8. ТЕХНІЧНА ПІДТРИМКА

8.1 Основні завдання технічної підтримки АС ЄДЕБО Університету є:

- Забезпечення працездатності робочих місць операторів структурних підрозділів Університету на рівні програмного забезпечення та технічних спроможностей комп'ютерної техніки;
- Організація (здійснення) ремонтних робіт щодо встановлення працездатності робочих місць операторів;
- Супроводження роботи відділів і служб Університету щодо підготовки інформації для вводу до ЄДЕБО;
- Проведення занять з операторами структурних підрозділів щодо вдосконалення їх знань, умінь та навичок по роботі з АС ЄДЕБО;
- Технічне обслуговування серверу АС ЄДЕБО Університету;
- Здійснення взаємодії з технічною підтримкою ПК ЄДЕБО у вирішенні конфліктів системи;
- Аналіз причин не працездатності робочих місць операторів і конфліктів програмного забезпечення ПК ЄДЕБО та АС ЄДЕБО Університету;
- Розробка пропозицій щодо вдосконалення роботи ПК ЄДЕБО та рекомендацій щодо роботи операторів структурних підрозділів Університету

8.2 Керівник групи технічної підтримки АС ЄДЕБО Університету є оператором АС ЄДЕБО Університету з правами адміністратора. Під час відсутності Адміністратора АС ЄДЕБО Університету він виконує обов'язки Адміністратора.

8.3 Склад групи технічної підтримки визначає Керівник ЦНІТ Університету за узгодженням з Адміністратором АС ЄДЕБО Університету.

Детальніше зміст цього розділу розкрито у Положенні про ЦНІТ Університету.

9. ФІНАНСУВАННЯ

9.1 Згідно Договору про надання технічних послуг з державним підприємством «Інфоресурс» Університет вартість послуг за наступними категоріями:

- організації доступу Навчального закладу до ЄДЕБО (1 робоче місце)
- підключення додаткового (одного) робочого місця для доступу до ЄДЕБО
- щоквартальної плати за послуги Розпорядника ЄДЕБО з підтримання доступу Університету до ЄДЕБО

9.2 Розмір щоквартальної плати за послуги Розпорядника ЄДЕБО з підтримання доступу Навчального закладу до ЄДЕБО на поточний календарний рік визначається залежно від кількості студентів, що навчались у Навчальному закладі станом на 1 жовтня попереднього календарного року (за даними форми державного статистичного спостереження № 2-ЗНК «Звіт вищого навчального закладу на початок навчального року», затвердженої наказом Державного

комітету статистики України від 14.07.2010 № 276) у розрахунку 0,36 грн. з урахуванням ПДВ за 1 (одного) студента.

9.3 Починаючи з 2013 року розмір щоквартальної плати за послуги Розпорядника ЄДЕБО з підтримання доступу Навчального закладу до ЄДЕБО встановлюється Сторонами окремо на кожний календарний рік шляхом підписання додаткової угоди до Договору.

10.ВІДПОВІДАЛЬНІСТЬ

10.1 Університет несе відповідальність за невиконання чи неналежне виконання умов Договору у порядку та межах, передбачених Договором та чинним законодавством України.

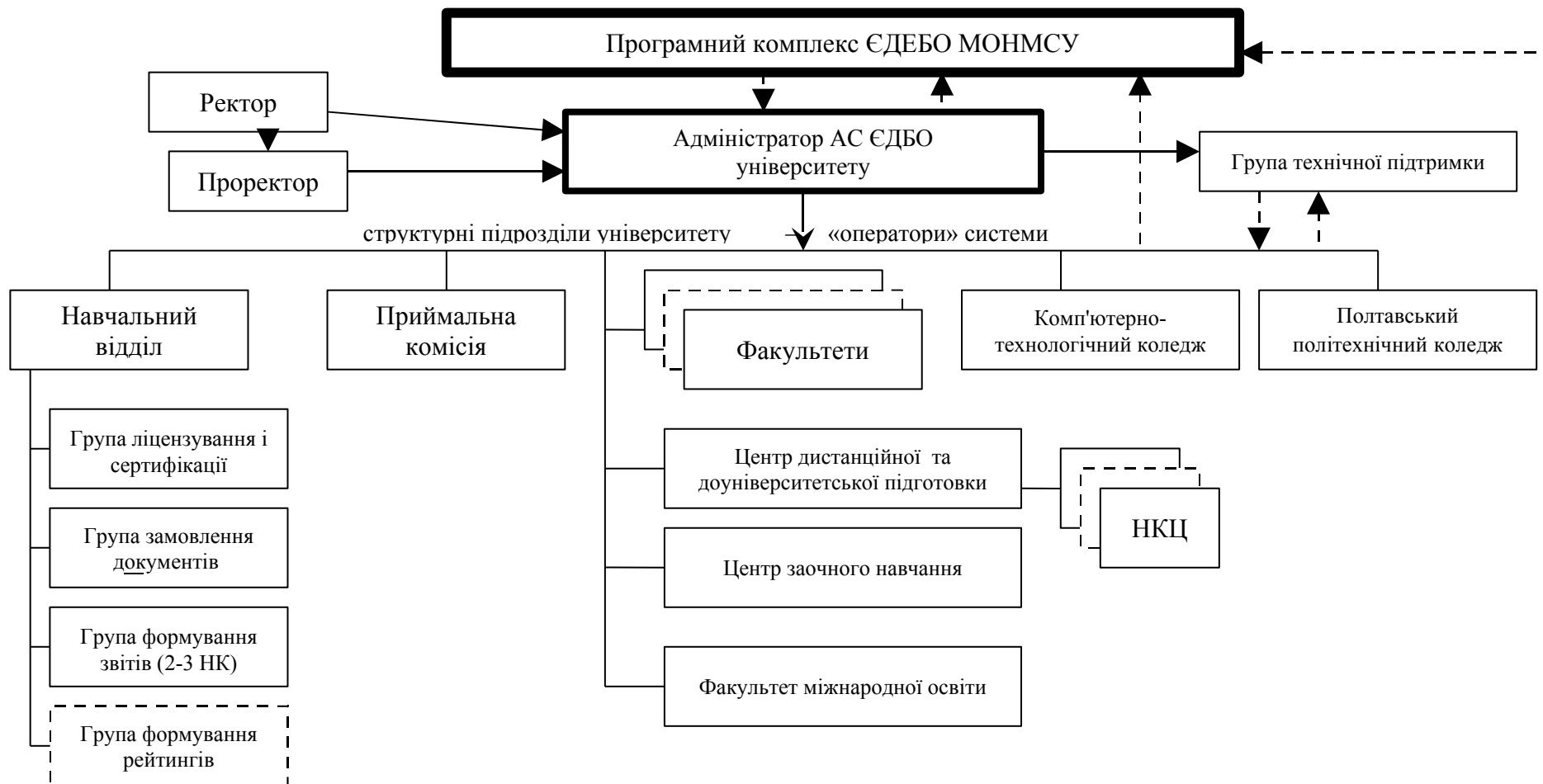
10.2 За порушення строків виконання зобов'язань за Договором, з винної сторони стягується пеня у розмірі 0,1 % вартості послуг, з яких допущено прострочення виконання, за кожен день прострочення, а за прострочення понад тридцять днів додатково стягується штраф у розмірі 7 відсотків вказаної вартості.

