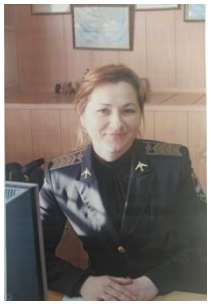
БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ / E-GOVERNANCE SECURITY

DOI: 10.18372/2225-5036.26.15575

СУЧАСНІ КОМПЛЕКСИ ПОСТ-КВАНТОВОЇ БЕЗПЕКИ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Анна Корченко, Євгенія Іванченко, Наталія Кошкіна, Олександр Кузнецов, Олена Качко, Олександр Потій, Віктор Онопрієнко, Всеволод Бобух

КОРЧЕНКО Анна Олександрівна, д.т.н., доцент.
Рік і місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, системи виявлення вторгнень, експертне оцінювання в сфері захисту інформації.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: annakor@ukr.net.
ORCID: 0000-0003-0016-1966.



ІВАНЧЕНКО Євгенія Вікторівна, к.т.н., професор.
Рік і місце народження: 1976 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2000 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, системи виявлення вторгнень, безпека хмарних технологій.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: evivancenko@gmail.com.
ORCID: 0000-0003-3017-5752.

КОШКІНА Наталія Василівна, д.т.н., с.н.с.
Рік та місце народження: 1977 рік, с. Велика Чернеччина, Сумська обл., Україна.
Освіта: Сумський державний педагогічний інститут ім. А.С. Макаренка, 1999.
Посада: старший науковий співробітник Інституту кібернетики ім. В.М. Глушкова НАН України з 2008 р.
Наукові інтереси: інформаційна та кібербезпека, стеганографія, стеганоаналіз.
Публікації: більше 50 наукових публікацій, серед яких монографії, наукові статті та тези.
E-mail: nata.koshkina@gmail.com.
ORCID: 0000-0001-5180-2255.

КУЗНЕЦОВ Олександр Олександрович, д. т. н., професор
Рік та місце народження: 1974 рік, м. Харків, Україна.
Освіта: Харківський військовий університет, 1996 рік.
Посада: професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук Харківського національного університету імені В.Н. Каразіна з 2008 р.
Наукові інтереси: інформаційна та кібербезпека, теорія інформації та кодування, криптографія та стеганографія.
Публікації: більше 300 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: kuznetsov@karazin.ua.
ORCID: 0000-0003-2331-6326.

Качко Олена Григорівна, к.т.н., професор.
Рік та місце народження: 1945 рік, м. Ізюм, Харківської області, Україна.
Освіта: Харківський національний університет радіоелектроніки (Харківський інститут радіоелектроніки), 1967 рік.
Посада: професор кафедри програмної інженерії, з 1999 р., заступник головного конструктору АТ «ІІТ» з 2011р.
Наукові інтереси: інформаційна та кібербезпека, теорія та практика розробки паралельних програм.
Публікації: більше 70 наукових публікацій, серед яких, навчальні посібники, монографії, наукові статті та тези.
E-mail: elena.kachko@nure.ua.
ORCID: 0000-0001-9249-0497.

ПОТІЙ Олександр Володимирович, д.т.н., професор, полковник.
Рік та місце народження: 1971 рік, м. Кривий Ріг, Україна.
Освіта: Харківське вище воєнне командно-інженерне училище ракетних військ стратегічного призначення, 1993 рік; Харківський військовий університет, 1996; Харківський університет Повітряних Сил, 2008.
Посада: Заступник Голови Державної служби спеціального зв'язку та захисту інформації України з 2020 р.
Наукові інтереси: інформаційна та кібербезпека, менеджмент інформаційної безпеки, криптографія.
Публікації: більше 100 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові та методичні статті та тези, національні стандарти, нормативні документи та навчальні курси, патенти.
E-mail: potav1971@gmail.com.
ORCID: 0000-0002-2366-0541.

ОНОПРІЄНКО Віктор Васильович, к.т.н.
Рік та місце народження: 1958 рік, с. Горбані, Переяслав-Хмельницький район, Київська обл., Україна.
Освіта: Київське вище інженерне радіотехнічне училище ППО, 1981 р.
Посада: Генеральний директор з 2015 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 8 наукових публікацій, серед яких, наукові статті.
E-mail: v25258@gmail.com.
ORCID: 0000 0002 1174 8968.

БОБУХ Всеволод Анатолійович, к.т.н.
Рік та місце народження: 1981 рік, м. Харків, Харківська обл., Україна.
Освіта: Харківський національний університет радіоелектроніки, 2002 рік.
Посада: начальник відділу апаратних засобів захисту інформації Приватного акціонерного товариства "Інститут інформаційних технологій".
Наукові інтереси: апаратні та апаратно-програмні засоби захисту інформації.
Публікації: більше 30 наукових публікацій, серед яких монографії, наукові статті, тези та патенти.
E-mail: bobukhv@iit.kharkov.ua.
ORCID: 0000-0002-1175-5092.

Анотація. *На теперішній час в умовах широкого впровадження в економіку, оборонну і безпекову сфери цифрових технологій в усіх провідних державах світу гостро стоїть проблема забезпечення безпеки їх кіберпростору, особливо в умовах нових загроз, що породжуються використанням квантових комп'ютерів. Тому створення в Україні відповідної системи безпеки кіберпросторового довкілля національної критичної інформаційної інфраструктури, зокрема комплексів та засобів виявлення вторгнень, криптографічного та стеганографічного захисту інформації, є сучасною та актуальною проблематикою, що безпосередньо стосується пост-квантової інформаційної та кібербезпеки нашої держави, а також має важливе загальнодержавне та оборонне значення і суттєво впливає на забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн. Виходячи з актуальності проблеми забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн, метою є удосконалення систем спеціального призначення за рахунок побудови комплексів криптографічного захисту інформації пост-квантової безпеки Державних електронних інформаційних ресурсів. Реалізовано проекти з розробки та впровадження програмно-технічних комплексів та апаратних засобів КЗІ для надавачів електронних довірчих послуг*

Збройних сил України, Міністерства внутрішніх справ, Державної прикордонної служби, Державної податкової служби України, Національного банку України, Приватбанку, Укрсіббанку, Альфа банку тощо, включно по два технологічні центри сертифікації ключів для Центрального засвідчувального органу України та засвідчувального центру Національного банку України. Таким чином, розроблені програмно-технічні комплекси та апаратні засоби КЗІ створили безпечне пост-квантове довкілля для державних електронних інформаційних ресурсів.

***Ключові слова**: мереж передачі даних спеціального призначення, криптографічні засоби, комплекси спеціального призначення, засоби захисту інформації, кіберпростір, пост-квантове довкілля, державні електронні інформаційні ресурси.*

Вступ

На даний час в умовах широкого впровадження в економіку, оборонну і безпекову сфери цифрових технологій в усіх провідних державах світу гостро стоїть проблема забезпечення безпеки їх кіберпростору, особливо в умовах нових загроз, що породжуються використанням квантових комп'ютерів

Для України ця проблема ще більш актуальна, адже з 2014 року проти нашої держави йде широкомасштабна гібридна та інформаційна агресія, одним з ефективних елементів якої є високотехнологічні впливи на державну інформаційну та критичну інфраструктуру.

Тому створення в Україні відповідної системи безпеки кіберпросторового довкілля, національної критичної інформаційної інфраструктури [2], зокрема комплексів та засобів виявлення вторгнень [3, 4], криптографічного [1] та стеганографічного [5] захисту інформації, є сучасною та актуальною проблематикою, що безпосередньо стосується пост-квантової інформаційної та кібербезпеки нашої держави, а також має важливе загальнодержавне та оборонне значення і суттєво впливає на забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн.

На теперішній час нашій державі створено необхідні засади для розгортання та побудови високотехнологічних пост-квантових безпечних мереж передачі даних спеціального призначення виключно на вітчизняному обладнанні криптографічного захисту інформації (КЗІ).

У [6] авторами роблено основні елементи загальнодержавної системи КЗІ, що стали основою стандартизації систем, комплексів та засобів КЗІ пост-квантової безпеки.

Для України актуальним є створення реальної системи пост-квантової безпеки. Це пов'язане з необхідністю розробки комплексів КЗІ для забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими і серверними частинами прикладних систем (TCP-з'єднань) або у розподілених системах на основі IP-мереж передачі даних.

Зазначені функції комплекси повинні виконувати шляхом застосування механізмів КЗІ, яка передається між клієнтом та сервером, зовнішніми каналами зв'язку або у вигляді мережевого IP-потоку між розподіленими локальними обчислювальними мережами (далі – ЛОМ) або між клієнтами та ЛОМ через зовнішні канали зв'язку.

Мета роботи

Виходячи з актуальності проблеми забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн, метою роботи є удосконалення систем спеціального призначення за рахунок побудови комплексів КЗІ пост-квантової безпеки державних електронних інформаційних ресурсів.

Постановка задачі

Для досягнення поставленої мети необхідно розробити технічні характеристики та побудувати криптографічні засоби захисту інформації для використання у вітчизняних комплексах спеціального призначення та обґрунтувати доцільність використання окремих рішень та виконаних впроваджень вітчизняних засобів захисту інформації при побудові мереж та комплексів спеціального призначення на рівні держави. Стосовно захисту електронних інформаційних ресурсів, розглянемо основні результати з розробки та дослідження зазначених засобів захисту інформації та їх практичне застосування в пост-квантовому довкіллі, основою побудови яких слугували наукові результати, отримані в [6].

Комплекс користувача ЦСК "ІІТ РИСТУВАЧ ЦСК-1"

Комплекс у складі системи електронного документообігу чи іншої прикладної системи (далі - системи) призначений для: автентифікації користувачів системи при підключенні до сервера та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером; забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Зазначені функції комплекс виконує шляхом застосування механізмів КЗІ, яка обробляється у системі. Автентифікація користувачів системи на сервері здійснюється під час підключення користувачів до сервера (встановлення з'єднання з сервером) шляхом реалізації протоколу взаємної автентифікації сторін. Забезпечення конфіденційності та цілісності інформації, яка передається між користувачем та сервером системи під час їх взаємодії, реалізується шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, реалізуються шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача системи так і на стороні сервера. Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритми шифрування за

ДСТУ ГОСТ 28147: 2009 та TDEA і AES за ISO/IEC 18033-3:2010; алгоритми ЕЦП за ДСТУ 4145-2002, RSA за PKCS#1 (RFC 3447) та ECDSA за ДСТУ ISO/IEC 14888-3:2014; алгоритми гешування за ГОСТ 34.311-95 та SHA (SHA-1 і SHA-224/256/ 384/512) за ДСТУ ISO/IEC 10118-3:2005; протоколи розподілу ключів за ДСТУ ISO/IEC 15946-3 (пп. 8.2) та RSA за PKCS#1 (RFC 3447).

Протоколи розподілу ключових даних реалізуються згідно ДСТУ ISO/IEC 15946-3 і вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р., та за алгоритмом направленого шифрування RSA згідно PKCS#1 (RFC 3447). Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України.

Протокол встановлення захищеного сеансу передачі даних користувачем та сервером реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3. Протокол взаємної автентифікації включає: формування користувачем та передачу даних автентифікації (запиту) на сервер; обробку запиту від користувача сервером; прийом та обробку відповіді користувача від сервера.

За результатом роботи протоколу на сервері та користувачеві встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES.

В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з'єднанні використовуються коди автентифікації повідомлень (імітовставки), які обчислюються за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES.

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та сервера системи.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера системи відносяться особисті ключі та сертифікати відповідно користувачів та сервера. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"), Aladdin eToken/JaCarta, Автор SecureToken, Технотрейд uaToken, SafeNet iKey, Giesecke&Devrient StarSign, Gemalto IDPrime, ДБОСофт iToken та Ефіт Key; смарт-карти "Карта-1" ("ІІТ Смарт-карта Карта-1"), Техноконсалтинг TEllipse, Aladdin eToken /JaCarta, Автор CryptoCard, Giesecke &Devrient StarSign та ДБОСофт Інтегра; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера системи, надання послуг фіксування часу, а також надання (за необхідності) користувачам системи засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів користувачів та сервера системи; надання послуг фіксування часу; надання користувачам системи (за необхідності) засобів генерації особистих та відкритих ключів.

Для взаємодії з центром сертифікації ключів (використання його інтерактивних служб) користувачі та сервери системи повинні мати можливість мережевого підключення до ЦСК. Усі механізми взаємодії з ЦСК виконують бібліотеки користувача ЦСК.

Зміна статусу сертифікатів (блокування, поновлення або скасування) та знищення особистих ключів користувачів та сервера системи здійснюється у відповідності до порядку, який визначений ЦСК (згідно регламенту ЦСК).В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

До складу комплексу входять: програмні засоби (бібліотеки) КЗІ (користувача ЦСК) "ІІТ Користувач ЦСК-1"; апаратні засоби КЗІ. До складу апаратних засобів комплексу можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301"). Структурна схема комплексу захисту наведена на рис. 1.

Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси. Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережеві криптомодулі тощо.

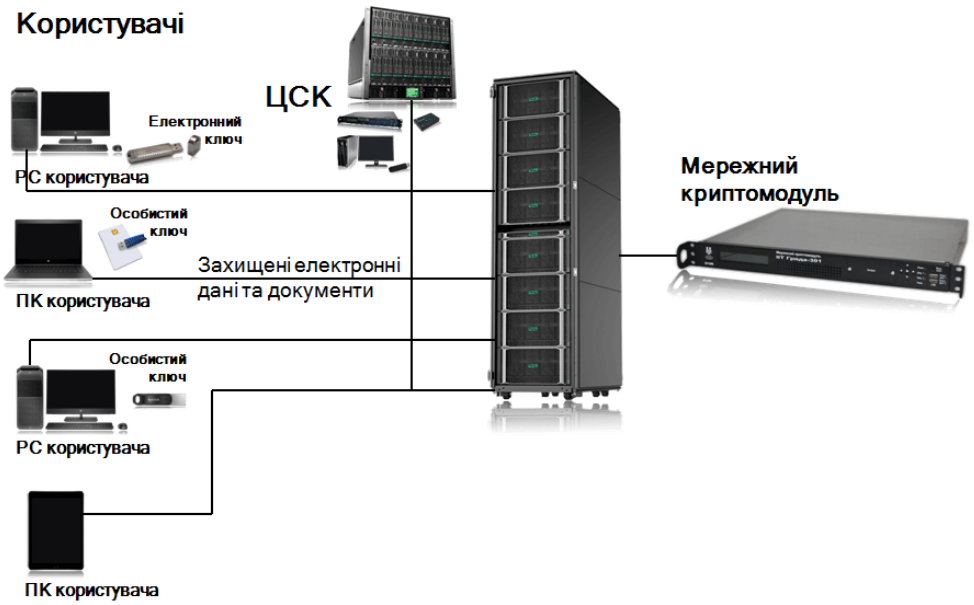


Рис. 1. Структурна схема комплексу захисту

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС), що включає зашифрування та розшифрування даних, формування та перевірку ЕЦП від даних, захист сеансів передачі даних (захист з'єднань; інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК); отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Бібліотеки користувача ЦСК інтегруються у зазначену систему (та інші прикладні системи) через визначені інтерфейси (Microsoft CSP, PKCS#11, GSS-API, JCA) і власні та реалізовані для ОС Microsoft Windows, Linux (SuSe/Red Hat/Ubuntu /Cent OS та ін.), UNIX (IBM AIX/Sun Solaris/Free BSD та ін.), Apple macOS/iOS, Google Android у вигляді бібліотек підключення (DLL/COM, SO, DyLib – 32/64-біта) або у вигляді архівів java-класів для JRE чи java-скриптів тощо. Для всіх бібліотек користувача ЦСК під всі ОС та платформи, що підтримуються, існують приклади використання. Бібліотеки користувача ЦСК інтегровані у різні прикладні системи, серед яких: більше 200 корпоративних та внутрішньовідомчих систем, а також електронних реєстрів тощо; системи електронної пошти (поштові клієнти та сервери): Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС-Он-Лайн Foss Mail та ін.; офісні пакети: Microsoft Office, Adobe Acrobat та ін.; системи електронного документообігу: Інфо+ АСКОД, ТрансЛінкКонсалтинг Док-Проф, Софтлайн Мегаполіс та ін.; системи подання звітності у електронному вигляді до Державної податкової служби України, Пенсійного фонду України, Держфінмоніторингу, МВС України та ін.; автоматизовані та інтегровані банківські системи: SAP for Banking, Oracle FlexCube та ін.; власні засоби та комплекси КЗІ.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів користувача системи. Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера системи. На сервері системи встановлюються та використовуються наступні складові частини комплексу: програмний комплекс захисту сервера, який включає бібліотеки користувача ЦСК (для відповідної серверної ОС); апаратний засіб КЗІ - мережевий криптомодуль.

На засобах користувачів системи (робочих станціях чи портативних комп'ютерах - РС та ПК) встановлюються та використовуються наступні складові частини комплексу: програмний комплекс захисту користувача, який включає бібліотеки користувача ЦСК (для відповідної ОС); апаратний засіб КЗІ - електронний ключ. Електронний ключ "Кристал-1" призначений для: автентифікації користувача системи перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача.

Мережевий криптомодуль "Гряда-301" призначений для: автентифікації сервера системи перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до сервера системи безпосередньо або через комутатори локальної обчислювальної мережі. Апаратна реалізація мережевого криптомодуля забезпечує

захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку сервера системи.

Програмно-технічний комплекс центру сертифікації КЛЮЧІВ (ЦСК) "ІІТ ЦСК-1"

Призначення комплексу: реалізація ЦСК регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів ЦСК (далі – користувачів), надання послуг фіксування часу, надання користувачам засобів ЕЦП та шифрування, а також засобів генерації особистих і відкритих ключів. Технічні засоби комплексу об'єднані у ЛОМ з використанням внутрішньої комунікаційної мережі з наявністю підключення до зовнішніх комунікаційних мереж.

Окремі технічні засоби комплексу ізольовані від мереж передачі даних. Порядок експлуатації комплексу у складі ЦСК відповідає вимогам правил посиленої сертифікації. Структурна схема комплексу наведена нижче (рис. 2).

Комплекс забезпечує реалізацію регламентних процедур та механізмів роботи ЦСК, пов'язаних з: обслуговуванням сертифікатів відкритих ключів (далі – сертифікатів) користувачів, що включає: реєстрацію користувачів, сертифікацію відкритих ключів користувачів, розповсюдження сертифікатів, управління статусом сертифікатів, розповсюдження інформації про статус сертифікатів; надання послуг фіксування часу; надання користувачам засобів ЕЦП та шифрування даних, а також засобів генерації та управління ключами.

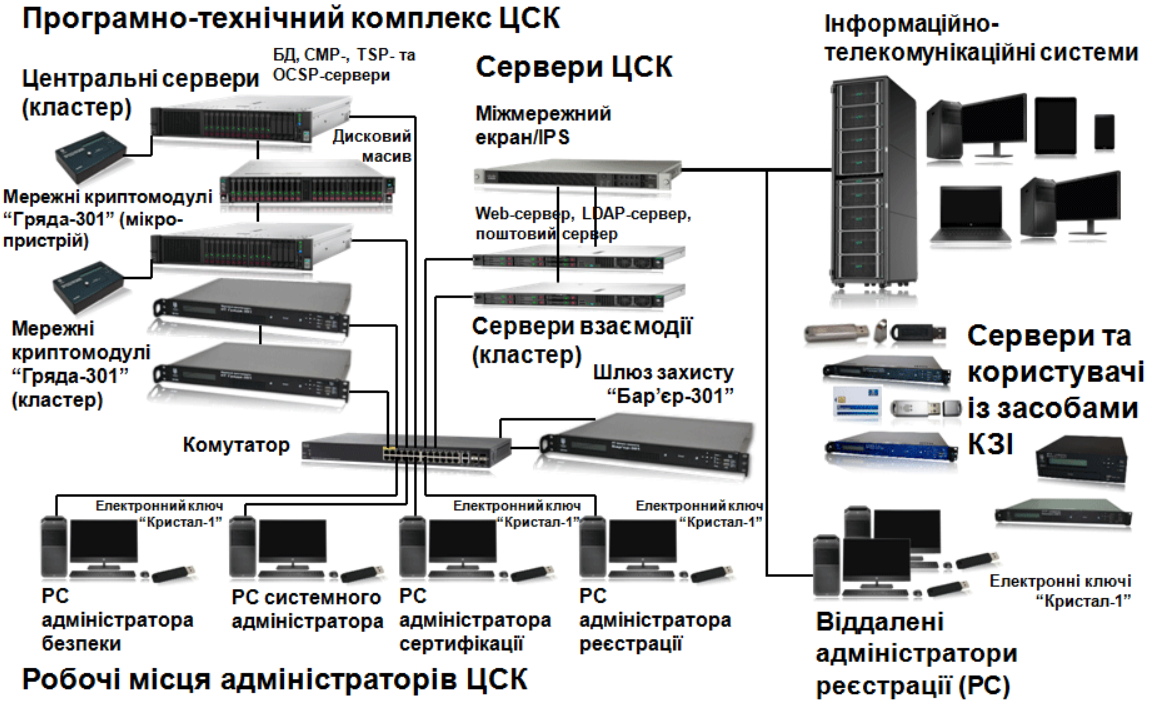


Рис. 2. Структурна схема комплексу

Комплекс забезпечує виконання наступних функцій, пов'язаних з обслуговуванням ЦСК сертифікатів користувачів: реєстрацію користувачів; сертифікацію відкритих ключів користувачів; розповсюдження сертифікатів відкритих ключів користувачів; управління статусом сертифікатів відкритих ключів користувачів та розповсюдження інформації про статус сертифікатів. Комплекс забезпечує виконання наступних функцій, пов'язаних з наданням ЦСК послуг фіксування часу: приймання та реєстрацію запитів користувачів на формування позначок часу; формування позначок часу; передачу сформованих позначок часу користувачам; внесення сформованих позначок часу у базу даних; зберігання сформованих позначок у базі даних; архівування бази даних позначок часу. До складу комплексу входять засоби користувачів у складі: засобів генерації особистих і відкритих ключів користувачів, які призначені для генерації особистого та відкритого ключів користувача, формування та передачу запиту на формування сертифіката користувача до ЦСК, отримання, перевірку, зберігання та використання сформованого сертифікату, формування та передачу запитів на блокування, скасування та поновлення сертифіката користувача до ЦСК; засобів ЕЦП та шифрування даних користувачів.

До складу комплексу входять такі технічні засоби: робочі станції (РС) обслуговуючого персоналу (адміністратора безпеки, системного адміністратора та адміністратора реєстрації); центральні сервери (сервери ЦСК); внутрішнє комунікаційне обладнання локальної обчислювальної мережі (ЛОМ); сервери взаємодії; міжмережевий екран (МЕ) та система виявлення втручань (IDS); комунікаційне обладнання для підключення до зовнішніх комунікаційних мереж (ЗКМ); РС генерації ключів користувачів (ізольована); РС віддалених адміністраторів реєстрації (відокремлені).

Окремо (до складу програмно-технічного комплексу відокремленого пункту реєстрації) входить РС віддаленого адміністратора. РС адміністратора безпеки, адміністратора сертифікації, системного адміністратора, адміністратора реєстрації, центральні сервери та сервери взаємодії мають взаємодіяти через внутрішню комунікаційну мережу на основі кабельної мережі та комутаторів і утворювати ЛОМ. Центральні сервери, сервери взаємодії, їх ДБЖ, мережевий комутатор, комутатор терміналів, МЕ, а також криптомодулі і мережні криптомодулі мають бути розміщені у екранованій шафі чи у звичайні шафі у екранованому приміщенні.

У випадку, якщо функції центральних серверів, що пов'язані з формуванням сертифікатів та списків відкликаних сертифікатів (під час яких використовується особистий ключ ЦСК) виконує РС адміністратора сертифікації, вона має бути реалізована на основі ПЕОМ у захищеному виконанні або розміщена у екранованій кабіні чи екранованому приміщенні. Сервери можуть бути з'єднані у окрему ЛОМ з використанням власного комутатора та підключатися до комутатора РС через електричний кабель або волоконно-оптичну лінію зв'язку (ВОЛЗ). Можливе також об'єднання комутаторів серверів та РС у один спільний комутатор ЛОМ. У цьому випадку РС обслуговуючого персоналу підключають до комутатора окремими електричними кабелями чи ВОЛЗ.

Сервери взаємодії мають підключатися до зовнішньої комунікаційної мережі через зовнішній МЕ (із вбудованою IPS). Для підключення серверів взаємодії до комутатора та до МЕ мають використовуватися різні мережні адаптери.

МЕ з IPS мають підключатися до зовнішньої комунікаційної мережі через комунікаційне обладнання оператора послуг передачі даних через електричний кабель або через ВОЛЗ. У випадку використання для такого підключення ВОЛЗ, мають використовуватися або оптичні мережні порти МЕ або конвертори довкілля.

