Керівництво Користувача 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 Користувача
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. Користувач Єдиної державної бази з питань освіти (далі - Користувач) здійснює обробку персональних даних (ПД) в веб-сервісі ЄДЕБО-клієнт.

1.2. Користувачем є співробітник навчального закладу 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 _____.

1.4. 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.

1.5. 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 органу навчального закладу _____ *(найменування навчального закладу)*.

1.6. Користувач несе персональну відповідальність за свої дії.

1.7. 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).

1.8. 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»).

1.9. 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.).

1.10. Методичне керівництво роботою Користувача здійснюється особою, яка визначена відповідальною за внесення відомостей та даних від _____ *(найменування навчального закладу)* до Єдиної державної електронній бази з питань освіти (далі - Адміністратор), яка призначена наказом керівника навчального закладу для роботи в веб-сервісі ЄДЕБО-клієнт.

ІІ. 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 учать 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 на

них 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 _____ по внутрішньому телефону _____.

2.9. Негайно повідомляти Адміністратору комплексу про незвичні параметри TCP-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 паролю 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 навчального закладу по внутрішньому телефону _____.

2.9. Користувачу забороняється:

- розголошувати захищаєму інформацію третім особам;
- використовувати особистий ключ у разі його компрометації;
- використовувати особистий ключ, що скасований або заблокований;
- копіювати захищаєму інформацію 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;
- несанкціоновано відкривати загальний доступ 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.

ІІІ. ОРГАНІЗАЦІЯ ПАРОЛЬНОГО ЗАХИСТУ

3.1. Особисті паролі доступу до елементів веб-сервісу ЄДЕБО-клієнт видаються користувачам Адміністратором веб-сервісу ЄДЕБО-клієнт навчального закладу.

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 A до Z;

б) малі літери англійського алфавіту від a 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», «qwerty» 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, електронної 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 І (АБО) 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.

З інструкцією ознайомлений:
Користувач робочої станції автоматизованої системи _____*(найменування навчального закладу)*

_____

(Посада) *(розпис)* *(П.І.Б.)*