ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ

СПЕЦІНФОСИСТЕМИ

ЗАТВЕРДЖЕНИЙ
UA.32436187.00001-01 91 01-ЛЗ

КЛЮЧ ЕЛЕКТРОННИЙ DIAMOND

ІНСТРУКЦІЯ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ

UA.32436187.00001-01 91 01

на 13 аркушах

Харків – 2022

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Інструкція щодо забезпечення безпеки експлуатації UA.332436187.00001-01 91 01 (далі – Інструкція) розроблена відповідно до вимог «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту», затвердженого наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 20.07.2007 за № 862/14129 (зі змінами).

Ця Інструкція визначає організаційно-технічні вимоги щодо забезпечення безпеки експлуатації засобу криптографічного захисту інформації «Ключ електронний DIAMOND» (далі – Виріб).

Виріб призначений для захисту відкритої та конфіденційної інформації від загроз порушення її цілісності, конфіденційності, автентичності та неспростовності, яка надходить, зберігається та оброблюється в системах оброблення інформації.

Виріб може бути використаний для криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.

Виріб може бути використаний в якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.

В Інструкції описані:

– права та обов'язки осіб, відповідальних за забезпечення безпеки експлуатації Виробу;

– порядок забезпечення безпеки Виробу під час його введення в експлуатацію, експлуатації та виведення з експлуатації;

– питання проведення тестування Виробу;

– дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри компрометації ключів;

– порядок проведення контролю за станом забезпечення безпеки Виробу.

Особи, винні в порушенні вимог цієї Інструкції, залежно від наслідків, притягуються до відповідальності відповідно до чинного законодавства.

1. ПРАВА ТА ОБОВ'ЯЗКИ ОСІБ, ВІДПОВІДАЛЬНИХ ЗА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ ВИРОБУ

1.1. Категорії користувачів Виробу

Користувачами Виробу є відповідальні посадові особи, поділені на дві категорії: адміністратор безпеки та користувач.

У випадку використання Виробу приватною особою або неможливості чи недоцільності виділення посади адміністратора безпеки дозволяється суміщення ролей адміністратора безпеки та користувача однією особою. При цьому для забезпечення достатнього рівня безпеки ця особа повинна використовувати різні паролі для ролей адміністратора безпеки та користувача.

1.2. Права та обов'язки адміністратора безпеки

1.2.1. Адміністратор безпеки відповідає за:

- налаштування параметрів безпеки Виробу;
- введення Виробу у експлуатацію;
- виведення з експлуатації Виробу;
- контроль за всіма пов'язаними із захистом з використанням Виробу подіями і за розслідуванням будь-яких реальних або підозрюваних порушень;
- оперативне припинення порушень безпеки, які виникають в процесі експлуатації Виробу;
- своєчасне інформування керівництва про всі випадки порушення безпеки інформації
- розробку внутрішніх процедур та інструкцій щодо запобігання компрометації ключових даних та іншої конфіденційної інформації при експлуатації Виробу;
- інформування керівництва організації, в якій використовується Виріб, про працездатність існуючих засобів захисту інформації.

1.2.2. Адміністратор безпеки зобов'язаний:

- знати і виконувати вимоги цієї Інструкції інших нормативних документів із забезпечення безпеки інформації, що обробляється Виробом, а також нормативно-правових актів з організації та забезпечення безпеки криптографічного захисту інформації з обмеженим доступом, дотримуватися режиму безпеки в роботі;
- систематично підвищувати власний професійний рівень;
- своєчасно повідомляти керівництву організації, в якій використовується Виріб, про факти порушення політики безпеки інформації та вживати невідкладні заходи щодо усунення наслідків таких порушень та ліквідації причин, що можуть спричинити зниження рівня безпеки інформації, що обробляється Виробом;
- забезпечувати повноту та якісне виконання організаційно-технічних заходів із захисту інформації;
- перевіряти відповідність прийнятих в організації, в якій використовується Виріб, правил, інструкцій щодо обробки інформації, здійснення контролю за виконанням цих вимог відповідно до визначеної політики безпеки інформації, контролювати забезпечення охорони і порядку зберігання документів (носіїв інформації), які містять дані, що підлягають захисту;
- забезпечувати організацію та проведення заходів з оновлення вбудованих мікропрограм Виробу;
- складати і подавати керівництву організації, в якій використовується Виріб, акти щодо виявлених порушень безпеки експлуатації Виробу, готувати рекомендації щодо їхнього усунення.