Для забезпечення централізованого моніторингу роботи складових частин комплексу до його складу може входити система моніторингу. Серверна частина системи моніторингу може встановлюватися на РС системного адміністратора або на окремий сервер моніторингу, а на всі сервери та РС комплексу мають бути встановлені агенти системи моніторингу. Взаємодія сервера з агентами моніторингу здійснюється за внутрішнім протоколом, а з іншими вузлами - за стандартними протоколами моніторингу (syslog, SNMP тощо). Комплекс взаємодіє з ПТК центрів та ІТС інших зовнішніх користувачів через сервери взаємодії. Функціональною основою комплексу є спеціалізовані апаратні та програмні засоби КЗІ і включає: програмний комплекс ЦСК "ІІТ ЦСК-1"; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301"); програмний комплекс віддаленого адміністратора реєстрації ЦСК "ІІТ ЦСК-1. Віддалений адміністратор реєстрації"; програмний комплекс користувача ЦСК "ІІТ Користувач ЦСК-1"; електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"). Мережевий криптомодуль "Гряда-301" (мікро-пристрій) призначений для апаратної реалізації формування ЕЦП і у складі центральних серверів чи РС адміністратора сертифікації і забезпечує використання та захист особистого ключа ЦСК. Особистий ключ ЦСК генерується, зберігається та використовується тільки у середині пристрою. Мережевий криптомодуль "Гряда-301" призначений для апаратної реалізації криптографічних перетворень у складі центральних серверів ЦСК (CMP, TSP та OCSP).

У складі програмного забезпечення користувачів ЦСК може використовуватися апаратний електронний ключ "Кристал-1". Електронний ключ призначений для апаратної реалізації криптографічних перетворень. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку апаратно-програмного довкілля.

Комплекс забезпечує функціональні характеристики, що наведені у табл. 1 та надавати доступ до ЦСК користувачам цілодобово 7 днів на тиждень.

Центральні сервери та сервери взаємодії можуть функціонувати автоматизовано. Існує можливість роботи серверів у різних режимах - основний чи резервний з повним чи частковим дублюванням функцій. Функціональні характеристики та режими експлуатації комплексу не залежать від типів та характеристик технічних засобів (РС, серверів та комунікаційного обладнання). У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритми шифрування за ДСТУ ГОСТ 28147:2009 та TDEA і AES за ISO/IEC 18033-3:2010; алгоритми ЕЦП за ДСТУ 4145-2002, RSA за PKCS#1 (RFC 3447) та ECDSA за ДСТУ ISO/IEC 14888-3:2014; алгоритми гешування за ГОСТ 34.311-95 та SHA (SHA-1 і SHA-224/256/384/512) за ДСТУ ISO/IEC 10118-3:2005; протоколи розподілу ключів за ДСТУ ISO/IEC 15946-3 (пп. 8.2) та RSA за PKCS#1 (RFC 3447).

Протоколи розподілу ключових даних реалізуються згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) і вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р., та за алгоритмом направленого шифрування RSA згідно PKCS#1 (RFC 3447).

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України.У ключовій системі комплексу виділені дві підгрупи ключових даних: службові ключові дані; ключові дані користувачів.

До складу службових відносяться: особистий ключ та сертифікат ЦСК; особисті ключі та сертифікати серверів ЦСК (CMP, TSP та OCSP); особисті ключі та сертифікати адміністраторів реєстрації та віддалених адміністраторів реєстрації. Особистий ключ ЦСК зберігається та застосовується тільки у криптомодулі, що входить до складу сервера ЦСК або РС адміністратора сертифікації. Особистий ключ ЦСК використовується для формування ЕЦП сертифікатів та списків відкликаних сертифікатів.

Сертифікат ЦСК використовується для перевірки ЕЦП, що накладається за допомогою особистого ключа ЦСК. Особисті ключі серверів ЦСК (OCSP та TSP) використовується для формування ЕЦП від позначок часу та інформації про статус сертифікатів.

Сертифікати серверів ЦСК використовується для перевірки ЕЦП, що накладається за допомогою відповідних особистих ключів серверів ЦСК.

Особисті ключі адміністраторів реєстрації та віддалених адміністраторів реєстрації призначені для формування ЕЦП запитів на формування сертифікатів, а також запитів на блокування, поновлення та скасування, а сертифікати – для перевірки ЕЦП від вказаних типів даних.

Ключі віддалених адміністраторів реєстрації призначені також для шифрування даних, що передаються між РС віддаленого адміністратора реєстрації та ЦСК (CMP-сервером ЦСК).

Таблиця 1

Функціональні характеристики комплексу

Показник	Значення
Кількість користувачів, яких обслуговує комплекс	не менше 1 000 000
Кількість користувачів, які можуть зареєструватися	не менше 5 000 за добу
Кількість користувачів, які одночасно мають доступ до сервера взаємодії (LDAP-каталогу та web-сторінки)	не менше 5 000
Час обробки запитів користувачів на формування, блокування, поновлення та скасування сертифікатів сервером ЦСК	не більше 1 с(не менше 100 запитів/с)
Час обробки запитів зовнішніх користувачів на визначення статусу сертифіката	не більше 1 с(не менше 500 запитів/с)
Час обробки запитів зовнішніх користувачів на формування позначки часу	не більше 1 с (не менше 500 запитів/с)

До ключових даних користувачів відносяться особисті ключі та сертифікати користувачів. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"), Aladdin eToken/JaCarta, Автор SecureToken, SafeNet iKey, Giesecke&Devrient StarSign, Gemalto IDPrime, ДБОСофт iToken та Ефіт Key; смарт-карти "Карта-1" ("ІІТ Смарт-карта Карта-1"), Техноконсалтинг TEllipse, Aladdin eToken/Ja Carta, Автор CryptoCard, Giesecke &Devrient StarSign та ДБОСофт Інтегра; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Комплекс захисту електронної пошти "ІІТ ЗАХИЩЕНА ЕЛЕКТРОННА ПОШТА"

Призначення комплексу: захист електронних поштових повідомлень при передачі та зберіганні. Захист забезпечується шляхом підпису повідомлень з використанням електронного цифрового підпису, а також шифруванням повідомлень користувача у поштовому клієнті (та сервері) при передачі та зберіганні.

Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК).

Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рис. 3.

До складу комплексу входять: програмні засоби КЗІ (програмні засоби захисту електронної пошти "ІІТ Захищена електронна пошта" для різних поштових клієнтів; бібліотеки користувача ЦСК зі складу програмного комплексу користувача ЦСК "ІІТ Користувач ЦСК-1"); апаратні засоби КЗІ.

До складу апаратних засобів комплексу можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Засоби захисту електронної пошти реалізують наступні функції: зашифрування електронних повідомлень; розшифрування електронних повідомлень; зашифрування та підпис електронних повідомлень; розшифрування та перевірку електронних повідомлень; відображення інформації про відправника захищеного електронного повідомлення та ін.

Програмні засоби захисту електронної пошти реалізують логіку роботи комплексу та інтегровані безпосередньо у поштові клієнти (та поштові сервери), через визначені механізми та інтерфейси.

Засоби захисту електронної пошти інтегровано у поштові клієнти Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС-Он-Лайн FossMail та ін., а також у спеціалізовані поштові сервери для окремих поштових клієнтів. Програмні засоби захисту електронної пошти можуть функціонувати у ОС Microsoft Windows 2000/ XP/2003 Server /7/ 2008 Server, Linux (SUSE/ Red Hat /Slackware та ін.) та UNIX (AIX/Solaris/BSD та ін.). Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо. Бібліотеки користувача центру

сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ. Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів поштового клієнта.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі поштового сервера системи.

Електронний ключ "Кристал-1" призначений для: автентифікації користувача (поштового клієнта) перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача.

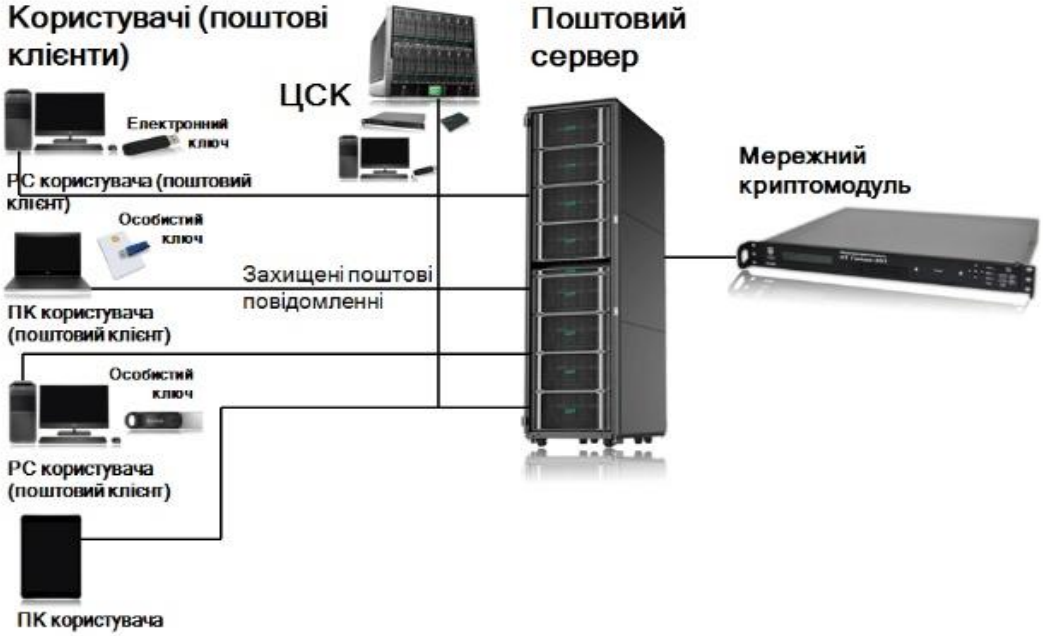


Рис. 3. Структурна схема комплексу

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача.

Мережевий криптомодуль "Гряда-301" призначений для: автентифікації поштового сервера перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/1000 для підключення до поштового сервера безпосередньо або через комутатори локальної обчислювальної мережі.

У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку. Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК).

У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані клієнтів (користувачів) та серверів.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних клієнтів (користувачів) та серверів відносяться особисті ключі та сертифікати відповідно користувачів та серверів.

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS# 11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог

до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12. Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів клієнтів (користувачів) та серверів, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів (користувачів) та серверів; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Комплекс захисту мережних з'єднань (TCP/IP) "ІІТ ЗАХИСТ З'ЄДНАНЬ-2"

Призначення комплексу: забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими та серверними частинами прикладних програмних систем (TCP-з'єднань).

Комплекс забезпечує: автентифікацію клієнтської частини прикладних програмних систем при підключенні до серверної частини; встановлення захищеного TCP-з'єднання між клієнтом та сервером; шифрування даних TCP-з'єднання, які передаються між клієнтом та сервером. Зазначені функції комплекс виконує шляхом застосування механізмів КЗІ, яка передається між клієнтом та сервером.

Комплекс підтримує взаємодію клієнтських та серверних частин (програмного забезпечення) прикладних програмних систем за протоколом TCP/IP. Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рис. 4. До складу комплексу входять: шлюз захисту (програмний комплекс "ІІТ Захист з'єднань-2. Шлюз захисту" або апаратний засіб - шлюз захисту "ІІТ ШЗ Бар'єр-301/ 301 (міні-пристрій)/301 (мікро-пристрій)"); програмний комплекс управління (віддаленого) шлюзами захисту "ІІТ Захист з'єднань-2. Віддалене управління шлюзами захисту"; програмний комплекс агента моніторингу шлюзів захисту "ІІТ Захист з'єднань-2. Агент моніторингу шлюзів захисту"; програмний комплекс моніторингу шлюзів захисту "ІІТ Захист з'єднань-2. Монітор шлюзів захисту"; програмний комплекс клієнта захисту "ІІТ Захист з'єднань-2. Клієнт"; proxy-клієнт захисту (програмний комплекс "ІІТ Захист з'єднань-2. Proxy захисту", далі – proxy захисту); програмний комплекс агента моніторингу proxy захисту "ІІТ Захист з'єднань-2. Агент моніторингу proxy захисту"; програмний комплекс моніторингу proxy захисту "ІІТ Захист з'єднань-2. Монітор proxy захисту"; програмний комплекс VPN-шлюзу "ІІТ Захист з'єднань-2. VPN-шлюз"; програмний комплекс VPN-клієнта "ІІТ Захист з'єднань-2. VPN-клієнт". До складу апаратних засобів комплексу також можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Шлюз захисту призначений для реалізації механізмів захисту сервера та виконує наступні функції: автентифікацію клієнтів захисту при підключенні до сервера; встановлення захищеного TCP-з'єднання з клієнтом в разі успішної автентифікації; встановлення відкритого TCP-з'єднання з сервером; прийом та розшифрування даних TCP-з'єднання від клієнта та передачі їх на сервер; прийом та зашифрування даних TCP-з'єднання від сервера та передачі їх клієнту; приймання та передачу управляючої (технологічної) інформації (моніторинг захисту тощо); прийом та введення в дію ключових даних. Програмний комплекс шлюзу захисту є серверною частиною комплексу захисту з'єднань та встановлюється на окремий мережевий вузол - шлюз захисту або безпосередньо на сервер, який захищається. Шлюз захисту у вигляді апаратного засобу є окремим пристроєм та виконаний у вигляді системної платформи у металевому корпусі висотою 1U та реалізує всі функції шлюзу захисту як окремого мережевого вузла. Типи та характеристики шлюзів захисту у вигляді апаратних засобів наведені у табл. 2. Встановлення параметрів та моніторинг стану роботи шлюзу захисту у вигляді апаратного засобу здійснюється віддалено через програмний комплекс управління шлюзами. Шлюз захисту у вигляді апаратного засобу підтримує також передачу події реєстрації за протоколом syslog та видачу інформації про стан функціонування та статистику роботи за протоколом SNMP. РС адміністратора з віддаленим управлінням призначена для управління шлюзами та постійного моніторингу роботи шлюзу і виконує наступні функції: налагодження конфігурації шлюзу захисту; передачу та приймання управляючої (технологічної) інформації (стан обробки з'єднань, список активних захищених з'єднань, резервні копії конфігурації і т. ін.) у/від шлюзу захисту; генерації та завантаження ключових даних у шлюз.

