Прим. № __

ЗАТВЕРДЖУЮ

Директор

ТОВ «АЙ-ДЖИ-ЕМ»

А.Ю. Шаманський

«14» серпня 2020 р.

Інструкція із забезпечення безпеки експлуатації програмного комплексу «Варта»

804.36002112.466452-02.91.01

2020 р.

Зміст

1 ГАЛУЗЬ ЗАСТОСУВАННЯ 3
2 ЗАГАЛЬНІ ПОЛОЖЕННЯ 4
3 ОБОВ'ЯЗКИ ТА ПОВНОВАЖЕННЯ ОБСЛУГОВУЮЧОГО ПЕРСОНАЛУ 5
3.1 Права та обов'язки відповідальної особи 5
3.2 Права та обов'язки користувачів 5
4 ПОРЯДОК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ ПРОГРАМНОГО КОМПЛЕКСУ 7
4.1 Порядок забезпечення безпеки експлуатації комплексу під час його встановлення (інсталяції програмного забезпечення), експлуатації, виведення з експлуатації, ремонту, а також у разі порушення функціонування 7
4.1.1 Організація та здійснення робіт 7
4.1.2 Вимоги до персоналу 7
4.1.3 Забезпечення безпеки під час встановлення та експлуатації 7
4.1.4 Забезпечення безпеки під час виведення з експлуатації, ремонту, а також у разі порушення функціонування 7
4.2 Дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри на компрометацію ключів 8
4.2.1 Загальні положення 8
4.2.2 Дії користувачів програмного комплексу 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, а також потребує виведення програмного комплексу з експлуатації 8
4.2.3 Дії користувачів програмного комплексу у разі несанкціонованого проникнення до приміщень (спроби проникнення) 8
4.2.4 Дії користувачів програмного комплексу при відмові електроживлення 9
4.2.5 Дії користувачів програмного комплексу при виявленні зловмисних дій зовнішніх або внутрішніх порушників або зараженні програм вірусами 9
4.2.6 Дії користувачів програмного комплексу при втраті носіїв ключової інформації або компрометації ключових даних 9
4.2.7 Дії користувачів програмного комплексу при підозрі на компрометацію ключових даних 9
4.3 Порядок проведення контролю за станом забезпечення безпеки програмного комплексу 9
4.4 Порядок допуску в приміщення, в яких встановлений програмний комплекс 10

1 Галузь застосування

Цей документ визначає організаційно-правові основи щодо забезпечення безпеки експлуатації інформаційно-телекомунікаційних систем (надалі – 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 шифрування даних програмний комплекс використовує криптографічний алгоритм шифрування, визначений ДСТУ ГОСТ 28147:2009, а також алгоритми DES, TDEA, AES відповідно до ISO/IEC 18033-3:2015.

Для формування та перевірки електронного цифрового підпису програмний комплекс використовує криптографічний алгоритм, визначений ДСТУ 4145-2002, а також алгоритм RSA відповідно до IETF RFC 3447.

Для узгодження сеансових (разових) ключів ДСТУ ГОСТ 28147:2009 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 цифрового підпису для алгоритму ДСТУ 4145-2002 та протоколу узгодження ключів формуються згідно вимог ДСТУ 4145-2002, особисті та відкриті ключі електронного цифрового підпису для алгоритму RSA - відповідно до вимог IETF RFC 3447.

3 Обов'язки та повноваження обслуговуючого персоналу

3.1 Права та обов'язки відповідальної особи

В організації, що експлуатує програмний комплекс, призначається відповідальна особа (адміністратор), в обов'язки якої входить:

- ведення обліку кожного екземпляру програмного комплексу та експлуатаційної документації до нього, що використовуються в організації;
- розробка нормативних документів, що регламентують питання інформаційної безпеки;
- розробка відповідних інструкцій для користувачів;
- проведення періодичного контролю виконання вимог, описаних в цьому документі, вимог нормативних документів і інструкцій, визначених в організації.

Відповідальна особа несе особисту відповідальність за всі одержані екземпляри програмного комплексу, експлуатаційну і технічну документацію до нього. Передача екземплярів програмного комплексу, експлуатаційної і технічної документації до них допускається тільки користувачам комплексу.