1.2.3. Адміністратору безпеки забороняється:

- обробляти з використанням Виробу інформацію, що містить відомості, які становлять державну таємницю;
- використовувати Виріб, що має ознаки зовнішнього втручання або проявляє ознаки неправильного функціонування;
- несанкціоновано вносити зміни у Виріб.

1.2.4. Адміністратор безпеки має право:

- подавати керівництву організації пропозиції щодо призупинення процесу обробки, заборони обробки, зміни режимів обробки інформації тощо у випадку виявлення порушень або у випадку виникнення реальної загрози порушення безпеки експлуатації Виробу;
- проводити службові розслідування у випадках виявлення порушень безпеки експлуатації Виробу;
- отримувати доступ до документів необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення.

1.3. Права та обов’язки користувача

1.3.1. Користувач відповідає за:

- генерацію ключових даних;
- використання ключових даних для здійснення криптографічних перетворень;
- знищення ключових даних;
- контроль працездатності Виробу.

1.3.1. Користувач зобов’язаний:

- знати і виконувати вимоги цієї Інструкції та Інструкції щодо порядку генерації ключових даних і поводження з ключовими документами,, дотримуватися режиму безпеки в роботі;
- зберігати ПЕОМ до якої підключається Виріб (або яка має доступ до Виробу) у порядку, що унеможливлює її несанкціоноване використання іншими особами;
- здійснювати заходи щодо недопущення втрати, крадіжки та несанкціонованого доступу до Виробу;
- не використовувати Виріб за призначенням у разі компрометації ключових даних;
- негайно інформувати адміністратора безпеки про випадки втрати Виробу, порушення його працездатності, компрометації ключових даних або підозрі на таку компрометацію.

1.3.2. Користувачу забороняється:

- розголошувати склад ключових даних або паролі доступу до Виробу;
- передавати Виріб іншим особам;
- використовувати Виріб, що має ознаки зовнішнього втручання або проявляє ознаки неправильного функціонування;
- встановлювати на ПЕОМ до якої підключається Виріб (або яка має доступ до Виробу) інше програмне забезпечення, окрім дозволеного адміністратором безпеки;
- обробляти з використанням Виробу відомості, які становлять державну таємницю.

1.3.3. Користувач має право:

- оскаржити дії чи бездіяльність адміністратора безпеки пов’язані з функціонуванням Виробу.

2. ПОРЯДОК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІД ЧАС ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ, ЕКСПЛУАТАЦІЇ ТА ВИВЕДЕННЯ З ЕКСПЛУАТАЦІЇ ВИРОБУ

2.1. Обов'язки з організації робіт з введення в експлуатацію та виведення з експлуатації Виробу покладені на адміністратора безпеки.

2.2. В організації, в якій використовується Виріб, встановлюють штатний розклад, на підставі якого розробляють функціональні обов'язки та посадові інструкції з детальним описом дій для кожної штатної одиниці. Витяг з посадової інструкції (пам'ятка користувачу) мають знаходитися на кожному робочому місці користувача Виробу. Орієнтовний зміст пам'ятки користувачу наведений в додатку 1 до цієї Інструкції.

2.3. Кожен Виріб повинен бути взяті на облік. Порядок обліку засобів криптографічного захисту повинен бути визначений внутрішньою інструкцією.