Агент моніторингу призначений для отримання результатів роботи шлюзу(ів) захисту і виконує наступні функції: отримання статистики роботи шлюзу захисту; надання можливості підключення моніторами шлюзу захисту для отримання даних моніторингу. Монітор шлюзів захисту призначений для відображення результатів моніторингу роботи шлюзу(ів) захисту і виконує наступні функції: отримання та відображення статистики роботи шлюзу(ів) захисту; перегляд журналів реєстрації шлюзу захисту; сповіщення адміністратора при виявленні збоїв або відмов у роботі шлюзу. Клієнт захисту з'єднань призначений для реалізації механізмів захисту клієнтських підключень та виконує наступні функції: ініціювання процесу автентифікації клієнта на шлюзі захисту при підключенні до сервера; встановлення захищеного TCP-з'єднання зі шлюзом захисту; зашифрування даних TCP-з'єднання при передачі на сервер; розшифрування даних TCP-з'єднання при прийомі з сервера. Proxy захисту є варіантом клієнтської частини комплексу та встановлюється біля РС (ПК) кліє-

нтів. При цьому, клієнтські засоби захисту не встановлюються на РС (ПК) клієнтів. Але клієнтське програмне забезпечення повинне здійснювати підключення не до сервера, а до proxy, який буде перенаправляти їх у захищеному вигляді до сервера через шлюз захисту.

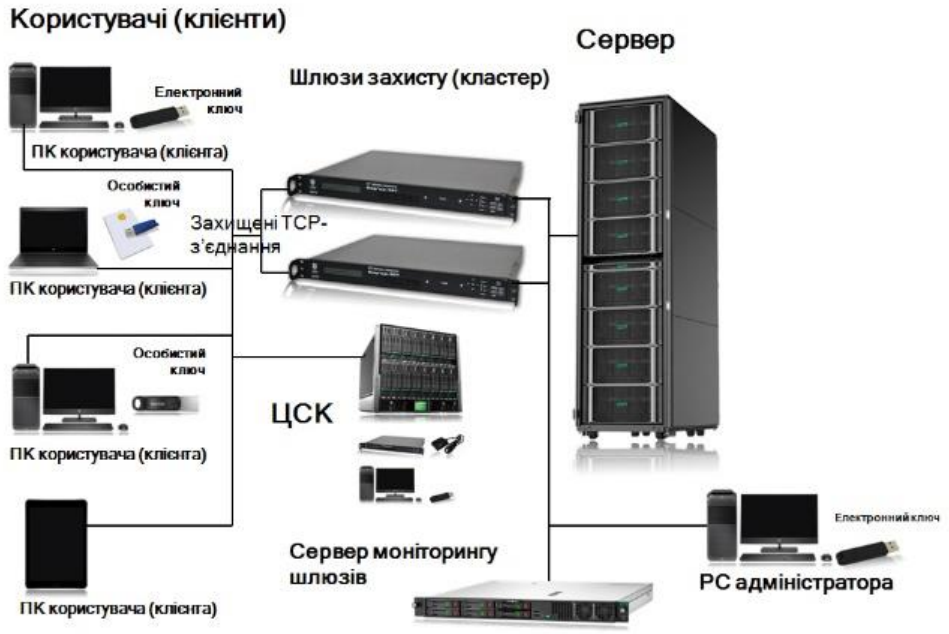


Рис. 4. Структурна схема комплексу

Таблиця 2

Типи та характеристики шлюзів захисту

Тип	Зовнішній вигляд	Інтер-фейси	Швидкість шифрування, Мбіт/с	Кількість автентифікацій клієнтів, автентифікацій/с
"Бар'єр-301" (міні-пристрій) ("ІІТ ШЗ "Бар'єр-301 (міні-пристрій)")		2 x Ethernet 100	40	10
"Бар'єр-301" (міні-пристрій) ("ІІТ ШЗ "Бар'єр-301 (міні-пристрій)")		2 x Ethernet 100/1000	125	50
"Бар'єр-301" ("ІІТ ШЗ "Бар'єр-301")		2 x Ethernet 100/1000 Опціонально – 2 x Ethernet 100/1000BASE-SX (оптичні, LC)	250	100

Монітор proxy захисту призначений для відображення результатів моніторингу роботи proxy захисту. Шлюз та клієнт захисту підтримують взаємодію клієнтських та серверних частин (клієнта та сервера) прикладних систем за протоколом TCP/IP. Під час встановлення клієнтською частиною прикладної системи TCP-з'єднання з сервером, клієнт захисту автентифікується на відповідному шлюзі захисту. Шлюз захисту при підключенні клієнта захисту проводить процедуру його автентифікації та в разі успішної автентифікації встановлює захищене TCP-з'єднання з клієнтом та відкрите TCP-з'єднання з сервером. Після проведення автентифікації (встановлення захищеного TCP-з'єднання – сеансу передачі даних) клієнт та шлюз захисту здійснюють шифрування даних (TCP-з'єднання), які передаються між клієнтом та сервером.

Клієнт захисту здійснює зашифрування даних, які відправляються від клієнта до сервера та перенаправляє їх до шлюзу, і навпаки – розшифровує дані, які приходять від сервера через шлюз.

Шлюз захисту здійснює розшифрування даних, які надходять від клієнта захисту та перенаправляє їх до сервера, і навпаки – зашифровує дані, які приходять від сервера та перенаправляє їх клієнту захисту.

VPN-шлюз призначений для реалізації механізмів створення віртуальної VPN-мережі та виконує наступні функції: створення віртуального мережевого інтерфейсу; отримання через шлюз захисту даних (MAC-кадрів) від VPN-клієнтів та передачі їх у віртуальний мережевий інтерфейс або комутації MAC-кадрів між VPN-клієнтами; отримання даних з віртуального мережевого інтерфейсу та передачі їх відповідному VPN-клієнту через шлюз захисту.

VPN-клієнт призначений для реалізації механізмів створення клієнтського підключення віртуальної VPN-мережі та виконує наступні функції: створення віртуального мережевого інтерфейсу; отримання даних (MAC-кадрів) з віртуального мережевого інтерфейсу та передачі їх на VPN-шлюз через клієнта захисту; отримання через клієнт захисту даних з VPN-шлюзу та передачі їх у віртуальний мережевий інтерфейс.

VPN-шлюз може бути інтегрований безпосередньо у шлюз захисту (програмний комплекс чи апаратний засіб). У випадку інтеграції VPN-шлюзу безпосередньо у шлюз захисту управління та моніторинг стану роботи VPN-шлюзу здійснюється шлюзом захисту. VPN-шлюз також підтримує можливість використання зовнішнього DHCP-сервера для динамічного надання VPN-клієнтам IP-адрес. У випадку інтеграції VPN-шлюзу безпосередньо у апаратний шлюз захисту, може використовуватися вбудований DHCP-сервер шлюзу захисту. Взаємодія VPN-клієнта з VPN-шлюзом здійснюється за протоколом TCP/IP. Для захисту мереженого з'єднання між VPN-клієнтом та VPN-шлюзом використовується клієнт захисту та шлюз захисту.

VPN-клієнт може також бути інтегрований безпосередньо у клієнта захисту. Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів клієнта захисту.

Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі програмного шлюзу захисту. Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для: автентифікації користувач (клієнта) перед початком роботи; зберігання та захисту особистого ключа користувач (клієнта); апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні клієнта.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК клієнта. Мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301") призначений для: автентифікації шлюзу захисту перед початком роботи; зберігання та захисту особистого ключа шлюзу захисту; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні шлюзу. Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до шлюзу захисту безпосередньо або через комутатори локальної обчислювальної мережі. У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12. 2012 р.

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України. Протокол встановлення захищеного сеансу передачі даних між клієнтом та шлюзом захисту реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3.

Протокол взаємної автентифікації включає: формування клієнтом та передачу даних автентифікації (запиту) на шлюз захисту; обробку запиту від клієнта шлюзом захисту; прийом та обробку відповіді клієнтом від шлюзу захисту.За результатом роботи протоколу на шлюзі захисту та клієнті встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування.

Шифрування даних у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між клієнтом та шлюзом захисту у результаті виконання протоколу взаємної автентифікації.

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані клієнтів, шлюзів захисту та адміністратора.

До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо. До ключових даних клієнтів, шлюзів захисту та адміністратора відносяться особисті ключі та сертифікати відповідно клієнтів, шлюзів захисту та адміністратора.

Ключові дані клієнтів, шлюзів захисту та адміністратора призначені для захисту управляючої та службової інформації при передачі між РС адміністратора та шлюзами захисту, а також для встановлення захищених з'єднань між клієнтами та шлюзами захисту та безпосередньо захисту мережевого з'єднання.

В якості носіїв ключової інформації для особистих ключів апаратних шлюзів захисту використовуються електронні ключі "Кристал-1". Шлюзи захисту також підтримують генерацію ключів безпосередньо у пристрої. Під час генерації ключів у шлюзі захисту формується запит на сертифікат, який передається у ЦСК з метою формування сертифікату. Після формування сертифікат (разом із ланцюжком сертифікатів) завантажується у шлюз захисту.

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS # 11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів клієнтів та шлюзів захисту, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів, шлюзів захисту та адміністратора; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Комплекс захисту інформації у IP-МЕРЕЖАХ "ІІТ ЗАХИСТ IP-ПОТОКУ"

Призначення комплексу: забезпечення конфіденційності та цілісності конфіденційної інформації, яка передається у розподілених системах на основі IP-мереж передачі даних.

Комплекс забезпечує: конфіденційність та цілісність інформації (мережевого IP-потоку), яка передається мережами зв'язку між розподіленими локальними обчислювальними мережами (ЛОМ) або між клієнтами та ЛОМ; організацію централізованого управління засобами захисту мережевого IP-потоку, організацію централізованої генерації та розподілу ключових даних для використання у цих засобах. Зазначені функції комплекс виконує шляхом застосування механізмів КЗІ, яка передається у вигляді мережевого IP-потоку між розподіленими ЛОМ або між клієнтами та ЛОМ через зовнішні канали зв'язку.

Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурні схеми комплексу за розміщенням його складових частин на окремих технічних засобах наведені на рис. 5 та рис. 6. IP-шифратор призначений для шифрування та контролю цілісності потоку IP-пакетів, що передаються через нього між різними ЛОМ або між клієнтами та ЛОМ і виконує такі функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу технологічної інформації (команд, поточного стану обробки потоку, резервних копій конфігурації тощо) у/від робочої станції адміністратора; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

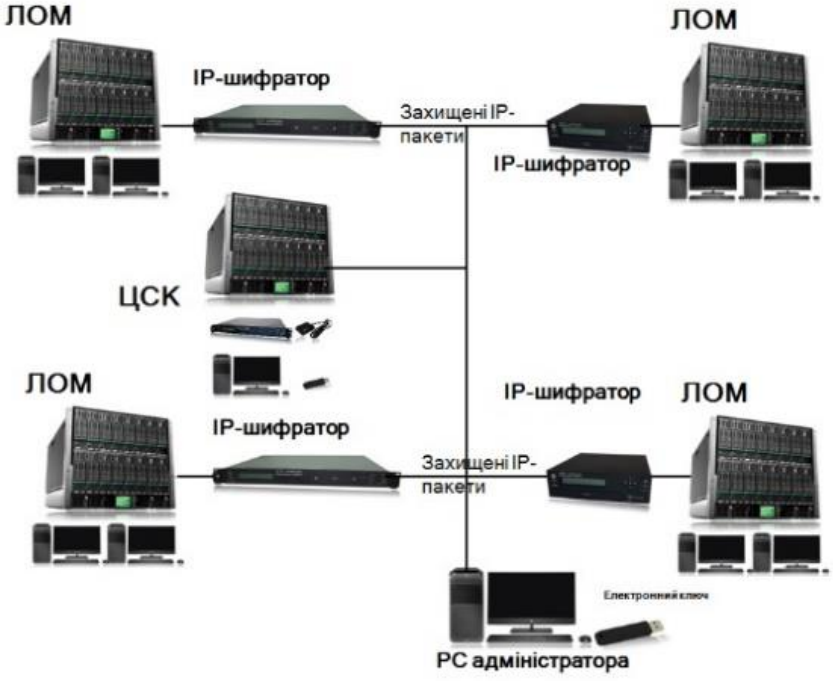


Рис. 5.Структурна схеми комплексу за розміщенням його складових частин

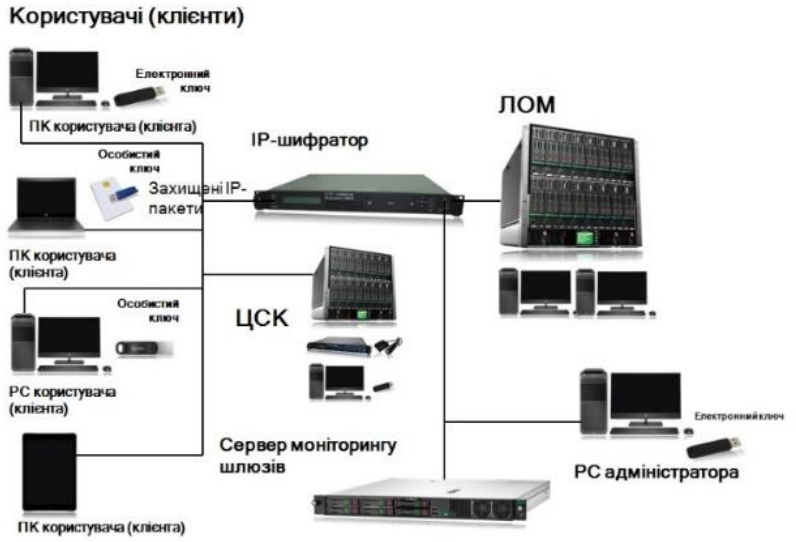


Рис. 6. Структурна схеми комплексу за розміщенням його складових частин

РС адміністратора мережі IP-шифраторів призначена для централізованого управління мережею IP-шифраторів і виконує такі функції: налагодження конфігурації кожного IP-шифратора; передачу та приймання управляючої (технологічної) інформації (стан обробки потоку, резервні копії конфігурації і т. ін.) у/від IP-шифраторів; генерації та завантаження ключових даних у IP-шифратори.

Клієнт IP-шифраторів призначений для шифрування та контролю цілісності потоку IP-пакетів, що передаються між ним та IP-шифратором(ами) і виконує такі функції: встановлення захищених з'єднань з IP-шифраторами; шифрування та контроль цілісності IP-пакетів.

IP-шифратори виконують шифрування та контроль цілісності потоків мережних IP-пакетів, що передаються через них між розподіленими ЛОМ або між клієнтами та ЛОМ.

Для забезпечення транзитної передачі даних IP-шифратори мають два мережних інтерфейси типу Ethernet – внутрішні та зовнішні. До внутрішніх інтерфейсів підключається комунікаційне обладнання ЛОМ, а зовнішні підключаються до зовнішньої мережі передачі даних.

IP-пакети, отримані через внутрішні мережні інтерфейси із ЛОМ зашифровуються та захищаються контрольною сумою і маршрутизуються на зовнішній інтерфейс для передачі через зовнішній мережі. IP-пакети, отримані через зовнішні інтерфейси із зовнішньої мережі розшифровуються та перевіряються на цілісність і маршрутизуються на внутрішній інтерфейс для передачі у ЛОМ.

IP-шифратори підтримують захист IP-потоку для повнозв'язної топології ЛОМ ("кожний з кожним").

Віддалене управління IP-шифраторами з РС адміністратора здійснюється через мережі передачі даних з підключенням до одного з інтерфейсів.

IP-шифратори, що входять до складу комплексу, функціонують у автоматизованому режимі з віддаленим управлінням з РС адміністратора.

Комплекс забезпечує характеристики, що наведені у табл. 3. Типи та характеристики IP-шифраторів наведені у табл. 4.

Таблиця 3

Характеристики комплексу

Характеристика	Значення
Кількість захищених з'єднань IP-шифраторів	не менше 1024 з'єднань (зв'язок IP-шифратора з 1024 іншими)
Кількість захищених з'єднань з клієнтами	не менше 4096 з'єднань (зв'язок IP-шифратора з 4096 клієнтами)
Швидкість обробки IP-потоку (захисту)	не менше 25 Мбіт/с (до 450 Мбіт/с)
Кількість IP-шифраторів, якими управляє один адміністратор мережі	не менше 1024

У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування). Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р.

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку.

Протокол встановлення захищеного сеансу передачі даних між IP-шифраторами або між клієнтом та IP-шифратором реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3. Протокол взаємної автентифікації включає: формування ініціатором (IP-шифратором чи клієнтом) та передачу даних автентифікації (запиту) на IP-шифратор; обробку запиту IP-шифратором; прийом та обробку відповіді ініціатором від IP-шифратора. За результатом роботи протоколу на IP-шифраторах чи IP-шифраторі та клієнті встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування IP-пакетів у дуплексному режимі.

Таблиця 4

Типи та характеристики IP-шифраторів

Тип	Зовнішній вигляд	Інтерфейси	Швидкість шифрування, Мбіт/с
"Канал-201" (мікро-пристрій) ("ІІТ IP-шифратор Канал-201 (мікро-пристрій)")		USB (RNDIS), Ethernet 10/100	40
"Канал-201" ("ІІТ IP-шифратор Канал-201")		2 x Ethernet 100/1000	125
"Канал-301" ("ІІТ IP-шифратор Канал-301")		2 x Ethernet 100/1000, опціонально - 2 x Ethernet 100/1000BASE-SX (оптичні, LC)	1000 (1 Гбіт/с)
"Канал-401" ("ІІТ IP-шифратор Канал-401")		2 x Ethernet 100/1000, 2 x SFP+ (1000/10000, оптичні SFP-модулі 1000BASE-SX, 10G-SR чи ін.)	5000 (5 Гбіт/с)

Шифрування IP-пакетів здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування. Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані IP-шифраторів, адміністратора та клієнтів. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо. До ключових даних IP-шифраторів, адміністратора та клієнтів відносяться особисті ключі та сертифікати відповідно IP-шифраторів, адміністратора та клієнтів. Ключові дані IP-шифраторів, адміністратора та клієнтів призначені для захисту управляючої та службової інформації при передачі між РС адміністратора та IP-шифраторами, а також для встановлення захищених з'єднань між IP-шифраторами або між клієнтами та IP-шифраторами та безпосередньо захисту IP-потоку.

В якості носіїв ключової інформації для особистих ключів IP-шифраторів використовуються електронні ключі "Кристал-1" ("ІІТ Е.ключ Кристал-1"). IP-шифратори також підтримують генерацію ключів безпосередньо у пристрої. Під час генерації ключів у IP-шифраторі формується запит на сертифікат, який передається у ЦСК з метою формування сертифікату. Після формування сертифікат (разом із ланцюжком сертифікатів) завантажується у IP-шифратор. IP-шифратори також підтримують генерацію ключів безпосередньо у пристрої.

Під час генерації ключів у IP-шифраторі формується запит на сертифікат, який передається у ЦСК з метою формування сертифікату. Після формування сертифікат завантажується у IP-шифратор. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"); інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус

сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12. Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів IP-шифраторів, адміністратора та клієнтів, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів. Програмно-технічний комплекс (ПТК) СК забезпечує: обслуговування сертифікатів IP-шифраторів, адміністратора та клієнтів, що включає: надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів.

Комплекс захисту інформації на носіях "ІІТ ЗАХИЩЕНИЙ ДИСК-4"

Призначення комплексу: забезпечення конфіденційності інформації, яка зберігається на носіях інформації робочих станцій, портативних комп'ютерів та серверів (жорстких дисках, електронних flash-дисках, картах пам'яті тощо) з використанням механізмів та засобів КЗІ. Структурна схема комплексу наведена на рис. 7.

До складу комплексу входять: програмний комплекс захисту інформації на носіях користувача "ІІТ Захищений диск-4. Користувач"; програмний комплекс захисту інформації на носіях сервера "ІІТ Захищений диск-4. Сервер". До складу апаратних засобів комплексу також може входити електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"). Програмні засоби комплексу забезпечують захист інформації на носіях інформації робочих станцій (РС) та серверів (жорстких дисках, електронних flash-дисках, картах пам'яті тощо).

Захист інформації забезпечується прозорим шифруванням областей дискового простору чи створенням віртуальних логічних дисків, які фізично є зашифрованими областями дисків чи файлами-образами.

Засоби захисту носіїв серверів підтримують автоматичне підключення захищених дисків, аварійне відключення та знищення захищених дисків, забезпечення доступу до них з ЛОМ та ін.

Засоби захисту носіїв портативних комп'ютерів забезпечують шифрування даних на вбудованих та на зовнішніх картах пам'яті. Програмні засоби комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі тощо.

Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для апаратної реалізації криптографічних перетворень усередині пристрою та реалізує: автентифікацію користувача перед початком роботи; зберігання та захист особистого ключа користувача.

Електронний ключ має електричний USB-інтерфейс для підключення. У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Рис. 7. Структурна схема комплексу "Електронний ключ"

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України. Шифрування секторів захищених дисків виконується в двох режимах: спочатку в режимі простої заміни, а потім в режимі гамування із зворотнім зв'язком згідно ДСТУ ГОСТ 28147:2009.

Шифрування здійснюється на ключі шифрування диску, який зберігається разом із диском. Захист ключа шифрування диску виконується на ключі захисту, який отримується шляхом гешування за ГОСТ 34.311-95 особистого ключа протоколу розподілу ключів.

Довгострокові ключові елементи (ДКЕ) для алгоритму шифрування ДСТУ ГОСТ 28147:2009 постачаються відповідно до вимог Держспецзв'язку України. До ключових даних комплексу відносяться особисті ключі користувачів і серверів, що використовують захищені диски. В якості особистих ключів можуть використовуватися особисті ключ користувачів центру сертифікації ключів (ЦСК, при цьому, в якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1").

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів (формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12).

Комплекс захисту SAP-системи "ІІТ ЗАХИСТ SAP"

Повна назва комплексу: комплекс захисту SAP-системи "ІІТ Захист SAP". Призначення комплексу: криптографічний захист інформації у SAP-системі, а саме: автентифікація користувачів SAP-системи та забезпечення конфіденційності і цілісності даних, які передаються між користувачами та сервером системи, з використанням механізмів КЗІ; забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у системі, з використанням електронного цифрового підпису.

Для організації ключової системи (управління ключовими даними) засобів комплексу використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК).

Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рис. 8.До складу комплексу входять: програмний комплекс захисту SAP-клієнта "ІІТ Захист SAP. Клієнт"; програмний комплекс захисту SAP-сервера "ІІТ Захист SAP. Сервер"; програмний комплекс віддаленого моніторингу захисту SAP-сервера "ІІТ Захист SAP. Віддалений монітор сервера". До складу апаратних засобів можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301"). Програмні засоби КЗІ реалізують логіку роботи комплексу та інтегровані безпосередньо у клієнтську та серверну частини SAP-системи (SAP-клієнта та SAP-сервер), через визначені у SAP-системі механізми та інтерфейси КЗІ.