10.3 У випадку втрати Користувачем ЄДЕБО секретного ключа або параметрів доступу до ЄДЕБО Користувач ЄДЕБО несе відповідальність згідно з чинним законодавством України.

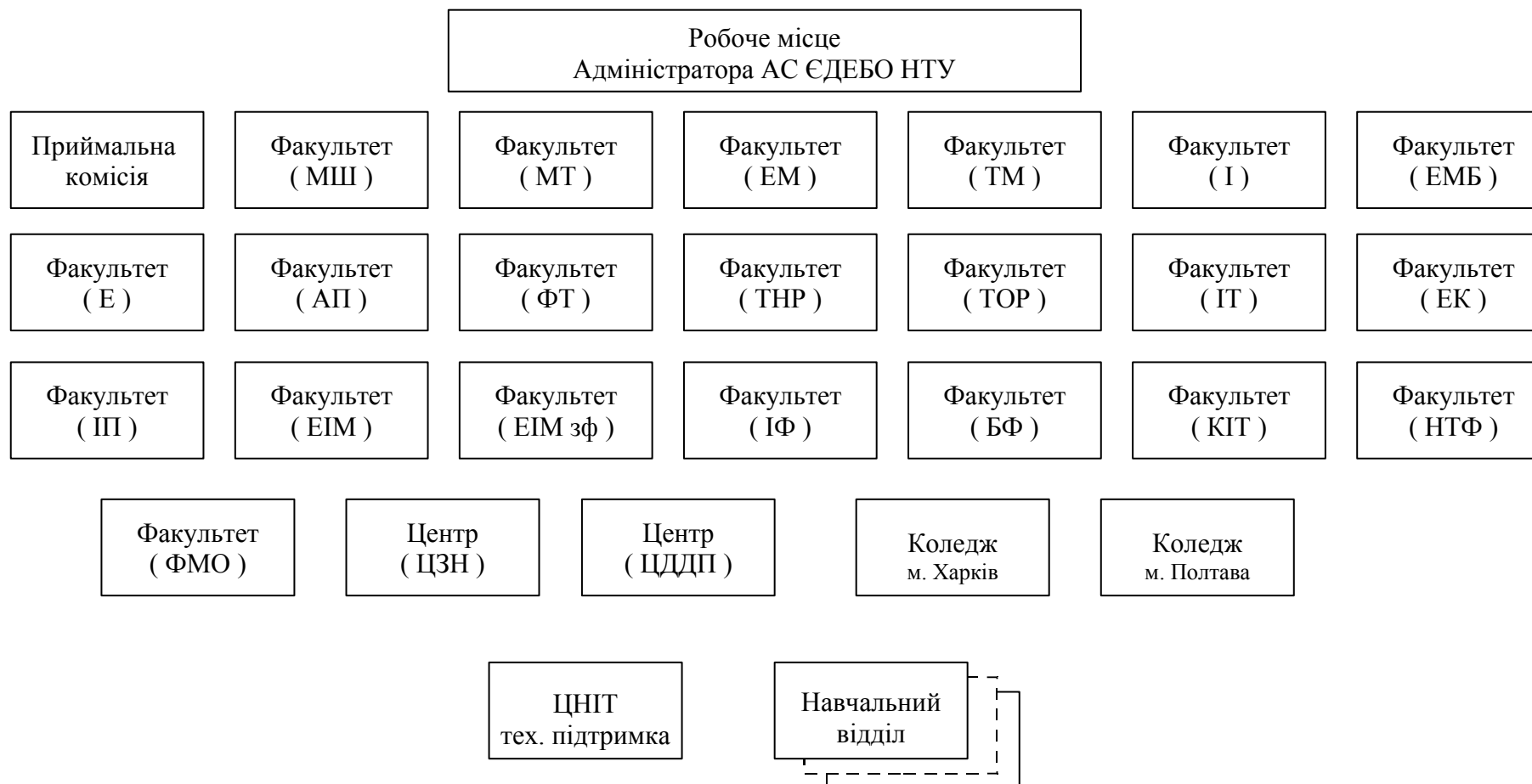
10.4 За достовірність інформації, яка вноситься до ЄДЕБО, за помилки, яких було допущено Користувачем ЄДЕБО під час роботи в ЄДЕБО, та які призвели до нанесення Розпоряднику ЄДЕБО та/або третім особам матеріальної та/або моральної шкоди, Університет несе відповідальність згідно з чинним законодавством України.