2.4. Охорона, розміщення та організація режиму роботи у приміщеннях, де зберігається та використовується Виріб, повинні виключати можливість неконтрольованого проникнення або перебування у цих приміщеннях сторонніх осіб, та забезпечувати уникнення крадіжки, ушкодження або іншого втручання в роботу Виробу.

2.5. Перед введенням в експлуатацію адміністратор безпеки має переконатись у відсутності ознак зовнішніх впливів, ушкоджень тощо Виробу та провести перевірку його працездатності відповідно до Інструкції з експлуатації Виробу. Впевнившись у цілісності та працездатності Виробу адміністратор безпеки має ініціалізувати Виріб. Під ініціалізацією Виробу мається на увазі встановлення первинного пароля адміністратора безпеки. У разі якщо ініціалізація Виробу виконана виробником, адміністратор безпеки має змінити стандартний пароль виробника на власний. Якщо ініціалізація Виробу виробником не проводилася адміністратор безпеки має встановити власний пароль як первинний (провести ініціалізацію). Ініціалізація Виробу виконується один раз протягом усього життєвого циклу. У разі втрати пароля адміністратора безпеки його відновлення неможливе.

2.6. Перед введенням в експлуатацію адміністратор безпеки проводить інструктаж користувача щодо порядку експлуатації Виробу за призначенням та дотримання вимог цієї інструкції. Для введенням в експлуатацію адміністратор безпеки повинен автентифікуватись на Виробі за допомогою свого пароля та встановити максимальну кількість невдалих спроб автентифікації користувача.

Після цього у присутності користувача виконати процедуру форматування Виробу. Під час форматування користувач має ввести пароль користувача Виробу. Після цього адміністратор безпеки передає користувачу виріб для використання за призначенням. Користувач має розписатися у журналі про проведення інструктажу та отримання Виробу.

2.7. Рекомендована максимальна кількість невдалих спроб автентифікації користувача складає 3-5.

2.8. Рекомендована довжина паролів доступу адміністратора безпеки та користувача складає 8-12 алфавітно-цифрових символів.

2.9. При виведенні Виробу з експлуатації адміністратором безпеки повинні бути знищені всі ключові дані що зберігаються у виробі. Знищення ключових даних здійснюється шляхом форматування Виробу та встановлення випадкового пароля користувача. У разі втрати пароля користувача адміністратора безпеки користувач сам повинен з використанням свого пароля знищити всі ключові дані на Виробі. У разі втрати і пароля адміністратора безпеки, і пароля користувача, Виріб повинен бути знищений фізично.

2.10. Всі операції щодо введення в експлуатацію, передачі користувачу, отримання від користувача та виведення з експлуатації виробів адміністратор безпеки заносить до відповідного журналу. Необхідність ведення, форма журналу та порядок його ведення мають бути визначені внутрішньою інструкцією підприємства чи організації що експлуатує Виріб.

2.11. Під час, коли Виріб не використовується (неробочий час), Виріб повинен зберігатися у спосіб що унеможливлює несанкціонований доступ до нього. Порядок

зберігання Виробу у неробочий час має бути визначений внутрішньою інструкцією. Можливими варіантами зберігання Виробу у неробочий час:

- зберігання в особистому сейфі користувача;
- зберігання в сейфі визначеної наказом керівника посадової особи у опечатаному індивідуальною печаткою користувача тубусі;
- користувач завжди зберігає Виріб при собі (найменш надійний).

3. ПОРЯДОК ТЕСТУВАННЯ ВИРОБУ

3.1. При підключенні до ПЕОМ (при подачі живлення) Виріб автоматично виконує самотестування. За необхідності проведення тестування підключеного до ПЕОМ Виробу необхідно його відключити і через декілька секунд знову підключити до ПЕОМ. Результат самотестування зчитується через бібліотеку взаємодії спеціалізованим програмним забезпеченням відповідно Настанови щодо експлуатування Виробу.