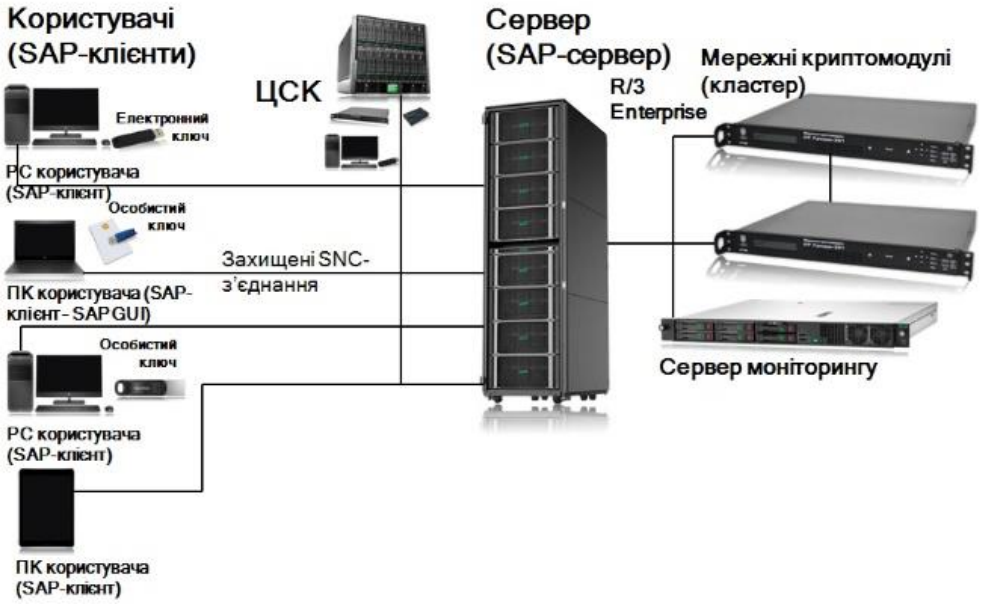


Рис. 8. Структурна схема комплексу

Програмні засоби КЗІ комплексу можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо. SNC-бібліотеки (бібліотеки захисту з'єднань) у складі SAP-клієнта та SAP-сервера призначені для реалізації механізмів автентифікації користувачів SAP-системи на сервері під час підключення користувачів до сервера (встановлення з'єднання з сервером), шляхом реалізації протоколу взаємної автентифікації сторін, та забезпечення конфіденційності і цілісності інформації, яка передається між користувачами та сервером SAP-системи під час їх взаємодії, шляхом шифрування інформації та формування і перевіряння криптографічних контрольних сум.

Протокол взаємної автентифікації сторін (встановлення захищеного з'єднання) включає наступні шаги (етапи): формування та передачу запиту від користувача SAP-системи на сервер; обробку запиту від користувача сервером (що включає, в тому числі, перевірку чинності сертифіката користувача), формування та відправку відповіді за результатами обробки запиту; прийом та обробку відповіді від сервера користувачем та прийняття рішення про успішність встановлення захищеного з'єднання (що аналогічно включає і перевірку чинності сертифіката сервера).

SSF-бібліотека (бібліотека захищеного зберігання та пересилання) у складі SAP-клієнта та SAP-сервера призначена для забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у SAP-системі, шляхом формування та перевіряння електронного цифрового підпису від даних та документів, як на стороні користувача SAP-системи, так і на стороні сервера.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання SNC- та SSF-бібліотеками в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС); зашифрування та розшифрування даних; формування та перевірку ЕЦП від даних; захист сеансів передачі даних (захист з'єднань); інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК); отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Засоби управління та моніторингу стану захисту клієнта призначені для встановлення параметрів

SNC- та SSF-бібліотек, параметрів бібліотеки користувача ЦСК, а також моніторингу та відображення стану їх роботи. Засоби управління захистом сервера призначені для встановлення параметрів SNC- та SSF-бібліотек, а також параметрів бібліотеки користувача ЦСК.

Агент моніторингу захисту SAP-сервера призначений для зберігання інформації про стан та статистику функціонування програмних засобів захисту сервера (списку активних захищених з'єднань SNC-бібліотеки тощо), а також ведення журналів реєстрації подій та надання доступу до цієї інформації засобам віддаленого моніторингу. Інформацію про стан та статистику функціонування до агента моніторингу передають SNC- та SSF-бібліотеки.

Програмний комплекс віддаленого моніторингу захисту SAP-сервера призначений для отримання від агента моніторингу сервера та відображення інформації про стан і статистику функціонування програмних засобів захисту та подій з журналів реєстрації.

SNC-бібліотеки (бібліотеки захисту з'єднань) реалізовані у відповідності до визначених розробником SAP-системи специфікацій програмних інтерфейсів: інтерфейсу GSS-API v2, який реалізує всі механізми КЗІ згідно з міжнародними технічними рекомендаціями RFC-2078; інтерфейс SNC-адаптера, який визначений у внутрішньому технічному документі компанії SAP та призначений для безпосередньої інтеграції бібліотеки у SAP-клієнт та SAP-сервер, і є проміжним інтерфейсом між GSS-API v2 та SAP-системою. SSF-бібліотеки (бібліотеки захищеного зберігання та пересилання) реалізовані у відповідності до визначеної розробником SAP-системи специфікації програмного інтерфейсу SSF-API. Зазначений інтерфейс визначений у внутрішньому технічному документі компанії SAP.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі користувача SAP-системи. Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера SAP-системи.

Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для: автентифікації користувача SAP-системи перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача SAP-системи.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача SAP-системи.

Мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301") призначений для: автентифікації сервера SAP-системи перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера SAP-системи.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до сервера SAP-системи безпосередньо або через комутатори локальної обчислювальної мережі. Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку сервера SAP-системи. У засобах комплексу використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147:2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р. Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку України. Протокол встановлення захищеного сеансу передачі даних між SAP-клієнтом та SAP-сервером реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно стандарту ДСТУ ISO/IEC 9798-3.

За результатом роботи протоколу на сервері та клієнті встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних у захищеному з'єднанні у дуплексному режимі.

Шифрування даних у захищеному з'єднанні здійснюється за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі гамування. В якості криптографічної контрольної суми для контролю цілісності даних у захищеному з'єднанні використовуються імітовставки, які обчислюються за алгоритмом шифрування згідно ДСТУ ГОСТ 28147:2009 у режимі вироблення імітовставки.Шифрування даних та обчислення імітовставок у захищеному з'єднанні здійснюється на основі сеансових ключів та векторів початкової ініціалізації (синхромаркерів), які розподіляються між клієнтом та сервером у результаті виконання протоколу взаємної автентифікації.

Організацію ключової системи засобів комплексу виконує центр сертифікації ключів (ЦСК). У комплексі використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та сервера SAP-системи. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера SAP-системи відносяться особисті ключі та сертифікати відповідно користувачів та сервера.

В якості носіїв ключової інформації для особистих ключів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301";

інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів користувачів та сервера; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Засоби електронного цифрового підпису (ЕЦП) для платформи ORACLE FLEXCUBE "ІІТ ЕЦП ДЛЯ ORACLE FLEXCUBE".

Призначення засобів: забезпечення цілісності та неспростовності авторства електронних даних та документів, що циркулюють у платформі, з використанням електронного цифрового підпису.

Зазначені функції засоби виконують шляхом застосування механізмів ЕЦП. Для організації ключової системи (управління ключовими даними) засобів використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурна схема засобів за розміщенням їх складових частин на окремих технічних засобах наведена на рис. 9.

До складу засобів входять: засоби ЕЦП для FlexCube-клієнта у складі бібліотеки користувача ЦСК для web-оглядача "ІІТ Користувач ЦСК-1. Бібліотека FlexCube (Active-X)" (Active-X-бібліотека ЕЦП), яка включає бібліотеку користувача ЦСК "ІІТ Користувач ЦСК-1. Бібліотека підпису"; програмний комплекс сервера ЕЦП для FlexCube-сервера у складі: програмний комплекс віддаленого моніторингу бібліотек користувача ЦСК "ІІТ Користувач ЦСК-1. Віддалений моніторинг бібліотек".

До складу апаратних засобів можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") чи електронний ключ "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"); мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301").

Програмні засоби ЕЦП реалізують логіку роботи засобів та інтегровані безпосередньо у клієнтську та серверну частини платформи Oracle FlexCube (FlexCube-клієнта та FlexCube-сервер), через визначені у платформі Oracle FlexCube механізми та інтерфейси ЕЦП.

Програмні засоби КЗІ можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо.

Active-X-бібліотека ЕЦП у складі FlexCube-клієнта, який виконується безпосередньо у web-оглядачі, призначена для забезпечення цілісності та неспростовності авторства електронних даних та документів, що обробляються клієнтом (користувачем), шляхом формування та перевіряння ЕЦП від даних та документів на стороні клієнта.

Рис. 9. Структурна схема комплексу

Web-служба ЕЦП у складі сервера ЕЦП, який підключений до FlexCube-сервера та доступний за протоколом SOAP, призначена для забезпечення цілісності та неспростовності авторства електронних даних та документів, що обробляються FlexCube-сервером, шляхом формування та перевіряння ЕЦП від даних та документів на стороні сервера.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання Active-X-бібліотекою та web-службою ЕЦП в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС); зашифрування та розшифрування даних; формування та перевірку ЕЦП від даних; захист сеансів передачі даних (захист з'єднань); інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК); отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Програмний комплекс віддаленого моніторингу бібліотек користувача ЦСК призначений для отримання від агента моніторингу бібліотек та відображення інформації про стан і статистику функціонування програмних засобів та подій з журналів реєстрації.

Зберігання інформації про стан та статистику функціонування програмних засобів, а також ведення журналів реєстрації подій та надання доступу до цієї інформації засобам віддаленого моніторингу здійснює агент моніторингу бібліотек. Інформацію про стан та статистику функціонування до агента моніторингу передають бібліотеки користувача ЦСК.

Active-X-бібліотека ЕЦП реалізована у вигляді Active-X-об'єкту у відповідності до визначених розробником платформи Oracle FlexCube специфікацій програмних інтерфейсів та доступна FlexCube-клієнту через виклики JavaScript-функції.

Web-служба ЕЦП реалізована у відповідності до визначеної розробником платформи Oracle Flex Cube специфікацій та доступна FlexCube-серверу за протоколом SOAP через java-модулі (JAX-WS) чи PL/SQL-модулі.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі користувача платформи Oracle FlexCube. Мережевий криптомодуль призначений для апаратної реалізації криптографічних перетворень усередині модуля у складі сервера платформи Oracle FlexCube. Електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1") призначений для: автентифікації користувача платформи Oracle FlexCube перед початком роботи; зберігання та захисту особистого ключа користувача; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні користувача платформи.

Електронний ключ має електричний USB-інтерфейс для підключення. Апаратна реалізація електронного ключа забезпечує захищеність виконання усіх криптографічних перетворень усередині пристрою та унеможливлює доступ до особистих ключів користувача з боку РС чи ПК користувача платформи Oracle FlexCube.

Мережевий криптомодуль "Гряда-301" ("ІІТ МКМ Гряда-301") призначений для: автентифікації сервера ЕЦП перед початком роботи; зберігання та захисту особистого ключа сервера; апаратної реалізації криптографічних перетворень у складі програмних засобів на стороні сервера ЕЦП.

Мережевий криптомодуль має мережевий електричний інтерфейс Ethernet 100/ 1000 для підключення до сервера ЕЦП безпосередньо або через комутатори локальної обчислювальної мережі. Апаратна реалізація мережевого криптомодуля забезпечує захищеність виконання усіх криптографічних перетворень усередині модуля та унеможливлює доступ до особистих ключів сервера з боку сервера ЕЦП.

У засобах використовуються такі криптографічні алгоритми та протоколи: алгоритм шифрування за ДСТУ ГОСТ 28147: 2009; алгоритм ЕП за ДСТУ 4145-2002; алгоритм гешування за ГОСТ 34.311-95; протокол розподілу ключових даних (направлене шифрування).

Протокол розподілу ключових даних (направлене шифрування) реалізований згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку №739 від 18.12.2012 р.

Генерація ключових даних здійснюється згідно методики генерації ключових даних, яка погоджена з Адміністрацією Держспецзв'язку. Організацію ключової системи засобів виконує центр сертифікації ключів (ЦСК).

У засобах використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та сервера ЕЦП. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (TSP-сервера та OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів, позначок часу тощо.

До ключових даних користувачів та сервера ЕЦП відносяться особисті ключі та сертифікати відповідно користувачів та сервера.

В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні диски (flash-диски); оптичні компакт-диски (CD); електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; мережевий криптомодуль "Гряда-301" (мікро-пристрій) ("ІІТ МКМ Гряда-301 (мікро-пристрій)") та мережевий криптомодуль "Гряда-301"; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS# 11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог

до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та сервера, надання послуг фіксування часу, а також надання (за необхідності) засобів генерації особистих та відкритих ключів.

Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів клієнтів користувачів та сервера; надання послуг фіксування часу; надання (за необхідності) засобів генерації особистих та відкритих ключів. В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1".

Засоби захисту входу в контролер домену MICROSOFT ACTIVE DIRECTORY "ІІТ ЗАХИЩЕНИЙ ВХІД"

Призначення засобів: автентифікація користувачів операційних систем (ОС) Microsoft Windows в контролері домену Microsoft Active Directory при вході в ОС та при доступі до ресурсів.

Зазначені функції засоби виконують шляхом застосування механізмів КЗІ.

Автентифікація користувачів в контролері домену здійснюється під час входу користувача до ОС з його робочій станції (РС) чи портативному комп'ютері (ПК) з використанням апаратних засобів КЗІ (носіїв ключової інформації) користувача, таких як електронні ключі та смарт-карти. Для організації ключової системи (управління ключовими даними) засобів користувачів та контролера домену використовується центр сертифікації ключів (програмно-технічний комплекс ЦСК). Структурна схема засобів за розміщенням їх складових частин на окремих технічних засобах наведена на рис. 10.

