Прим. № __

ЗАТВЕРДЖУЮ

Директор
ТОВ «АЙ-ДЖИ-ЕМ»

_____ А.Ю. Шаманський

«14» серпня 2020 р.

# Інструкція про порядок генерації ключових даних та поводження із ключовими документами програмного комплексу «Варта»

**804.36002112.466452-02.92.03**

**2020 р.**

## Зміст

1 Галузь застосування ..... 3
2 Загальні положення ..... 4
3 Організація ключової системи ..... 5
3.1 Склад ключової системи ..... 5
3.2 Носії ключової інформації ..... 5
3.3 Термін дії ключових даних та носіїв ключової інформації ..... 5
3.4 Порядок постачання ключів ..... 6
4 Порядок обліку та зберігання носіїв ключової інформації ..... 6
4.1 Порядок обліку носіїв ключової інформації ..... 6
4.2 Порядок зберігання носіїв ключової інформації ..... 6
5 Порядок використання ключів користувачів ..... 7
6 Порядок знищення ключових даних та носіїв ключової інформації ..... 8

# 1 Галузь застосування

Цей документ визначає порядок поводження (обліку, зберігання, знищення) з ключовими документами, що мають обіг в інформаційно-телекомунікаційних системах (далі - ІТС), в яких використовується програмний комплекс «Варта» (далі – програмний комплекс).

Цей документ обов'язковий для виконання користувачами та обслуговуючим персоналом ІТС, в яких використовується програмний комплекс.

# 2 Загальні положення

Програмний комплекс призначений для забезпечення криптографічного захисту електронних документів з метою їх подальшого зберігання або передачі каналами телекомунікаційного зв'язку, а також для управління ключовими даними користувачів.

Програмний комплекс призначений для захисту конфіденційної та відкритої інформації (крім службової та такої, що становить державну таємницю), від загрози порушення конфіденційності, цілісності та автентичності.

Для симетричного шифрування даних програмний комплекс використовує криптографічні алгоритми шифрування, визначені ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014, а також алгоритми DES, TDEA, AES відповідно до ISO/IEC 18033-3:2015.

Для формування та перевірки електронного підпису програмний комплекс використовує криптографічний алгоритм, визначений ДСТУ 4145-2002, а також алгоритм ECDSA відповідно до ДСТУ ISO/IEC 14888-3:2015 та алгоритм RSA відповідно до IETF RFC 3447.

Для узгодження сеансових (разових) ключів використовується протокол узгодження ключів, визначений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739.

Особисті та відкриті ключі електронного підпису для алгоритму ДСТУ 4145-2002 та протоколу узгодження ключів, визначеного наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 формуються згідно вимог ДСТУ 4145-2002, особисті та відкриті ключі для алгоритму ECDSA – відповідно до вимог ДСТУ ISO/IEC 15946-1:2015, особисті та відкриті ключі для алгоритму RSA - відповідно до вимог IETF RFC 3447.

Детально права та обов'язки користувачів програмного комплексу викладені у «Інструкції із забезпечення безпеки експлуатації програмного комплексу» (804.38777989.466452-02.91.01).

# 3 Організація ключової системи

## 3.1 Склад ключової системи

В ІТС повинні використовуватися наступні ключові дані:

- особистий і відкритий ключі алгоритму ДСТУ 4145-2002, що застосовуються для електронного підпису та протоколу узгодження ключів;
- особистий і відкритий ключі алгоритму ECDSA, що застосовуються для електронного підпису та протоколу узгодження ключів;
- особистий і відкритий ключі алгоритму RSA, що застосовуються для електронного підпису та асиметричного шифрування даних;
- ключові дані (сеансовий (разовий) ключ та довгостроковий ключовий елемент (далі - ДКЕ)) для алгоритму шифрування, визначеного ДСТУ ГОСТ 28147:2009;
- сеансові (разові) ключі алгоритмів шифрування DES, TDEA, AES.

Особисті та відкриті ключі генеруються програмним комплексом. Особисті ключі зберігаються в файлових контейнерах на носіях ключової інформації. Відкриті ключі зберігаються у складі сертифікатів відкритих ключів.

Сеансовий (разовий) ключ генерується новий для кожного повідомлення, яке повинно бути зашифроване, або узгоджується між абонентами відповідно до протоколу узгодження ключів, визначеного наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739.

Довгостроковий ключовий елемент отримується з сертифікатів відкритих ключів.

## 3.2 Носії ключової інформації

В якості носіїв ключової інформації, що використовуються в ІТС, застосовуються такі носії даних:

- для розміщення особистих ключів користувачів – зовнішній носій даних типу CD-R, DVD-R, гнучкий диск, flash-memory тощо, або жорсткі диски ПЕОМ ІТС;
- для розміщення відкритих ключів користувачів – жорсткі диски ПЕОМ ІТС.

## 3.3 Термін дії ключових даних та носіїв ключової інформації

Термін дії для особистих ключів дорівнює терміну дії відповідних їм відкритих ключів. Термін дії відкритих ключів визначається терміном чинності відповідних сертифікатів відкритих ключів.

Термін чинності сертифікатів відкритих ключів визначається не повинен перевищувати 2 роки.

Термін дії ДКЕ обмежується терміном дії відкритого ключа, до сертифікату якого він входить.

Термін дії сеансового ключа обмежується часом зашифрування та розшифрування повідомлення.

Термін дії особистих та відкритих ключів, а також ДКЕ починається з моменту формування відповідних сертифікатів відкритих ключів.

Термін дії носіїв ключової інформації дорівнює терміну дії ключових даних, які на них розміщені.

По закінченню терміну дії ключів вони повинні бути змінені.