Правом доступу до робочих місць із встановленими екземплярами програмного комплексу повинні володіти лише особи, що пройшли відповідну підготовку. Відповідальна особа повинна ознайомити кожного користувача програмного комплексу з необхідною документацією, а також з іншими нормативними документами, створеними на її основі.

3.2 Права та обов'язки користувачів

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;
- використовувати особистий ключ виключно у порядку, визначеному експлуатаційною документацією;
- не використовувати особистий ключ у разі його компрометації;
- негайно інформувати центр сертифікації ключів про такі події, що трапилися до закінчення строку чинності сертифіката відкритого ключа користувача, 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 яких він розміщується;
  - виявлену неточність або зміну даних, зазначених у власному сертифікаті відкритого ключа;
- використовувати програмний комплекс тільки за призначенням в порядку, визначеному в експлуатаційній документації;
- підтримувати у робочому стані програмно-технічні засоби, які необхідні для роботи програмного комплексу згідно вимог експлуатаційної документації;
- забезпечувати цілісність та незмінність 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;
- розголошувати склад інформації на власному носії ключової інформації або пароль доступу до нього, а також передавати цей носій 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;
- записувати на носії ключової інформації іншу інформацію окрім такої, що передбачена для функціонування програмного комплексу;
- при зміні паролю доступу до носія ключової інформації вводити у якості нового значення його попереднє значення або тривіальне значення;
- застосовувати програмний комплекс, який проявляє явні ознаки неправильного функціонування;
- несанкціоновано вносити зміни до програмного комплексу;
- залишати власний носій ключової інформації у зчитувачі після закінчення роботи з ним;
- залишати без контролю увімкнені незаблоковані (засобами операційної системи) комп'ютери, які використовуються при функціонуванні програмного комплексу, після зчитування особистого ключа.

4 Порядок забезпечення безпеки експлуатації програмного комплексу

4.1 Порядок забезпечення безпеки експлуатації комплексу під час його встановлення (інсталяції програмного забезпечення), експлуатації, виведення з експлуатації, ремонту, а також у разі порушення функціонування

4.1.1 Організація та здійснення робіт

Обов'язки з організації робіт із встановлення, експлуатації, виведення з експлуатації, технічного та гарантійного обслуговування програмного комплексу покладаються на відповідальну особу.

4.1.2 Вимоги до персоналу

До робіт з встановлення, експлуатації, виведення з експлуатації, технічного та гарантійного обслуговування комплексу повинен залучатися обслуговуючий персонал, 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.

Право роботи з програмним комплексом повинен мати персонал, який має відповідні знання, досвід та навички, необхідні для забезпечення виконання ІТС своїх функцій згідно експлуатаційного призначення. Відповідальна особа повинна ознайомити всіх користувачів із вимогами щодо безпечної експлуатації програмного комплексу в складі ІТС. Функції та відповідальність обслуговуючого персоналу повинні бути передбачені їх посадовими обов'язками (посадовими інструкціями).

4.1.3 Забезпечення безпеки під час встановлення та експлуатації

Охорона, розміщення, устаткування та організація режиму роботи у приміщеннях, де експлуатується програмний комплекс, повинні виключати можливість неконтрольованого проникнення або перебування у цих приміщеннях сторонніх осіб, та забезпечувати недопущення крадіжки, втрати, ушкодження обладнання, крадіжки та знищення (руйнування) інформації або інших дій, що можуть привести до виведення технічних засобів із штатного режиму роботи.

4.1.4 Забезпечення безпеки під час виведення з експлуатації, ремонту, а також у разі порушення функціонування

Носії, на яких розміщуються особисті ключі користувачів, за умов позаштатних ситуацій, описаних нижче, або після виходу їх з ладу не підлягають ремонту та знищуються способом, що не дозволяє їх відновлення. Про це складається відповідний акт знищення.

Акти знищення складаються посадовими особами, які проводили знищення (щонайменш, дві посадові особи). Акти знищення складаються в довільній формі та повинні відображати відомості щодо технічних засобів, що знищуються, методи та результати знищення.

Ремонт інших засобів ІТС виконується у порядку, який передбачений для них їх експлуатаційними документами.

4.2 Дії персоналу в умовах надзвичайних ситуацій, стихійного лиха та підозри на компрометацію ключів

4.2.1 Загальні положення

Усі користувачі програмного комплексу повинні бути ознайомлені з цією інструкцією, планами евакуації з приміщень, іншими розпорядчими документами щодо дій персоналу у надзвичайних ситуаціях.