Рис. 10. Структурна схема комплексу

До складу засобів входять програмні засоби інтеграції носіїв ключової інформації (в т.ч. і апаратних засобів КЗІ) користувачів в ОС - програмний комплекс захисту входу користувача "ІІТ Захищений вхід. Користувач" для ОС Microsoft Windows, який включає: міні-драйвери смарт-карт носіїв ключів (як апаратних засобів КЗІ так і віртуальних); віртуального драйвера смарт-карт; програмних засобів (бібліотек) КЗІ (користувача ЦСК) "ІІТ Користувач ЦСК-1".

До складу апаратних засобів КЗІ користувачів можуть входити: електронний ключ "Кристал-1" ("ІІТ Е.ключ Кристал-1"); електронний ключ "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К"); смарт-карта "Карта-1" ("ІІТ Смарт-карта Карта-1").

Програмні засоби інтегруються безпосередньо у підсистему автентифікації ОС на стороні користувача контролеру домену Microsoft Active Directory.

Програмні засоби для автентифікації на контролері домену можуть використовувати зовнішні апаратні засоби КЗІ (носії ключової інформації) користувача, такі як електронні ключі та смарт-карти.

Міні-драйвер смарт-карт призначений для інтеграції апаратних засобів КЗІ (носіїв ключової інформації) у підсистему автентифікації ОС на стороні користувача та забезпечення розпізнавання апаратних засобів у підсистемі автентифікації ОС та їх використання в процесі автентифікації на контролері домену.

Віртуальний драйвер смарт-карт використовуються для носіїв ключової інформації та апаратних засобів КЗІ (наприклад, електронних ключів), які не є смарт-картами та потребують емуляції поведінки смарт-карти у ОС з метою їх розпізнавання ОС на стороні користувача в якості смарт-карти.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання мінідрайвером смарт-карт в якості базових засобів КЗІ та виконують наступні функції у їх складі: роботу з носіями ключової інформації (зчитування особистих ключів з носіїв) та взаємодію з апаратними засобами КЗІ); роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС); інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК); пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК) тощо.

Електронні ключі, смарт-карти чи інші носії ключової інформації (апаратні засоби КЗІ) призначені для зберігання особистого ключа автентифікації користувача на контролері домену. Програмні засоби інтеграції носіїв ключової інформації (апаратних засобів КЗІ) користувачів в ОС встановлюються та використовуються виключно на стороні користувача на його РС (ПК). Для автентифікації користувачів на контролері домену (сервері) має бути налаштована служба Microsoft Active Directory та створений і налаштований домен, а користувачі, які мають автентифікуватися в контролері, повинні бути користувачами створеного домену. На контролері домену не здійснюється встановлення жодних складових частин засобів.

В якості ОС користувачів, в які інтегровано засоби автентифікації, можуть використовуватися ОС Microsoft Windows XP/ Vista/7/8/8.1/10. В якості ОС контролера домену (сервера) можуть використовуватися ОС Microsoft Windows 2003/2008/2012/ 2016/2019 Server. У засобах використовуються такі криптографічні алгоритми та протоколи: алгоритми шифрування TDEA і AES за ISO/IEC 18033-3:2010; алгоритм ЕЦП RSA за PKCS# 1 (RFC 3447); алгоритми гешування SHA (SHA-1 і SHA-224/256/384/512) за ДСТУ ISO/IEC 10118-3:2005; протокол розподілу клю-

чів RSA за PKCS#1 (RFC 3447). Автентифікація користувача на контролері домену здійснюється за протоколом Kerberos, який реалізований штатними засобами ОС користувача та контролера домену. Під час автентифікації штатні засоби ОС користувача здійснюють звертання (використовують) міні-драйвер смарт-карт для виконання криптографічних перетворень.

У засобах використовуються дві підгрупи ключових даних: ключові дані ЦСК; ключові дані користувачів та контролера домену. До складу ключових даних ЦСК відносяться сертифікати ЦСК та серверів ЦСК (OCSP-сервера), які використовуються для перевірки ЕЦП сертифікатів, списків відкликаних сертифікатів тощо. До ключових даних користувачів та контролера домену відносяться особисті ключі та сертифікати відповідно користувачів та контролера домену. В якості носіїв ключової інформації для особистих ключів та криптомодулів можуть використовуватися: електронні ключі "Кристал-1", "Алмаз-1К" ("ІІТ Е.ключ Алмаз-1К") та ін.; інші носії, електронні ключі, смарт-карти та криптомодулі з бібліотеками підтримки, що відповідають технічним рекомендаціям PKCS#11.

Формати ключових даних та іншої спеціальної інформації відповідають вимогам міжнародних стандартів, рекомендацій та діючих нормативних документів: формати сертифікатів та списків відкликаних сертифікатів – згідно ДСТУ ISO/IEC 9594-8:2006 та технічних рекомендацій RFC 5280; формати підписаних даних (даних з ЕП) – згідно ДСТУ ETSI EN 319 122-1:2016 і ДСТУ ETSI EN 319 122-2:2016, технічних рекомендацій RFC 5652 (PKCS#7) та 5126; формати захищених даних (зашифрованих даних) – згідно вимог до форматів криптографічних повідомлень та технічних рекомендацій RFC 5652 (PKCS#7); формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката (протокол OCSP) – згідно технічних рекомендацій RFC 2560; формати запитів на формування позначок часу та самих позначок часу (протокол TSP) – згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161; формати особистих ключів – згідно технічних рекомендацій RFC 5958 (PKCS#8) та PKCS#12.

Центр сертифікації ключів (ЦСК) призначений для обслуговування сертифікатів відкритих ключів користувачів та контролера домену, а також надання (за необхідності) користувачам і контролеру домену засобів генерації особистих та відкритих ключів. Програмно-технічний комплекс (ПТК) ЦСК забезпечує: обслуговування сертифікатів користувачів та контролера домену; надання користувачам та контролеру домену (за необхідності) засобів генерації особистих та відкритих ключів. Для взаємодії з центром сертифікації ключів (використання його інтерактивних служб) користувачі та контролер домену повинні мати можливість мережевого підключення до ЦСК. Усі механізми взаємодії з ЦСК виконують бібліотеки користувача ЦСК. Зміна статусу сертифікатів (блокування, поновлення або скасування) та знищення особистих ключів користувачів та контролера домену здійснюється у відповідності до порядку, який визначений ЦСК (згідно регламенту ЦСК).

В якості ПТК ЦСК має використовуватися комплекс "ІІТ ЦСК-1". Далі наведемо розроблені і впроваджені апаратні засоби КЗІ.

Електронний ключ "Кристал-1Д"

Засіб (див. рис. 11) виконує наступні функції: автентифікацію оператора ЕОМ при доступі до ключа; генерацію ключів; зберігання ключів у внутрішній пам'яті та захист їх від НСД; формування і перевірку ЕП; розподіл ключових даних та шифрування даних; зберігання довільних даних у внутрішній пам'яті та захист їх від НСД; контроль цілісності і працездатності вбудованого програмного забезпечення та ін.

Рис. 11. Електронний ключ "Кристал-1Д"

Засіб призначений для захисту службової інформації. Електронний ключ виконаний у вигляді малогабаритного знімного USB-пристрою. Конструктивно електронний ключ виконаний на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар та встановлена у металевий корпус, що формує зовнішній вигляд засобу. На друкованій платі встановлюються електроні компоненти та USB-з'єднувач типу A-plug (виделка). Швидкість формування ЕП – 100 мс. Швидкість розподілу ключових даних – 800 мс. Швидкість шифрування – 800 Кбіт/с.

IP-шифратор "Канал-101ДЕ"

IP-шифратор (див. рис. 12) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

Рис. 12. Р-шифратор "Канал-101ДЕ"

Засіб призначений для захисту службової інформації. IP-шифратор виконаний у вигляді окремого малогабаритного мережевого пристрою. Конструктивно IP-шифратор є мініатюрною системною платформою у металевому корпусі та має 2 мережних інтерфейси Ethernet 100Base-TX. Швидкість шифрування – не менше 30 Мбіт/с (до 40 Мбіт/с).

IP-шифратор "Канал-201Д"

IP-шифратор (див. рис. 13) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та

введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами. Засіб призначений для захисту службової інформації. IP-шифратор виконаний у вигляді окремого мережевого вузла.

Рис. 13. IP-шифратор "Канал-201Д"

Конструктивно IP-шифратор є системною платформою у металевому корпусі висотою 2U та може встановлюватись в 19-ти дюймову стійку за допомогою полки. Засіб має 2 дуплексні оптичні мережні інтерфейси Ethernet 100Base-SX (тип роз'єму - FC). Засіб має систему спеціального захисту від витоку інформації каналами ПЕМВН. Швидкість шифрування - не менше 75 Мбіт/с (до 100 Мбіт/с).

IP-шифратор "Канал-301Д"

IP-шифратор (див. рис. 14) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

Засіб призначений для захисту службової інформації. IP-шифратор виконаний у вигляді окремого мережевого вузла.

Рис. 14. IP-шифратор "Канал-301Д"

Конструктивно IP-шифратор є системною платформою у металевому корпусі висотою 2U та призначену для встановлення в 19-ти дюймову стійку. Засіб має 2 дуплексні оптичні мережні інтерфейси Ethernet 1000Base-SX (тип роз'єму - FC). Засіб має систему спеціального захисту від витоку інформації каналами ПЕМВН. Швидкість шифрування – не менше 350 Мбіт/с (до 1 Гбіт/с).

IP-шифратор "Канал-401Д"

IP-шифратор (див. рис. 15) виконує наступні функції: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; приймання та передачу управляючої (технологічної) інформації; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами. IP-шифратор виконаний у вигляді окремого мережевого вузла. Конструктивно IP-шифратор є системною платформою у металевому корпусі висотою 2U та призначену для встановлення в 19-ти дюймову стійку. Засіб має 2 дуплексні оптичні мережні інтерфейси Ethernet 10GBASE-SR (тип роз'єму - FC). Засіб має систему спеціального захисту від витоку інформації каналами ПЕМВН. Швидкість шифрування – не менше 5 Гбіт/с (до 15 Гбіт/с).

Рис. 15. IP-шифратор "Канал-401Д"

АС «Оберіг» Міністерства оборони України

Комплекси КЗІ, які побудовані з використанням IP-шифратор Канал-101ДЕ та Канал-301Д, входять до складу спеціального забезпечення та віддаленого управління «ІІТ захист IP-потоку-2Д.

Віддалене управління IP-шифраторами», що є основними складовими елементами захисту інформації автоматизованої інформаційно-телекомунікаційній системи «Оберіг» (далі – АС «Оберіг»).

Комплекс КЗІ АС «Оберіг» призначений для збирання, зберігання, обробки та використання даних про військовозобов'язаних (призовників), створена для забезпечення військового обліку громадян України та на теперішний час охоплюють понад 600 мереж спеціального призначення.

АС «Оберіг» створено та розгорнуто у відповідності до Закону України № 1951-VIII від 16 березня 2017 року «Про Єдиний державний реєстр військовозобов'язаних», Концепції військової кадрової політики у ЗС України на період до 2020 року (затверджена наказом Міністерства оборони України № 342 від 26.06.2017) та є одною зі складових розвитку військової кадрової політики – впровадження єдиної автоматизованої інформаційно-аналітичної системи обліку та управління персоналом до окремої військової частини та застосовування її у повсякденній діяльності служб персоналу. АС «Оберіг» впроваджено та стало функціонує у: кадрових органах ЗС України верхнього рівня, які здійснюють функції управління персоналом (Департаменті кадрової політки МО України, Головному управлінні персоналом ГШ ЗС України, Кадровому центрі ГШ ЗС України), та середнього рівня (управління персоналу та Кадрові центри видів ЗС України) та об'єднує дані від систем, які вже працюють у ЗС або будуть створюватись. АС «Оберіг» має потужний механізм для аналітичного опрацювання всієї інформації, яка вноситься до загальних баз даних, та можливість відображати данні у зручній наочній формі.

Крім того, АС «Оберіг» має низку переваг, а саме: є можливість створювати аналітичні звіти; до підсистеми закладено потужний пошуковий механізм за всіма типами даних, що внесені до баз даних; забезпечено цілісність та повноту накопиченої інформації; унеможливлено багаторазове введення даних та наявність розбіжностей в них; розширені можливості для створення і здійснення не тільки звітності, але й смартформ (бланків, що автоматично заповнюються на основі запитів); ведення документообігу. Окремі елементи АС «Оберіг» встановлено та використовується у:

Міністерство оборони України; Генеральному штабі Збройних Сил України; обласні військові комісаріати та оперативні командування (у межах повноважень за військово-адміністративним поділом території України); районні (міські) військові комісаріати.