10.5 Розпорядник ЄДЕБО не несе відповідальності за якість та надійність роботи підключення до мережі Інтернет, яке використовує Навчальний заклад для доступу до ЄДЕБО та за збої у роботі комп'ютерної техніки Навчального закладу.

Структура АС ЄДЕБО Університету



Структура робочих місць Операторів АС ЄДЕБО



ІНСТРУКЦІЯ

Адміністратору АС ЄДЕБО Університету по забезпеченню безпеки експлуатації ПК ЄДЕБО - клієнт

I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Особа, яка визначена відповідальною за внесення відомостей та даних від Національного Технічного Університету «Харківський Політехнічний Інститут» (далі – Університет) до Єдиної Державної Електронній Базі з питань Освіти (далі - Адміністратор) призначається наказом ректора Університету, відповідно до якого здійснює обробку даних, зокрема персональних даних (далі – ПД), в веб-сервісі ЄДЕБО-клієнт.

1.2. Адміністратор підпорядковується Ректору Університету (проректору з науково-педагогічної роботи).

1.3. Ця Інструкція є керівним документом Адміністратора Національного Технічного Університету «Харківський Політехнічний Інститут» (НТУ «ХПІ»).

Інструкція визначає організаційно-правові основи щодо забезпечення безпеки експлуатації програмного комплексу захисту захищеного з'єднання (далі - Комплекс) при роботі в Єдиної Державної Електронній Базі з питань Освіти (далі - ЄДЕБО).

Ця Інструкція розроблена у відповідності до вимог законодавчих актів та нормативних документів, які регламентують захист конфіденційної інформації або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також нормативних документів з технічного захисту інформації.

Вимоги цієї Інструкції повинні виконуватися в усіх режимах функціонування автоматизованої системи (далі - АС) Університету як підсистеми ЄДЕБО.

1.4. Адміністратор у своїй роботі керується цією Інструкцією, Політикою інформаційної безпеки Університету, керівними і нормативними документами України в галузі технічного захисту інформації, експлуатаційною документацією на встановлені на об'єкті інформатизації системи захисту від несанкціонованого доступу до інформації та регламентуючими документами органу Університету НТУ «ХПІ».

1.5. Адміністратор відповідає за забезпечення стійкої працездатності елементів в веб-сервісі ЄДЕБО-клієнт і засобів захисту, при обробці персональних даних (далі - ПД).

Вимоги Адміністратора, пов'язані з виконанням ним своїх функцій, є обов'язковими для виконання всіма співробітниками Університету.

1.6. Об'єктами захисту в веб-сервісі ЄДЕБО-клієнт є ПД, які обробляються в ЄДЕБО.

Персональні дані, за режимом доступу є інформацією з обмеженим доступом (далі - ІзОД).

1.7. Найбільш ймовірними каналами витоку інформації для АС є:

- несанкціонований доступ до інформації, що обробляється в АС;
- розкрадання технічних засобів, в яких зберігається інформація, або окремих носіїв інформації;
- перегляд інформації з екранів дисплеїв моніторів та інших засобів її відображення за допомогою оптичних пристроїв;
- вплив на технічні чи програмні засоби з метою порушення цілісності (знищення, спотворення) інформації, працездатності технічних засобів, засобів захисту інформації, адресності та своєчасності обміну, в тому числі електромагнітного, через спеціально впроваджені електронні та програмні засоби («закладки»).

1.8. Робота з ІзОД (у тому числі зі службовими документами обмеженого доступу, ПД і т.д.) будується на наступних принципах:

- принцип персональної відповідальності - в будь-який момент часу за кожен документ (не залежно від типу носія: паперовий, електронний) повинен відповідати і розпоряджатися конкретний працівник, видача документів здійснюється тільки під розпис;
- принцип контролю та обліку - всі операції з документами повинні відображатися у відповідних журналах і картках (передача з рук в руки, зняття копії і т.п.).

1.9. Адміністратором призначається особа з числа найбільш кваліфікованих користувачів ПЕОМ Університету, в якому експлуатується веб-сервіс ЄДЕБО-клієнт.

Адміністратор в питаннях захисту інформації взаємодіє з співробітниками служби захисту інформації Університету.

1.10. Методичне керівництво роботою Адміністратора здійснюється відповідальним за забезпечення захисту ПД Університету.

II. ПРАВА ТА ОБОВ'ЯЗКИ

2.1. Адміністратор спільно з фахівцями з інформаційних технологій та захисту інформації:

- забезпечує підтримку підсистем управління доступом, реєстрації та обліку інформаційних ресурсів;
- контролює цілісність програмно-апаратного середовища, в якому зберігається оброблювальна інформація;
- контролює доступність і конфіденційність інформації, що зберігається, обробляється і передається по каналах зв'язку інформації з застосуванням захищеного з'єднання (стійке функціонування Локальної Обчислювальної Мережі (далі – ЛОМ) і її підсистем).

2.2. Права Адміністратора:

2.2.1. Вимагати від керівництва забезпечення фізичної охорони приміщень, де розташовані або зберігаються робочі станції та шлюзи захисту, носії ключової інформації (далі - НКІ), конверти з паролями.

2.2.2. Отримувати від Адміністраторів ЛОМ інформацію, необхідну для

налаштування Комплексу.

2.2.3. Доводити до відома розробників пропозиції та зауваження по роботі апаратних, програмних та апаратно-програмних засобів, що входять до складу Комплексу.

2.2.4. Подавати пропозиції щодо залучення організацій-ліцензіатів для виконання окремих робіт із забезпечення безпеки;

2.2.5. Звертатися до посадових осіб Державного підприємства (ДП) «Інфоресурс» з метою обслуговування ключових даних для здійснення захищеного з'єднання.

2.2.6. Вимагати від посадових осіб ДП «Інфоресурс» скасування, блокування або поновлення ключових даних для здійснення захищеного з'єднання.