3.2. Під час використання апаратного недетермінованого генератора випадкових бітів (НГВБ) автоматично проводиться його безперервне тестування. Результат самотестування, який свідчить про помилку, повертається при звертанні до НГВБ через бібліотеку взаємодії спеціалізованим програмним забезпеченням Виробу.

3.3. Забороняється використовувати Виріб якщо результат самотестування або результат безперервного тестування НГВБ свідчить про його неправильне функціонування.

4. ДІЇ ПЕРСОНАЛУ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

4.1. Усі адміністратори безпеки та користувачі Виробу повинні бути ознайомлені з цією Інструкцією, планами евакуації з приміщень, іншими розпорядчими документами щодо дій персоналу у надзвичайних ситуаціях.

4.2. У всіх приміщеннях біля дверей на видному місці повинні бути розміщені таблички з номерами телефонів посадових осіб, диспетчерів, служби охорони, аварійних служб, швидкої допомоги.

4.3. У всіх приміщеннях біля дверей на видному місці повинні бути розміщені вуглекислотні або порошкові вогнегасники.

4.4. Порядок дій служби охорони будівель, де розташовані приміщення при взаємодії з відповідальними особами в звичайних умовах та при надзвичайних ситуаціях обумовлюється у відповідних внутрішньо-об’єктових інструкціях, які затверджуються і узгоджуються у встановленому порядку.

4.5. У разі порушення нормальних умов життя і діяльності людей, спричинене аварією, катастрофою, стихійним лихом чи іншою небезпечною подією, яка призвела (може призвести) до загибелі людей та (або) значних матеріальних втрат користувач має припинити використання виробу, вимкнути ПЕОМ та зберігати Виріб у порядку зберігання Виробу у неробочий час (п.2.11 цієї Інструкції).

5. ДІЇ У ВИПАДКУ КОМПРОМЕТАЦІЇ АБО ПІДОЗРИ НА КОМПРОМЕТАЦІЮ КЛЮЧІВ

5.1. Дії користувачів при втраті Виробу або компрометації ключових даних, що містяться в ньому:

- користувач повідомляє адміністратора безпеки про втрату Виробу або компрометацію ключових даних;
- користувач разом з адміністратором безпеки вживають заходів щодо блокування можливості використання втрачених (скомпрометованих) ключових даних;
- адміністратор безпеки повідомляє керівництво організації, в якій використовується Виріб, про компрометацію ключових даних користувача та проводить службове розслідування з метою попередження подібних ситуацій в майбутньому.

5.2. Дії користувачів Виробу у разі підозри на компрометацію ключових даних, що містяться в них:

- користувач припиняє використання Виробу та повідомляє адміністратора безпеки про підозру на компрометацію ключових даних;
- користувач разом з адміністратором безпеки вживають заходів щодо блокування можливості використання ключових даних, щодо яких виникла підозра компрометації;
- адміністратор безпеки проводить службове розслідування з метою з’ясування того, чи насправді відбувся факт компрометації;
- у разі, якщо факт компрометації підтвердився, виконуються дії, наведені в п.5.1 цієї Інструкції. В іншому випадку вживаються дії щодо поновлення можливості використання цих ключових даних.

5.3. При виявленні користувачем пошкодження корпусу Виробу, інших ознак зовнішнього втручання до Виробу, інших зловмисних дій зовнішніх або внутрішніх порушників:

- користувач припиняє використання Виробу та повідомляє про виявлений випадок адміністратора безпеки та виконуються дії, наведені в п.5.1 цієї Інструкції.