### 3.4 Порядок постачання ключів

Особисті ключі на носіях формуються користувачами ІТС самостійно за допомогою програмного комплексу.

Відповідні сертифікати відкритих ключів формуються надавачами електронних довірчих послуг за відповідною заявкою користувачів ІТС.

## 4 Порядок обліку та зберігання носіїв ключової інформації

### 4.1 Порядок обліку носіїв ключової інформації

Відповідальна особа організації, в якій експлуатується програмний комплекс, надає користувачу пам'ятку (друковану або в електронному вигляді) щодо поводження із носіями ключової інформації (додаток 1 до цієї Інструкції).

Вимог до обов'язкового обліку носіїв ключової інформації користувачів не висувається.

### 4.2 Порядок зберігання носіїв ключової інформації

Носій ключової інформації зберігається у користувача із забезпеченням неможливості несанкціонованого доступу до нього. Користувач є відповідальним за надійне збереження носія ключової інформації та унеможливлення несанкціонованого доступу до нього.

Всі носії ключової інформації зберігаються протягом терміну їх дії.

При зберіганні носіїв ключової інформації категорично забороняється передавати іншим особам ці носії або паролі доступу до них, а також дозволяти застосовувати їх іншим особам.

# 5 Порядок використання ключів користувачів

Для використання свого особистого ключа користувач приєднує носій ключової інформації до ПЕОМ (якщо носій є з'ємним) та вводить пароль доступу до нього.

Введення паролю доступу до носія ключової інформації повинно здійснюватися таким чином, щоб не допустити ознайомлення з ним сторонніх осіб.

Після закінчення роботи користувач відключає носій ключової інформації (якщо носій є з'ємним) та зберігає його із забезпеченням неможливості несанкціонованого доступу до нього.

# 6 Порядок знищення ключових даних та носіїв ключової інформації

Знищення особистого ключа електронного підпису та/або протоколу розподілу ключів користувача здійснюється користувачем особисто.

Знищення ключових даних на носії ключової інформації здійснюється шляхом видалення відповідного файлу ключового контейнера (в разі, якщо носій даних дозволяє таке видалення) або шляхом фізичного знищення носія (в разі, якщо носій не дозволяє видалення файлів, наприклад, є носієм даних однократного запису).

Додаток 1

# ПАМ'ЯТКА КОРИСТУВАЧУ ЩОДО ПОВОДЖЕННЯ ІЗ НОСІЯМИ КЛЮЧОВОЇ ІНФОРМАЦІЇ

## 1. Загальні положення

Програмний комплекс «Варта» (далі – програмний комплекс) призначений для забезпечення криптографічного захисту електронних документів з метою їх подальшого зберігання або передачі каналами телекомунікаційного зв'язку, а також для управління ключовими даними користувачів.

Програмний комплекс призначений для захисту конфіденційної та відкритої інформації (крім службової та такої, що становить державну таємницю).

## 2. Обов'язки користувача програмного комплексу

Користувач зобов'язаний:

- зберігати особистий ключ, носій ключової інформації, на якому він розміщений, та пароль доступу до нього у таємниці, не допускати використання особистого ключа іншими особами;
- не використовувати особистий ключ у разі його компрометації;
- негайно інформувати надавача електронних довірчих послуг, що видав сертифікат відкритого ключа, про такі події, що трапилися до закінчення строку чинності сертифіката відкритого ключа, а саме:
  - втрату або компрометацію власного особистого ключа або носія ключової інформації, на якому він розміщується;
  - втрату контролю щодо власного особистого ключа через компрометацію або втрату паролю доступу до носія ключової інформації, на якому він розміщується;
  - виявлену неточність або зміну даних, зазначених у власному сертифікаті відкритого ключа;
- підтримувати у робочому стані програмно-технічні засоби згідно вимог експлуатаційної документації;
- забезпечувати цілісність програмного комплексу;
- виключати можливість впливу на програмний комплекс або на його роботу інших осіб або програмно-технічних засобів.

Користувачу забороняється:

- обробляти засобами програмного комплексу інформацію, що містить відомості, які становлять державну таємницю або конфіденційну інформацію, що є власністю держави;
- передавати носій ключової інформації іншим особам, виводити значення особистих ключів та інших ключових даних на дисплей, принтер або інші засоби візуального відображення інформації;
- повторно використовувати носії ключової інформації без попереднього знищення на них ключової інформації встановленим порядком;
- використовувати носії ключової інформації у режимах, що не передбачені порядком їх штатного застосування;
- при зміні паролю доступу до носія ключової інформації вводити у якості нового значення його попереднє значення;
- застосовувати програмний комплекс, який проявляє явні ознаки неправильного функціонування;
- несанкціоновано вносити зміни до програмного комплексу;

- залишати без контролю увімкнені незаблоковані (засобами операційної системи) комп'ютери, які використовуються при функціонуванні програмного комплексу, після зчитування особистого ключа;
- користувач несе відповідальність за зберігання власного носія ключової інформації та паролю доступу до нього.

### 3. Порядок дій користувача при компрометації ключів та носіїв ключової інформації

Під компрометацією криптографічних ключів мається на увазі втрата, розголошення, несанкціоноване копіювання та інші дії, в результаті яких криптографічні ключі можуть стати доступними несанкціонованим особам.

Криптографічні ключі, відносно яких виникла підозра в компрометації, необхідно негайно вивести з дії.

У випадку компрометації ключових даних, носія ключової інформації або виникнення обґрунтованої підозри щодо такої компрометації користувач негайно повідомляє відповідальну особу організації, в якій використовується програмний комплекс, та надавача електронних довірчих послуг та діє відповідно до вказівок відповідальної особи та згідно регламенту роботи надавача електронних довірчих послуг.