2.2.7. Подавати пропозиції до посадових осіб ДП «Інфоресурс» щодо вдосконалення програмного Комплексу веб-сервіс ЄДЕБО-клієнт з урахування досвіду експлуатації в умовах Університету

2.2.8. Подавати пропозиції до посадових осіб Університету щодо втілення до повсякденної діяльності структурних підрозділів, відділів і служб Університету вимог ЄДЕБО. Здійснювати взаємодію підрозділів забезпечення навчального процесу з метою підготовки та подання до ЄДЕБО об'єктивної і достовірної інформації.

2.2.9. Готувати розпорядження ректора Університету (проректора з науково-педагогічної роботи) з питань вдосконалення роботи ЄДЕБО НТУ «ХПІ» та своєчасно доводити їх до структурних підрозділів, відділів і служб Університету.

2.3. Адміністратор зобов'язаний:

2.3.1. Знати і виконувати вимоги чинних нормативних та керівних документів, а також внутрішніх інструкцій, керівництва по захисту інформації і розпоряджень, що регламентують порядок дій із захисту інформації.

2.3.2. Забезпечувати установку, настройку і своєчасне оновлення елементів в веб-сервісі ЄДЕБО-клієнт:

- програмного забезпечення робочої станції (РС) і серверів (операційні системи, прикладне та спеціальне ПЗ);

- апаратних засобів;

- апаратних і програмних засобів захисту.

2.3.3. Забезпечувати працездатність елементів в веб-сервісі ЄДЕБО-клієнт та локальної обчислювальної мережі Університету.

2.3.4. Здійснювати контроль за порядком обліку, створення, зберігання і використання резервних та архівних копій масивів даних, машинних (вихідних) документів.

2.3.5. Забезпечувати функціонування і підтримувати працездатність засобів захисту в рамках покладених на нього функцій.

2.3.6. У разі відмови працездатності технічних засобів та програмного забезпечення елементів в веб-сервісі ЄДЕБО-клієнт, у тому числі засобів захисту інформації, вживати заходів по їх своєчасному відновленню і

виявленню причин, що призвели до відмови працездатності.

2.3.7.Проводити періодичний контроль вжитих заходів по захисту, в межах покладених на нього функцій.

2.3.8.Зберігати, здійснювати прийом та видачу персональних паролів користувачів, здійснювати контроль за правильністю використання персонального пароля Користувачем веб-сервісу ЄДЕБО-клієнт Університету (далі - Користувач).

2.3.9.Забезпечувати постійний контроль за виконанням користувачами встановленого Комплексу заходів щодо забезпечення безпеки експлуатації Комплексу захисту захищеного з'єднання з веб-сервісом ЄДЕБО-клієнт.

2.3.10.Інформувати відповідального за забезпечення захисту ПД Університету про факти порушення встановленого порядку робіт і спробах несанкціонованого доступу до інформаційних ресурсів в веб-сервісі ЄДЕБО-клієнт.

2.3.11.Звертатися до ректору Університету з пропозиціями щодо припинення обробки інформації, як в цілому, так і для окремих користувачів, в разі виявлення порушень встановленої технології обробки інформації, що захищається, або порушення функціонування веб-сервісу ЄДЕБО-клієнт або засобів захисту.

2.3.12. При виявленні порушення першої категорії (витік інформації) Адміністратор зобов'язаний негайно припинити роботи на АС.

При виявленні порушень першої, другої та третьої категорій адміністратор зобов'язаний подати службову записку керівництву і занести відповідний запис до журналу обліку роботи ЄДЕБО НТУ «ХПІ» з викладом факту порушення, вжиті та / або рекомендовані їм дії.

2.3.13. Вживати заходів щодо запобігання порушенням, що можуть призвести до компрометації особистих ключових даних для здійснення захищеного з'єднання з веб-сервісом ЄДЕБО-клієнт.

2.3.14.Ініціювати та брати участь у службових розслідуваннях за фактами порушення встановлених вимог забезпечення інформаційної безпеки, несанкціонованого доступу, втрати, пошкодження інформації, що захищається, носіїв ключової інформації та компонентів Комплексу.

2.3.15.Забезпечувати суворе виконання вимог щодо забезпечення безпеки інформації при організації обслуговування технічних засобів і відправку їх в ремонт. Технічне обслуговування та ремонт засобів обчислювальної техніки, призначених для обробки персональних даних, проводяться організаціями, що мають відповідні ліцензії. При проведенні технічного обслуговування і ремонту забороняється передавати ремонтним організаціям вузли і блоки з елементами накопичення і зберігання інформації. Непрацездатні елементи і блоки засобів обчислювальної техніки замінюються на елементи і блоки, що пройшли спеціальні дослідження та спеціальну перевірку.

2.3.16. Бути присутнім при виконанні технічного обслуговування елементів АС, сторонніми фізичними людьми та організаціями. Брати участь у випробуваннях і перевірках АС.

2.3.17. Вживати заходів з реагування, у разі виникнення позаштатних ситуацій та аварійних ситуацій, з метою ліквідації їх наслідків згідно вимог цієї Інструкції.

2.3.18. Не допускати до роботи на робочих станціях і серверах структурного підрозділу сторонніх осіб.

2.3.19. Здійснювати контроль монтажу обладнання структурного підрозділу фахівцями сторонніх організацій.

2.3.20. Брати участь у прийманні для потреб структурного підрозділу нових програмних засобів.

2.3.21. Узагальнювати результати своєї діяльності та готувати пропозиції щодо її вдосконалення.

2.3.22. Вести журнал обліку роботи з АС, що обробляє інформацію обмеженого доступу (персональні дані).

2.3.23. При зміні конфігурації автоматизованої системи вносити відповідні зміни в паспорт АС, на якій здійснюється обробка інформації з обмеженим доступом (персональних даних).

2.4. Адміністратору Комплексу заборонено:

2.4.1. Здійснювати експлуатацію засобів, що входять до складу Комплексу, при їх несправності.

2.4.2. Змінювати налаштування технічних засобів Комплексу таким чином, що створює загрози безпеки або порушує вимоги організаційно-розпорядчих документів організації, в якій експлуатується Комплекс.