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

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

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.

4.2.2 Дії користувачів програмного комплексу 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, а також потребує виведення програмного комплексу з експлуатації

1) Користувачі негайно вимикають комп'ютери, джерела безперебійного живлення, інші електроприлади.

2) Відповідальна особа вилучає у користувачів носії ключової інформації.

3) Відповідальна особа упаковує носії ключової інформації, носії даних із програмним забезпеченням комплексу, експлуатаційну документації та, за необхідності, інші документи та матеріали у контейнер, опечатує його та виносить у безпечне приміщення або будівлю.

4) Опечатані контейнери повинні знаходитися під охороною до закінчення надзвичайної ситуації та відновлення штатної роботи програмного комплексу.

4.2.3 Дії користувачів програмного комплексу у разі несанкціонованого проникнення до приміщень (спроби проникнення)

Якщо при відкритті приміщень було виявлено, що двері приміщень були відкриті, зламані замки дверей або порушена контрольна печатка, виконуються наступні дії:

1) Забороняється заходити самостійно у приміщення.

2) Особа, що виявила порушення, сповіщає по телефону відповідальну особу про факт та місце проникнення у приміщення.

3) Відповідальна особа сповіщає керівництво організації, в якій використовується програмний комплекс, про факт та місце проникнення у приміщення.

4) Особа, що виявила порушення, знаходиться біля дверей приміщення, не допускаючи у нього нікого до прибуття відповідальних осіб.

4.2.4 Дії користувачів програмного комплексу при відмові електроживлення

1) Користувачі сповіщають по телефону відповідальну особу про факт відмови електроживлення та негайно вимикають комп'ютери, джерела безперебійного живлення, інші електроприлади.

2) Відповідальна особа вживає заходів щодо відновлення електроживлення та поновлення функціонування програмного комплексу.

4.2.5 Дії користувачів програмного комплексу при виявленні зловмисних дій зовнішніх або внутрішніх порушників або зараженні програм вірусами

1) Відповідальна особа негайно повідомляє керівництво організації, в якій використовується програмний комплекс, про виявлені атаки та викритих порушників.

2) Якщо внаслідок зловмисних дій було порушено штатну роботу програмного комплексу, відповідальна особа виконує дії з відновлення його штатної роботи.

3) У разі виявлення зараження вірусами користувачі припиняють роботу, а відповідальна особа проводить ліквідацію зараження та відновлення працездатності програмного комплексу.

4.2.6 Дії користувачів програмного комплексу при втраті носіїв ключової інформації або компрометації ключових даних

1) Користувач направляє заявку на скасування сертифікату відкритого ключа до центру сертифікації ключів, яким був сформований сертифікат відповідного відкритого ключа.

2) Користувач генерує нову пару ключів та направляє заявку на отримання нового сертифікату відкритого ключа до центру сертифікації ключів.

4.2.7 Дії користувачів програмного комплексу при підозрі на компрометацію ключових даних

1) Користувач направляє заявку на блокування сертифікату відкритого ключа до центру сертифікації ключів, яким був сформований сертифікат відповідного відкритого ключа.

2) Відповідальна особа організовує проведення службового розслідування (із залученням усіх необхідних для цього осіб та використанням необхідних технічних засобів), метою якого є з'ясування того чи дійсно мала місце компрометація ключових даних користувача.

3) У випадку, якщо факт компрометації підтвердився, виконуються дії в порядку, встановленому для компрометації особистого ключа.

У випадку, якщо факт компрометації не підтвердився, користувач відправляє заявку на поновлення (розблокування) сертифікату відкритого ключа до центру сертифікації ключів.

4.3 Порядок проведення контролю за станом забезпечення безпеки програмного комплексу

В організаціях, в яких використовується програмний комплекс, поточний контроль за його обігом здійснюється відповідальною особою.

Тестування програмного комплексу здійснюється його користувачем в порядку, встановленому відповідальною особою, у разі виникнення підозри на порушення його цілісності.

4.4 Порядок допуску в приміщення, в яких встановлений програмний комплекс

Програмний комплекс не накладає спеціальних обмежень на присутність в приміщеннях, в яких він встановлений, сторонніх осіб, що не є його користувачами.