Керівництво Адміністратора навчального закладу
по забезпеченню безпеки експлуатації програмного комплексу захисту
захищеного з’єднання при роботі в веб-сервісі ЄДЕБО-клієнт

_____

(найменування навчального закладу)

ЗАТВЕРДЖУЮ
Керівник навчального закладу

«___» _____ 2012 року

Типова форма керівництва Адміністратора
навчального закладу по забезпеченню безпеки експлуатації
програмного комплексу захисту захищеного з’єднання
при роботі в веб-сервісі ЄДЕБО-клієнт

(типова форма наводиться як приклад, який в кожному навчальному закладі можливо застосовувати з урахуванням умов діяльності відповідної посадової особи)

Керівник структурного
підрозділу _____

м. _____2012

ЗМІСТ

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Особа, яка визначена відповідальною за внесення відомостей та даних від _____ *(найменування навчального закладу)* до Єдиної державної електронній бази з питань освіти (далі - Адміністратор) призначається наказом керівника навчального закладу, відповідно до якого здійснює обробку даних, зокрема персональних даних (ПД), в веб-сервісі ЄДЕБО-клієнт.

1.2. Адміністратор підпорядковується _____.

1.3. Ця Інструкція є керівним документом Адміністратора _____ *(найменування навчального закладу)*.

Інструкція визначає організаційно-правові основи щодо забезпечення безпеки експлуатації програмного комплексу захисту захищеного з'єднання при роботі в 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) навчального закладу.

1.4. Адміністратор 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 органу навчального закладу _____ *(найменування навчального закладу)*.

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

Вимоги Адміністратора, пов'язані з виконанням ним своїх функцій, обов'язкові для виконання всіма співробітниками навчального закладу.

1.6. Об'єктами захисту в веб-сервісі ЄДЕБО-клієнт є ПД, які обробляються в Єдиної державної електронній бази з питань освіти (далі – Єдина база).

ПД, крім знеособлених ПД, 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 навчального закладу, в якому експлуатується веб-сервіс ЄДЕБО-клієнт.

Адміністратор в питаннях захисту інформації взаємодіє з співробітниками служби захисту інформації навчального закладу.

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

ІІ. ПРАВА ТА ОБОВ'ЯЗКИ

2.1. Адміністратор спільно з фахівцями з інформаційних технологій та захисту інформації *(за наявності)*:

- 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 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 (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 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.

2.3. На Адміністратора покладаються такі обов'язки:

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 навчального закладу *(за наявності)*.

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 навчального закладу (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 навчального закладу про факти порушення встановленого порядку робіт і спробах несанкціонованого доступу до інформаційних ресурсів в веб-сервісі ЄДЕБО-клієнт.

2.3.11. Звертатися до керівника навчального закладу з вимогою 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 АС 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 учать 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 поводження з ключовими даними комплексу.

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 керівника навчального закладу 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 взяті на облік. Під час встановлення програмного комплексу захищеного з’єднання з веб-сервісом ЄДЕБО-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 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:

- 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 і пр. службової інформації;
- заміна системного блоку з зазначенням факту гарантованого видалення інформації з жорсткого магнітного диска;
- 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.

Таблиця 3.1. Форма журналу реєстрації робіт АС (РС) та зразок заповнення.

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.

Таблиця 4.1. – Порядок дій в умовах надзвичайних ситуацій.

Надзвичайна ситуація	Порядок дій
Компрометація ключових даних захищеного з'єднання	Повідомити керівництво навчального закладу, 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 навчального закладу, де експлуатується РС з с 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 навчального закладу, де експлуатується РС. Спробувати вияснити 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 навчального закладу, 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.).

Таблиця 5.1. – Порядок дій в умовах надзвичайних ситуацій

Заходи, які повинен виконувати Адміністратор	Порядок здійснення контролю	Періодичність здійснення контролю (не рідше)
Контроль за зберіганням особистого ключа Адміністратора	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 навчального закладу, що експлуатує РС.

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.

З інструкцією ознайомлений:

Адміністратор автоматизованої системи _____*(найменування навчального закладу)*

_____

(Посада) *(розпис)* *(П.І.Б.)*