2.4.3. Порушувати встановлений порядок поведінки з ключовими даними.

2.4.4. Передавати будь-кому без реєстрації у відповідних журналах носії ключових даних, за які він є відповідальним, та повідомляти відповідні паролі доступу до ключових даних.

ІІІ. ПОРЯДОК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

3.1. Організація робіт з експлуатації Комплексу.

Обов'язки з організації робіт з встановлення, експлуатації, виведення з експлуатації, технічного обслуговування та ремонту РС покладені на Адміністратора.

Залучення сторонніх організацій дозволяється лише з дозволу Ректора Університету у якому експлуатується РС за обґрунтованим зверненням Адміністратора. Адміністратор повинен контролювати хід робіт, що проводяться представниками постачальника або інших організацій.

До робіт з встановлення, експлуатації, виведення з експлуатації, технічного та гарантійного обслуговування, ремонту засобів, що входять до складу РС, а також у разі порушення їх функціонування, повинен залучатися персонал (зокрема, Адміністратор), який має необхідний кваліфікаційний рівень, рівень компетенції, та повноваження на виконання такого виду робіт, або співробітники організацій, з якими укладені відповідні угоди про технічне та гарантійне обслуговування.

3.2. Забезпечення безпеки під час встановлення та експлуатації Комплексу

3.2.1. Заходи із захисту інформації у Комплексі

Персональна електронно-обчислювальна машина (ПЕОМ), на якій буде розміщено РС Адміністратора повинна бути взята на облік. Під час встановлення програмного Комплексу захищеного з'єднання з веб-сервісом СДЕБО-клієнт Адміністратором повинні бути опечатані:

- системний блок РС Адміністратора;
- двері серверної шафи;
- двері приміщення, де розміщена серверна шафа.

На РС Адміністратора повинна бути встановлена лише одна операційна система, яка передбачена робочою документацією РС.

Налаштування операційної системи повинні відповідати робочій документації. Комплектація ПЕОМ і перелік встановленого загальносистемного і спеціального програмного забезпечення повинні бути відображені у паспорті-формулярі.

На РС адміністратора Комплексу повинні бути вжити заходи:

- по виключенню можливості по входу в режим зміни конфігурації BIOS;
- по забороні (налаштуваннями BIOS) завантаження з будь-якого з'ємного носія;
- по відключенню через BIOS не задіяних пристроїв вводу-виводу;
- по видаленню програмного забезпечення, яке не є необхідним для виконання службових обов'язків;
- по синхронізації часу з Всесвітнім координованим часом з точністю до однієї секунди.

Роботи по інсталяції, ремонту обладнання повинні здійснюватись у присутності і під контролем Адміністратора. До планування і розгортання РС можуть бути залучені адміністратори ЛОМ крім робіт, що пов'язані з встановленням, зберіганням, відновленням з резервної копії та знищенням ключових даних.

3.2.2. Заходи з технічного захисту інформації.

Перелік, періодичність, порядок здійснення заходів з технічного захисту інформації і відповідальні посадові особи визначаються організаційно-розпорядчими документами, що діють в навчальному закладі, який експлуатує РС.

3.3. Забезпечення безпеки під час виведення з експлуатації, ремонту тощо.

Перед передачею носія ключової інформації в ремонт, адміністратор Комплексу повинен знищити всі ключові дані, що зберігалися в носії або шляхом форматування.

Якщо носії ключової інформації не підлягають ремонту, то вони знищуються механічно. Про це складається відповідний акт знищення.

3.4. Реєстрації в журналі обліку робіт АС (РС), на якій оброблюється інформація з обмеженим доступом (персональні дані) підлягають:

- факту гарантованого видалення інформації з жорсткого магнітного диска;
- оновлення програмного забезпечення АС (РС);
- оновлення антивірусних баз;
- розкриття системного блоку з метою модернізації або ремонту із зазначенням мети розтину і проведених робіт;

- створення резервної копії бази даних та іншої службової інформації;
- заміна системного блоку з зазначенням
- відхилення в нормальній роботі системних і прикладних програмних засобів ускладнюють експлуатацію АС (РС);
- вихід з ладу або нестійке функціонування вузлів ПЕОМ або периферійних пристроїв (дисководів, принтера і т.п.);
- перебої в системі електропостачання, тощо.

3.5. Форма журналу реєстрації робіт АС (РС) та зразок заповнення наведені у таблиці 3.1.

Форма журналу реєстрації робіт АС (РС) та зразок заповнення.

Таблиця 3.1

Дата	Найменування робіт	П.І.Б. виконавця робіт	АС№	Розпис
1	2	3	4	5
01.02.2012	Оновлення антивірусної бази, сканування дисків	П.І.Б.	АС № 1 -АС №6	
02.01.2012	Переустановлення операційної системи	П.І.Б.	АС №3	
09.02.2012	Заміна маніпулятора миша	П.І.Б.	АС №7	
14.02.2012	Резервне копіювання інформації: «Мої документи»	П.І.Б.	АС №4 АС № 1 -АС №6	

IV. ДІЇ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Порядок дій Адміністратора у надзвичайних ситуаціях основних типів визначено у таблиці 4.1.

Порядок дій в умовах надзвичайних ситуацій.

Таблиця 4.1.

Надзвичайна ситуація	Порядок дій
Компрометація ключових даних захищеного з'єднання	Повідомити керівництво Університету, де експлуатується РС з захищеним з'єднанням. Зупинити роботу захищеного з'єднання (дати вказівку адміністратору ЛОМ). Подати запит на скасування ключових даних захищеного з'єднання. Провести внутрішнє розслідування.
Порушення електропостачання	Після відновлення електропостачання перевірити цілісність конфігурації захищеного з'єднання, за необхідності відновити конфігурацію з резервної копії.