Спеціальна інформаційно-телекомунікаційна система Національної системи конфіденційного зв'язку

Спеціальна інформаційно-телекомунікаційна система органів виконавчої влади є складовою Національної системи конфіденційного зв'язку (СІТС НСКЗ) створено відповідно до Закону України від 10.01.2020 № 2919-III «Про Національну систему конфіденційного зв'язку» та Розпорядження Кабінету Міністрів України від 11.06.2003 № 338-р «Про створення спеціальної інформаційно-телекомунікаційної системи органів виконавчої влади» з метою побудови спеціальної інформаційно-телекомунікаційної системи органів виконавчої влади та забезпечення циркуляції інформації з обмеженим доступом, крім інформації, що становить державну таємницю, в інтересах органів державної влади та органів місцевого самоврядування, юридичних та фізичних осіб незалежно від форми власності, створюються належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.

Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям встановлюється Кабінетом Міністрів України (постанова КМУ від 11.10.2002 №1519 «Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям»).

Головним виконавцем робіт із створення СІТС НСКЗ визначено державне підприємство «Українські спеціальні системи» (далі – ДП «УСС») яка виконує роботи із створення абонентських пунктів СІТС НСКЗ із використанням криптографічного захисту службової інформації IP-шифратор «Канал-101ДЕ», IP-шифратор «Канал-201Д» та IP-шифратор «Канал-301Д» та їх підключення до головного комутаційного центру.

На сьогодні ДП «УСС» є провідним надавачем послуг конфіденційного зв'язку, у тому числі надання у користування захищених каналів передачі даних, захищеного доступу до Інтернету органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним особам у мережі НСКЗ.

Засоби КЗІ на базі IP-шифраторів «Канал-101ДЕ», «Канал-201Д» та «Канал-301Д» використовуються для забезпечення функціонування абонентських пунктів СІТС НСКЗ та організації захищеного каналу зв'язку для доступу автоматизованих робочих місць в багатьох міністерствах та відомствах України та на теперішній час охоплюють понад 2 000 мереж спеціального призначення.

Захищена телекомунікаційна мережа Державної міграційної служби України

На виконання вимог Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» та відповідно до «Плану заходів із запровадження документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, у які імплантовано безконтактний електронний носій, і створення національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства на 2014 - 2017 роки», затвердженого розпорядженням Кабінету Міністрів України від 20 серпня 2014 р. № 780-р, проведено роботи з розгортання в територіальних органах Державної міграційної служби України та їх підрозділах захищеної телекомунікаційної мережі шляхом встановлення відповідного обладнання та організації захищених каналів зв'язку.

Для організації захищених каналів зв'язку використовується обладнання криптографічного захисту службової інформації IP-шифратор «Канал-101ДЕ», IP-шифратор «Канал-201Д» та IP-шифратор «Канал-301Д» виробництва Приватного акціонерного товариства «Інститут інформаційних технологій» (АТ «ІІТ»).

Висновки

В роботі реалізовано проекти з розробки та впровадження програмно-технічних комплексів та апаратних засобів КЗІ для надавачів електронних довірчих послуг Збройних сил України, Міністерства внутрішніх справ, Державної прикордонної служби, Державної податкової служби України, Національного банку України, Приватбанку, Укрсіббанку, Альфа банку тощо, всього – 17 комплексів, включно по два технологічні центри сертифікації ключів для Центрального засвідчувального органу України та засвідчувального центру Національного банку України. Таким чином, розроблені програмно-технічні комплекси та апаратні засоби КЗІ створили безпечне пост-квантове довкілля для державних електронних інформаційних ресурсів.

Література

[1]. О.О. Кузнецов, О.В. Потій, М.О. Полуяненко, Ю.І. Горбенко. *Потокові шифри. Монографія*. Під загальною редакцією І.Д. Горбенка. Х.: Форт, 2019.- 541 с.

[2]. *ISCI'2017: Information Security in Critical Infrastructures*. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017.–207 p.

[3]. Паціра Є.В. *Энциклопедия безопасности авиации* / Кулик М.С., Харченко В.П., Корченко О.Г. // Монографія. – К.: Техника, 2008. – 1000 с.

[4]. Корченко А.О. *Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія*, Київ, ЦП «Компринт», 2019. – 361 с.

[5]. Zadiraka V. Spectral methods of computer steganography problem decision / V. Zadiraka, N. Koshkina // *Methods of effective protection of information flows*. – Ternopil: Terno-graf, 2014. – Ch. 4. – pp. 96–120.

[6]. А. Корченко, Є. Іванченко, Н. Кошкіна, О. Кузнецов, О. Качко, О. Потій, В. Онопрієнко, В. Бобух. Стандартизація систем, комплексів та засобів КЗІ для застосування у пост-квантовому довкілі. *Захист інформації*. Том 22, № 4. К.: НАУ, 2020, С. 227-262.

УДК 004.056

Корченко А.А., Иванченко Е.В., Кошкина Н.В., Кузнецов А.А., Качко Е.Г., Потый А.В., Оноприенко В.В., Бобух В.А. Современные комплексы пост-квантовой безопасности государственных электронных информационных ресурсов.

Аннотация. В настоящее время в условиях широкого внедрения цифровых технологий в экономическую, оборонную сферы и сферу безопасности, во всех ведущих странах мира остро стоит проблема обеспечения безопасности их киберпространства, особенно в условиях новых угроз, порождаемых использованием квантовых компьютеров. Поэтому создание в Украине соответствующей системы безопасности киберпространственной окружающей среды национальной критической информационной инфраструктуры, в частности комплексов и средств обнаружения вторжений, криптографической и стеганографической защиты информации, является современной и актуальной проблематикой, которая непосредственно касается пост-квантовой информационной и кибербезопасности нашего государства, а также имеет важное общегосударственное и оборонное значение и существенно влияет на обеспечение национальной безопасности Украины в условиях ведения информационных и гибридных войн. Исходя из актульности проблемы обеспечения национальной безопасности Украины в условиях ведения информационных и гибридных войн, целью работы является совершенствование систем специального назначения за счет построения комплексов криптографической защиты информации пост-квантовой безопасности государственных электронных информационных ресурсов. В работе реализованы проекты по разработке и внедрению программно-технических комплексов и аппаратных средств криптографической защиты информации для поставщиков электронных доверительных услуг Вооруженных сил Украины, Министерства внутренних дел, Государственной пограничной службы, Государственной налоговой службы Украины, Национального банка Украины, Приватбанка, УкрСиббанка, Альфа банка и т.д., включительно по два технологических центра сертификации ключей для Центрального удостоверяющего органа Украины и удостоверяющего центра Национального банка Украины. Таким образом, разработанные программно-технические комплексы и аппаратные средства криптографической создали безопасную пост-квантовую окружающую среду для государственных электронных информационных ресурсов.

Ключевые слова: сетей передачи данных специального назначения, криптографические средства, комплексы специального назначения, средства защиты информации, киберпространство, пост-квантовая окружающая среда, государственные электронные информационные ресурсы.

Korchenko A., Ivanchenko Ye., Koshkina N., Kuznetsov O., Kachko O., Potiy O., Onoprienko V., Bobukh V. Modern developed of post-quantum safety of state-owned electronic information resources.

Abstract. Currently, in the context of the widespread introduction of digital technologies in the economic, defense and security spheres, in all the leading countries of the world there is an acute problem of ensuring the security of their cyberspace, especially in the context of new threats generated by the use of quantum computers. Therefore, the creation in Ukraine of an appropriate security system for the cyberspace environment, national critical information infrastructure, in particular intrusion detection systems and tools, cryptographic and steganographic information protection, is a modern and topical issue that directly concerns the post-quantum information and cybersecurity of our state, and also has an important national and defense significance and significantly affects the national security of Ukraine in the context of information and hybrid wars. Proceeding from the urgency of the problem of ensuring the national security of Ukraine in the context of information and hybrid wars, the aim of the work is to improve special purpose systems by building complexes of cryptographic information protection of post-quantum security of state electronic information resources.The work has implemented projects for the development and implementation of software and hardware systems and hardware cryptographic protection of information for providers of electronic trust services of the Armed Forces of Ukraine, the Ministry of Internal Affairs, the State Border Guard Service, the State Tax Service of Ukraine, the National Bank of Ukraine, Privatbank, UkrSibbank, Alfa Bank, etc., including two technological and logical centers for certification of keys for the Central Certification Authority of Ukraine and the Certification Center of the National Bank of Ukraine. Thus, the developed software and hardware systems and cryptographic hardware have created a secure post-quantum environment for state electronic information resources.

Keywords: special purpose data transmission networks, cryptographic tools, special purpose complexes, information protection means, cyberspace, post-quantum environment, state electronic information resources.

Корченко Анна Олександрівна, д.т.н., доцент, професор кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.

Корченко Анна Александровна, д.т.н., доцент, профессор кафедры безопасности информационных технологий факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета.

Korchenko Anna, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Technology Security, Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.

Іванченко Євгенія Вікторівна, к.т.н., професор, професор кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.
Иванченко Евгения Викторовна, к.т.н., профессор, профессор кафедры безопасности информационных технологий факультета кибербезопасности, компьютерной и программной инженерии Национального авиационного университета.
Ivanchenko Yevheniya, Candidate of Technical Sciences, Professor, Professor of the Department of Information Technology Security, Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.

Кошкіна Наталія Василівна, д.т.н., старший науковий співробітник, старший науковий співробітник відділу оптимізації чисельних методів, Інститут кібернетики імені В.М. Глушкова НАН України.
Кошкина Наталья Васильевна, д.т.н., старший научный сотрудник, старший научный сотрудник отдела оптимизации численных методов, Институт кибернетики имени В.М. Глушкова НАН Украины.
Koshkina Natalia, Doctor of Technical Sciences, Senior Researcher, Senior Research Fellow, Department of Optimization of Numerical Methods, Institute of Cybernetics Glushkova NAS of Ukraine.

Кузнецов Олександр Олександрович, д.т.н., професор, професор кафедри безпеки інформаційних систем і технологій факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна, заступник головного конструктора приватного акціонерного товариства «Інститут інформаційних технологій».
Кузнецов Александр Александрович, д.т.н., профессор, профессор кафедры безопасности информационных систем и технологий факультета компьютерных наук Харьковского национального университета имени В. Н. Каразина, Заместитель главного конструктора частного акционерного общества «Институт информационных технологий».
Kuznetsov Oleksandr, Doctor of Technical Sciences, Professor, Professor of the Department of Information Systems Security and Technologies, Faculty of Computer Science, VN Karazin Kharkiv National University, Deputy Chief Designer of the Private Joint-Stock Company "Institute of Information Technologies".

Качко Олена Григорівна, к.т.н., професор, професор кафедри програмної інженерії факультету комп'ютерних наук Харківського національного університету радіоелектроніки, заступник головного конструктора приватного акціонерного товариства «Інститут інформаційних технологій».
Качко Елена Григорьевна, к.т.н., профессор, профессор кафедры программной инженерии факультета компьютерных наук Харьковского национального университета радиоэлектроники, заместитель главного конструктора частного акционерного общества «Институт информационных технологий».
Kachko Olena, Candidate of Technical Sciences, Professor, Professor of the Department of Software Engineering, Faculty of Computer Science, Kharkiv National University of Radio Electronics, Deputy Chief Designer of the Private Joint-Stock Company "Institute of Information Technologies".

Потій Олександр Володимирович, д.т.н., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України.
Потий Александр Владимирович, д.т.н., профессор, заместитель Председателя Государственной службы специальной связи и защиты информации Украины.
Potiy Oleksandr, Doctor of Technical Sciences, Professor Deputy Head of the State Service for Special Communications and Information Protection of Ukraine.

Онопрієнко Віктор Васильович, кт.н., старший науковий співробітник, генеральний директор приватного акціонерного товариства «Інститут інформаційних технологій».
Оноприенко Виктор Васильевич, к.т.н., старший научный сотрудник, генеральный директор частного акционерного общества «Институт информационных технологий».
Onoprienko Viktor, Candidate of Technical Sciences, Senior Researcher General Director of the Private Joint-Stock Company "Institute of Information Technologies".

Бобух Всеволод Анатолійович, к.т.н., начальник відділу апаратних засобів захисту інформації приватного акціонерного товариства «Інститут інформаційних технологій».
Бобух Всеволод Анатольевич, начальник отдела аппаратных средств защиты информации частного акционерного общества «Институт информационных технологий».
Bobukh Vsevolod, Candidate of Technical Sciences, Head of the Department of Information Protection Hardware of the Private Joint-Stock Company "Institute of Information Technologies".

Отримано *22 березня 2021 року*, затверджено редколегією *19 квітня 2021 року*