5.4. При виявленні користувачем або адміністратором безпеки встановлення на ПЕОМ іншого програмного забезпечення, окрім дозволеного адміністратором безпеки, або зараження ПЕОМ вірусами:

- користувач припиняє використання Виробу та повідомляє про виявлений випадок адміністратора безпеки;
- користувач разом з адміністратором безпеки вживають заходів щодо блокування можливості використання втрачених (скомпрометованих) ключових даних;
- адміністратор безпеки проводить службове розслідування з метою з’ясування того, чи відбувся факт компрометації ключів;
- адміністратор безпеки проводить видалення недозволеного ПЗ або ліквідацію зараження;
- у разі, якщо факт компрометації підтвердився, виконуються дії, наведені в п.5.1 цієї Інструкції. В іншому випадку вживаються дії щодо поновлення можливості використання цих ключових даних.

6. ПОРЯДОК ПРОВЕДЕННЯ КОНТРОЛЮ ЗА СТАНОМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ ВИРОБУ

6.1. В організаціях, в яких використовується Виріб, адміністратором безпеки здійснюється поточний та щорічний контроль.

6.2. Контроль за станом забезпечення безпеки полягає в контролі адміністратором безпеки за виконанням вимог цієї Інструкції, внутрішніх інструкцій організації із контролю матеріальних цінностей та вимог нормативно-правових актів в сфері криптографічного захисту інформації.

6.3. Результати щорічного контролю стану забезпечення безпеки експлуатації Виробу оформляються звітом, який затверджується керівником організації, в якій використовується Виріб.

7. ПОРЯДОК ДОПУСКУ В ПРИМІЩЕННЯ, В ЯКИХ РОЗМІЩУЄТЬСЯ ВИРІБ

7.1. Організація що використовує Виріб має визначити порядок доступу до приміщень у яких експлуатується Виріб у відповідних внутрішньо-об’єктових інструкціях.

Додаток 1

ПАМ’ЯТКА КОРИСТУВАЧУ

Виріб призначений для захисту відкритої та конфіденційної інформації від загроз порушення її цілісності, конфіденційності, автентичності та неспростовності, яка надходить, зберігається та оброблюється в системах оброблення інформації.

Виріб може бути використаний для криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.

Виріб може бути використаний в якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.

Користувачами Виробу є відповідальні посадові особи, поділені на дві категорії: адміністратор безпеки та користувач.

Адміністратор безпеки відповідає за введення в експлуатацію, налаштування параметрів безпеки та виведення з експлуатації Виробу.

Користувач відповідає за:
- генерацію ключових даних;
- використання ключових даних для здійснення криптографічних перетворень;
- знищення ключових даних;
- контроль працездатності Виробу.

Користувач зобов’язаний:
- знати і виконувати вимоги Інструкції щодо забезпечення безпеки експлуатації та Інструкції щодо порядку генерації ключових даних і поводження з ключовими документами, дотримуватись режиму безпеки в роботі;
- зберігати ПЕОМ до якої підключається Виріб (або яка має доступ до Виробу) у порядку, що унеможливлює її несанкціоноване використання іншими особами;
- здійснювати заходи щодо недопущення втрати, крадіжки та несанкціонованого доступу до Виробу;
- не використовувати Виріб за призначенням у разі компрометації ключових даних;
- негайно інформувати адміністратора безпеки про випадки втрати Виробу, порушення його працездатності, компрометації ключових даних або підозрі на таку компрометацію.

Користувачу забороняється:
- розголошувати склад ключових даних або паролі доступу до Виробу;
- передавати Виріб іншим особам;
- використовувати Виріб, що має ознаки зовнішнього втручання або проявляє ознаки неправильного функціонування;
- встановлювати на ПЕОМ до якої підключається Виріб (або яка має доступ до Виробу) інше програмне забезпечення, окрім дозволеного адміністратором безпеки;
- обробляти з використанням Виробу відомості, які становлять державну таємницю.

Користувач має право:
- оскаржити дії чи бездіяльність адміністратора безпеки пов’язані з функціонуванням Виробу.

Експлуатація Виробу здійснюється у відповідності до *Настанови щодо експлуатування.*

Контактна інформація адміністратора безпеки Виробу

_____
(заповнюється в організації, що використовує Виріб)
_____