Стихійне лихо	Повідомити керівництво Університету, де експлуатується РС з захищеним з'єднанням. Організувати фізичну охорону і евакуацію в безпечне місце РС Адміністратора. Діяти у відповідності із організаційно-розпорядчими документами організації, де експлуатується РС, та планом заходів з оперативного реагування на надзвичайні ситуації та поновлення функціонування.
Вихід з ладу захищеного з'єднання	Повідомити керівництво Університету, де експлуатується РС. Спробувати виявити причину виходу з ладу захищеного з'єднання. Звернутися до ДП «Інфоресурс», повідомивши можливу причину виходу з ладу.
Неможливість віддаленого підключення до веб-сервісу ЄДЕБО-клієнт	Повідомити керівництво Університету, де експлуатується РС. Звернутися до розробника ДП «Інфоресурс». Здійснити налаштування параметрів захищеного з'єднання.
Вихід з ладу ЕК для локального підключення, що іде у комплекті із шлюзом захисту	Повідомити керівництво організації, де експлуатується Комплекс. Звернутися до розробника шлюзу захисту.

V. ПОРЯДОК КОНТРОЛЮ ЗА СТАНОМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Поточний контроль здійснюється Адміністратором у відповідності до своїх обов'язків (дивись таблицю 5.1).

Порядок здійснення поточного контролю

Таблиця 5.1

Заходи, які повинен виконувати Адміністратор	Порядок здійснення контролю	Періодичність здійснення Контролю (не рідше)
Контроль за зберіганням ключа Адміністратора особистого	Перевірити цілісність печаток на тубусах з ключовими носіями. Перевірити цілісність конверту з паролями доступу до ключових носіїв	Перед використанням
Контроль за веденням журналів обліку прийому-передачі ключів	Перевірити останню дату запису у журналі обліку прийому-передачі ключів. Перевірити шляхом опитування, що носії ключової інформації знаходиться у тієї особи, підпис якої стоїть останнім в журналі	Перед використанням

Контроль відповідності комплектації РС Адміністратора паспорту-формуляру	Приймати участь у ремонті та модернізації РС Адміністратора. У випадку виявлення невідповідностей провести службове розслідування і внести відповідні зміни в паспорт-формуляр	Після ремонту або модернізації РС адміністратора
--	--	--

VI. ПОРЯДОК ДОПУСКУ В ПРИМІЩЕННЯ

6.1. Двері в приміщення, де розташована РС Адміністратора мають бути обладнані електронною системою розмежування доступу або принаймні двома надійними замками різних конструкцій і пристроєм для опечатування. Ключі від цих приміщень Адміністратор повинен отримувати під розпис і здавати в опечатаному тубусі.

6.2. Перелік осіб, які можуть мати доступ до цих приміщень та інші аспекти контролю фізичного доступу визначаються організаційно-розпорядчими документами Університету.

VII. ВІДПОВІДАЛЬНІСТЬ

7.1. Норми даної Інструкції є обов'язковими для усіх посадових осіб.

За порушення вимог цієї Інструкції винні посадові особи несуть дисциплінарну, адміністративну, цивільно-правову та кримінальну відповідальність відповідно до чинного законодавства України, зокрема, ст.27 Закону України "Про інформацію", ст.11 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", ст.9 Закону України "Про телекомунікації" та ст.361-363 Кримінального кодексу України.

7.2. Адміністратор несе всю повноту відповідальності за якість і своєчасність виконання завдань і функцій, покладених на його відповідно до цієї Інструкції та іншими нормативними документами щодо захисту інформації.

ІНСТРУКЦІЯ
Користувачу (Оператору) АС ЄДЕБО Університету
по забезпеченню безпеки експлуатації ПК ЄДЕБО - клієнт

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Користувач Єдиної Державної Електронній Базі з питань Освіти (далі - Користувач) здійснює обробку персональних даних (ПД) в веб-сервісі ЄДЕБО-клієнт.

1.2. Користувачем є співробітник Національного Технічного Університету «Харківський Політехнічний Інститут» (НТУ «ХПІ») (далі – Університет) призначений наказом керівника навчального закладу для роботи в веб-сервісі ЄДЕБО-клієнт, який бере участь у межах своїх функціональних обов'язків у процесах автоматизованої обробки інформації і має доступ до апаратних засобів, програмного забезпечення, даних і засобів захисту.

1.3. Користувач підпорядковується керівнику структурного підрозділу та Адміністратору ЄДЕБО Університету.

1.3. Ця Інструкція є керівним документом Користувача Національного Технічного Університету «Харківський Політехнічний Інститут» (НТУ «ХПІ»).

Інструкція визначає організаційно-правові основи щодо забезпечення безпеки експлуатації програмного комплексу (далі – Комплекс) захисту захищеного з'єднання при роботі в Єдиної Державної Електронній Базі з питань Освіти (далі - ЄДЕБО).

Ця Інструкція розроблена у відповідності до вимог законодавчих актів та нормативних документів, які регламентують захист конфіденційної інформації або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також нормативних документів з технічного захисту інформації.

Вимоги цієї Інструкції повинні виконуватися в усіх режимах функціонування автоматизованої системи (далі - АС) Університету.

1.4. Користувач у своїй роботі керується цією Інструкцією, Політикою інформаційної безпеки навчального закладу, керівними і нормативними документами України в галузі технічного захисту інформації, експлуатаційною документацією на встановлені на об'єкті інформатизації системи захисту від несанкціонованого доступу до інформації та регламентуючими документами Університету.

1.5. Користувач несе персональну відповідальність за свої дії.

1.6. Об'єктами захисту в веб-сервісі ЄДЕБО-клієнт є ПД, які обробляються в ЄДЕБО.

Персональні дані, за режимом доступу є інформацією з обмеженим доступом (далі - ІЗОД)

1.7. Найбільш ймовірними каналами витоку інформації для АС є:

- несанкціонований доступ до інформації, що обробляється в АС;

- розкрадання технічних засобів, в яких зберігається інформація, або

окремих носіїв інформації;

-перегляд інформації з екранів дисплеїв моніторів та інших засобів її відображення за допомогою оптичних пристроїв;

-вплив на технічні чи програмні засоби з метою порушення цілісності (знищення, спотворення) інформації, працездатності технічних засобів, засобів захисту інформації, адресності та своєчасності обміну, в тому числі

електромагнітного, через спеціально впроваджені електронні та програмні засоби («закладки»).

1.8. Робота з ІзОД (у тому числі зі службовими документами обмеженого доступу, ПД і т.д.) будується на наступних принципах:

–принцип персональної відповідальності - в будь-який момент часу за кожен документ (не залежно від типу носія: паперовий, електронний) повинен відповідати і розпоряджатися конкретний працівник, видача документів здійснюється тільки під розпис;

–принцип контролю та обліку - всі операції з документами повинні відображатися у відповідних журналах і картках (передача з рук в руки, зняття копії і т.п.).

1.9. Методичне керівництво роботою Користувача здійснюється особою, яка визначена відповідальною за внесення відомостей та даних від Університету до Єдиної державної електронній бази з питань освіти (далі - Адміністратор), яка призначена наказом Ректора Університету для роботи в веб-сервісі ЄДЕБО-клієнт.

II. ПРАВА ТА ОБОВ'ЯЗКИ

2.1. Права Користувача:

2.1.1. Запитувати та одержувати від Адміністратора всю необхідну для виконання службових обов'язків інформацію.

2.1.2. Вимагати від Адміністратора своєчасного повідомлення про готовність технічних і програмних засобів робочої станції (далі - РС) до експлуатації.

2.1.3. Звертатися до Адміністратора за консультаціями з питань забезпечення інформаційної безпеки технологічних процесів обробки інформації на закріплених за ним засобах.

2.1.4. Подавати обґрунтовані пропозиції Адміністратору про припинення інформаційного обміну або зміну режиму функціонування Комплексу;

2.1.5. Ініціювати та брати участь у службових розслідуваннях за фактами порушення встановлених вимог забезпечення інформаційної безпеки, несанкціонованого доступу, втрати, пошкодження інформації, що захищається, та ввірених йому технічних засобів РС.

2.1.6. Користуватися наданим йому програмним забезпеченням клієнтського місця РС.

2.1.7. Звертатися до Адміністратора у разі несправності програмного забезпечення клієнтського місця РС.

2.1.8. Звертатися до Адміністратора з метою оновлення та обслуговування атрибутів авторизації.

2.1.9. Вимагати від Адміністратора скасування, блокування або поновлення

своїх атрибутів авторизації.

2.2. Користувач зобов'язаний:

2.1. Знати і виконувати вимоги чинних нормативних та керівних документів, а також внутрішніх інструкцій, керівництва по захисту інформації і розпоряджень, що регламентують порядок дій із захисту інформації.

2.2. Ознайомитись та дотримуватись вимог документів, що визначають порядок підключення РС Користувача до веб-сервісі ЄДЕБО-клієнт.

2.3. Виконувати на РС тільки ті процедури, які визначені йому для роботи в веб-сервісі ЄДЕБО-клієнт.

2.4. Знати і дотримуватися встановлені вимоги по режиму обробки ІзОД (ПД), обліку, зберігання та пересилання носіїв інформації, забезпечення безпеки ПД, а також керівних та організаційно-розпорядчих документів.

2.5. Дотримуватися вимоги парольної політики (розділ 3).

2.6. Дотримуватися правил при роботі в мережах загального доступу і (або) міжнародного обміну - Інтернет і інших (розділ 4).

2.7. Екран монітора в приміщенні розташовувати під час роботи так, щоб виключалася можливість несанкціонованого ознайомлення з відображуваної інформацією сторонніми особами, штори на віконних отворах повинні бути завішані (жалюзі закриті).

2.8. Про всі виявлені порушення, пов'язані з інформаційною безпекою навчального закладу, а так само для отримань консультацій з питань інформаційної безпеки, необхідно звернутися в співробітників технічної підтримки по внутрішньому телефону 7076907.

2.9. Негайно повідомляти Адміністратору Комплексу про незвичні параметри ТСП-пакетів, що проходить через захищене з'єднання (велика кількість напіввідкритих з'єднань тощо).

2.10. В межах своїх повноважень допомагати Адміністратору Комплексу у виявленні і відбитті атак на РС.

2.11. Зберігати в таємниці особистий ключ та приймати всі можливі заходи для запобігання його втраті, розкриттю, перекручуванню та несанкціонованому використанню.

2.12. Використовувати особистий ключ виключно для здійснення захищеного з'єднання з веб-сервісом ЄДЕБО-клієнт, та додержуватися інших обмежень щодо використання атрибутів авторизації.

2.13. Негайно інформувати Адміністратора про наступні події, що трапилися до закінчення строку чинності атрибутів авторизації:

компрометацію особистого ключа; компрометацію пароллю захисту особистого ключа; виявлену неточність або зміни даних атрибутів авторизації.

2.11. Для отримання консультацій з питань роботи та налагодженню елементів веб-сервісу ЄДЕБО-клієнт необхідно звертатися до Адміністратора Університету по внутрішньому телефону.

2.9. Користувачу забороняється:

-розголошувати інформацію яка підлягає захисту третім особам;

-використовувати особистий ключ у разі його компрометації;

-використовувати особистий ключ, що скасований або заблокований;

- копіювати інформацію яка підлягає захисту на зовнішні носії без дозволу свого керівника;
- самостійно встановлювати, тиражувати, або модифікувати програмне забезпечення і апаратне забезпечення, змінювати встановлений алгоритм функціонування технічних і програмних засобів;
- несанкціоноване відкриття загального доступу до папок на своїй РС;
- заборонено підключати до РС і корпоративної інформаційної мережі особисті зовнішні носії та мобільні пристрої;
- відключати (блокувати) засоби захисту інформації;
- обробляти на РС інформацію та виконувати інші роботи, не передбачені переліком прав Користувача з доступу до веб-сервісу ЄДЕБО-клієнт;
- повідомляти (або передавати) стороннім особам особисті ключі та атрибути доступу до ресурсів веб-сервісу ЄДЕБО-клієнт;
- без погодження з Адміністратором здійснювати вносити зміни в налаштування РС, що можуть вплинути на безпеку або працездатність веб-сервісу ЄДЕБО-клієнт;
- залучати сторонніх осіб для проведення ремонту або настройки РС, без узгодження з відповідальним за забезпечення захисту ПД;
- залишати на робочих столах, в столах і незакритих сейфах документи обмеженого поширення, а також залишати незамкненими і не опечатаними після закінчення роботи сейфи, приміщення і сховища з документами конфіденційного характеру;
- виконувати роботи з документами обмеженого доступу на дому, виносити їх із службових приміщень, знімати копії або робити виписки з таких документів без дозволу керівника;
- накопичувати непотрібну для роботи конфіденційну інформацію;
- використовувати компоненти програмного та апаратного забезпечення АС в неслужбових цілях;
- самовільно вносити будь-які зміни в конфігурацію апаратно-програмних засобів РС або встановлювати додатково будь-які програмні та апаратні засоби;
- здійснювати обробку конфіденційної інформації в присутності сторонніх (не допущених до даної інформації) осіб;
- навмисно використовувати недокументовані властивості і помилки в програмному забезпеченні або в налаштуваннях засобів захисту, які можуть привести до виникнення кризової ситуації.

2.10.При відсутності візуального контролю за РС: доступ до комп'ютера повинен бути негайно заблокований. Для цього необхідно натиснути одночасно комбінацію клавіш «Ctrl» «Alt» «Del» і вибрати опцію «Блокування».

2.11.Вживати заходів з реагування, у разі виникнення позаштатних ситуацій та аварійних ситуацій, з метою ліквідації їх наслідків, в рамках покладених, в межах покладених на нього функцій.

III. ОРГАНІЗАЦІЯ ПАРОЛЬНОГО ЗАХИСТУ

3.1.Особисті паролі доступу до елементів веб-сервісу ЄДЕБО-клієнт

видаються користувачам Адміністратором веб-сервісу ЄДЕБО-клієнт Університету.

3.2. Повна планова зміна паролів у веб-сервісі ЄДЕБО-клієнт проводиться не рідше одного разу на 3 місяці.

3.3. Правила формування пароля:

- пароль не може містити ім'я облікового запису користувача або будь-яку його частину.

- пароль повинен складатися не менше ніж з 8 символів.

- у паролі повинні бути присутніми символи трьох категорій з числа наступних чотирьох:

а) великі літери англійського алфавіту від А до Z;

б) малі літери англійського алфавіту від а до z;

в) десяткові цифри (від 0 до 9);

г) символи, які не належать алфавітно-цифровому набору (наприклад, !, \$,

- забороняється використовувати в якості пароля ім'я входу в систему, прості паролі типу «123», «111», «а б в г д» і їм подібні, а так само імена і дати народження своєї особистості і своїх родичів, клички домашніх тварин, номери автомобілів, телефонів та інші паролі, які можна вгадати, ґрунтуючись на інформації про користувача.

- забороняється використовувати в якості пароля один і той же символ що повторюється або повторювану комбінацію з декількох символів;

- забороняється використовувати в якості пароля комбінацію символів, що набираються в закономірному порядку на клавіатурі (наприклад, 1234567 тощо);

- забороняється вибирати паролі, які вже використовувалися раніше.

3.4. Правила введення пароля:

- введення пароля повинен здійснюватися з урахуванням регістра, в якому пароль було встановлено;

- під час введення паролів необхідно виключити можливість його підглядання сторонніми особами або технічними засобами (відеокамери та ін.).

3.5. Правила зберігання пароля:

- забороняється записувати паролі на папері, у файлі, електронній записнику та інших носіях інформації, в тому числі на предметах;

- забороняється повідомляти іншим користувачам особистий пароль і реєструвати їх в системі під своїм паролем.

3.6. Особи, які використовують паролювання, зобов'язані:

- чітко знати і суворо виконувати вимоги цієї інструкції та інших керівних документів з паролювання.

- своєчасно повідомляти Адміністратору інформаційної безпеки про втрату, компрометації, несанкціонованому зміну паролів і несанкціонованому зміну термінів дії паролів.

IV. ПРАВИЛА РОБОТИ В МЕРЕЖАХ ЗАГАЛЬНОГО ДОСТУПУ

I МІЖНАРОДНОГО ОБМІНУ

4.1. Робота в мережах загального доступу і (або) міжнародного обміну (мережі Інтернет та інших) (далі - Мережа) на елементах веб-сервісу

ЄДЕБО-клієнт, повинна проводитися при службової необхідності.

4.2. При роботі в Мережі забороняється:

- здійснювати роботу при відключених засобах захисту (антивірус і інших);
- передавати по Мережі захищається інформацію без використання засобів захисту каналів зв'язку;
- забороняється завантажувати з Мережі програмне забезпечення та інші файли;
- забороняється відвідування сайтів сумнівної репутації (сайти що містять нелегально поширюване програмне забезпечення тощо).
- забороняється нецільове використання підключення до мережі.

V. ВІДПОВІДАЛЬНІСТЬ

5.1. Користувач несе відповідальність за дотримання вимог цієї Інструкції, а також інших нормативних документів в галузі захисту інформації. За розголошення інформації обмеженого доступу, а також за порушення порядку роботи з документами або машинними носіями, що містять таку інформацію, працівники можуть бути притягнуті до дисциплінарної або іншої, передбаченої законодавством відповідальності.

5.2. За розголошення інформації обмеженого доступу, порушення порядку роботи з документами або машинними носіями, що містять таку інформацію, працівники можуть бути притягнуті до дисциплінарної або іншої, передбаченої законодавством відповідальності.

5.3. Вимоги інструкції доводяться до користувачів під розпис в окремій відомості за формою: