DOI 10.33099/2618-1614-2022-19-2-51-55
УДК 004.056

О. С. Бойченко,
кандидат технічних наук, начальник науково-дослідного відділу охорони державної таємниці та захисту інформації, Житомирський військовий інститут імені С. П. Корольова,

В. В. Умінський,
кандидат технічних наук, старший науковий співробітник, заступник начальника кафедри охорони державної таємниці та захисту інформації, Житомирський військовий інститут імені С. П. Корольова,

Б. В. Кримець,
головний спеціаліст відділу Центрального управління охорони державної таємниці та захисту інформації, Генеральний штаб Збройних Сил України

Удосконалення інфраструктури відкритих ключів Збройних Сил України

У статті проведено аналіз інфраструктури відкритих ключів Збройних Сил України та національної системи електронних довірчих послуг України. За результатами аналізу визначене актуальне науково-практичне завдання щодо розробки технології надання електронних довірчих послуг в інформаційно-комунікаційних системах Збройних Сил України, де обробляється інформація, що містить державну таємницю. Обґрунтовані додаткові вимоги до інфраструктури відкритих ключів ЗСУ щодо захисту інформації під час обміну секретними електронними документами користувачами інформаційно-комунікаційних систем ЗСУ різного рівня секретності. Розроблено типову структуру програмно-технічного комплексу системи обігу секретних електронних документів ЗСУ, в якій введені нові апаратно-програмні рішення для організації обміну секретними електронними документами між користувачам інформаційно-комунікаційних систем ЗСУ різного рівня секретності. Наведена інфраструктура відкритих ключів ЗСУ забезпечить роботу військовослужбовцям та працівникам ЗСУ, які мають сертифікат відкритого ключа, з будь-якого робочого місця в інформаційно-комунікаційних системах ЗСУ різного рівня секретності згідно з політикою безпеки інформації у відповідній інформаційно-комунікаційній системі ЗСУ.

Ключові слова: інфраструктура відкритих ключів, електронні довірчі послуги, секретний електронний документ.

На початку XXI ст. з метою розширення послуг із захисту інформації та інформаційних ресурсів почав широко застосовуватись електронний підпис, заснований на відповідних криптографічних механізмах. Це сприяло тому, що в інформаційно-комунікаційних системах (ІКС) в умовах протидії порушникам (зловмисникам) почали надаватися базові послуги (виконуватися функції) або вирішуватися завдання забезпечення з необхідним рівнем гарантій конфіденційності, цілісності, справжності (автентичності), неспростовності (спостережливості), доступності та надійності.

Провідними вченими України в галузі криптографічного захисту інформації була розроблена, впроваджена, а на сьогодні постійно вдосконалюється національна система електронних довірчих послуг (ЕДП).

Національна система ЕДП – організаційно-технічна система, яка інтегрує сертифікати відкритих ключів, засоби електронного підпису чи печатки, надавачів ЕДП та власників сертифікатів у єдину структуру.

Основними складовими національної системи ЕДП є Центральний засвідчувальний орган, кваліфіковані надавачі ЕДП, надавачі ЕДП, засвідчувальний центр Національного банку України з кваліфікованими надавачами ЕДП і надавачами ЕДП банків, контролюючий орган та користувачі ЕДП [1].

З метою забезпечення функціонування національної системи ЕДП в Україні прийнято низку нормативно-правових документів, які регламентують склад і порядок надання ЕДП [1–4].

У Збройних Силах України (ЗСУ) кваліфіковані ЕДП посадовим особам Міністерства оборони України, Апарату Головнокомандувача ЗСУ, Генерального штабу ЗСУ, органів військового управління, вищих військових навчальних закладів, військових частин, установ, організацій ЗСУ та інших військових формувань, організацій, що діють в інтересах обороноздатності держави, надає кваліфікований надавач ЕДП «Центр сертифікації ключів Збройних Сил України» (КНЕДП «ЦСК ЗСУ») [5]. Відомості про КНЕДП «ЦСК ЗСУ» внесені до довірчого списку, розміщеного на офіційному сайті Центрального засвідчувального органу Міністерства цифрової трансформації України [6].

До переліку кваліфікованих ЕДП, надання яких забезпечує КНЕДП «ЦСК ЗСУ», належать:

- створення, перевірка та підтвердження кваліфікованого електронного підпису чи печатки;
- формування, перевірка та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;
- формування, перевірка та підтвердження кваліфікованої електронної позначки часу [5].

КНЕДП «ЦСК ЗСУ» забезпечує надання кваліфікованих ЕДП в автоматизованій системі управління повсякденною діяльністю ЗСУ «Дніпро» та в інформаційних системах з доступом до мережі Інтернет (ІСД-Інтернет).

Але у ЗСУ існують проблемні питання, які не дають змоги повною мірою забезпечити електронну взаємодію та захист інформації в ІКС відповідно до вимог законодавства України та стандартів НАТО:

1. ЕДП у ЗСУ надаються для ІКС ЗСУ, в яких обробляється відкрита інформація або інформація, що належить до державних інформаційних ресурсів.

2. Повільне впровадження технічних рішень, які забезпечать можливість надання ЕДП в ІКС, де обробляється службова інформація, за рахунок використання мережевих шлюзів, що мають чинний експертний висновок у галузі криптографічного й технічного захисту інформації.

3. Відсутність можливості надання кваліфікованих ЕДП у захищеній системі обміну інформацією (ЗСОІ) ЗСУ не дає змоги застосувати кваліфікований електронний підпис для забезпечення обміну секретними електронними документами (електронного документообігу інформації, що становить державну таємницю).

4. Відсутність складової системи надання кваліфікованих ЕДП, які розгортаються на відокремлених пунктах реєстрації в польових умовах для забезпечення розмежування доступу та автентифікації посадових осіб ЗСУ в ІКС у районах виконання завдань та на навчаннях.

5. Відсутність порядку взаємодії інфраструктури відкритих ключів ЗСУ з інфраструктурами відкритих ключів збройних сил держав – членів НАТО. Керівні документи, які регламентують порядок перевірки цифрових сертифікатів випущених надавачами кваліфікованих ЕДП у збройних силах держав – членів НАТО нині перебувають на стадії розробки. Саме відсутність таких керівних документів унеможливлює ЗСУ стати повноправним учасником федеративної мережі місій і здійснювати обмін інформацією та розвідувальними даними під час спільних операцій держав – членів НАТО та країн-партнерів.

Тому перед ЗСУ постає важливе завдання з розробки технології надання кваліфікованих ЕДП в ІКС ЗСУ, в яких обробляється секретна інформація. Виникнення цього актуального науково-технічного завдання зумовлене об'єктивним протиріччям між високими вимогами до захисту секретної інформації відповідно до вимог законодавства України і стандартів НАТО та принциповою неможливістю її захисту за рахунок використання існуючої інфраструктури відкритих ключів у ЗСУ.

Метою статті є вдосконалення інфраструктури відкритих ключів (ІВК) ЗСУ для надання кваліфікованих ЕДП в ІКС ЗСУ, де обробляється секретна інформація.

Виклад основного матеріалу

Головною вимогою до ІВК ЗСУ є забезпечення гарантованої довіри до ЕДП, які надаються в ІКС, де обробляється відкрита, службова та секретна інформація.

Для надання ЕДП в ІКС ЗСУ, де обробляється секретна інформація, необхідно забезпечити доступ до цієї ІКС за рахунок застосування організаційних і технічних заходів [7]. Організаційні заходи мають забезпечити обмеження доступу підписувачам та користувачам ЕДП до об'єкта інформаційної діяльності, на якому розміщене автоматизоване робоче місце (АРМ) з можливістю роботи в ІКС, де обробляється секретна інформація, відповідно до форми допуску до державної таємниці користувача ЕДП. Технічні заходи повинні бути реалізовані за рахунок використання функцій ідентифікації та авторизації користувачів ІКС, де обробляється секретна інформація. Наведенні вище функції не передбачені в існуючих ІКС та системах спеціального зв'язку. Відсутня також функція розмежування доступу до відповідних електронних документів. Згідно з вимогами нормативної документації з технічного захисту інформації наявність розмежування доступу до секретного документа є одним з методів протидії несанкціонованому доступу [7].

Під секретним електронним документом слід розуміти секретний документ, інформація в якому зафіксована у вигляді електронних даних, включно з обов'язковими реквізитами секретного документа.

З метою вдосконалення ІВК ЗСУ необхідно передбачити:

1) створення єдиної бази даних секретних електронних документів ЗСУ з упровадженою системою розмежування доступу;

2) створення механізму взаємодії між ІКС, у яких обробляється інформація з різним грифом секретності (грифом обмеження доступу);

3) розширення повноважень КНЕДП «ЦСК ЗСУ» щодо впровадження механізму надання кваліфікованих ЕДП в ІКС, у яких обробляється інформація з різним грифом секретності (грифом обмеження доступу);

4) цілодобовий доступ до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, а також до інформації про статус відкритих ключів користувачам ІКС, у яких обробляється секретна інформація;

5) розробку військових публікацій, які регламентують установлення довіреної ідентифікації між ІКС ЗСУ та ІКС збройних сил держав – членів НАТО у федеративній мережі місій.

Ураховуючи викладене, ІВК ЗСУ матиме уповноважений орган у сфері ЕДП у ЗСУ, КНЕДП «ЦСК ЗСУ», підписувачів та користувачів ЕДП (*рис. 1*).

Уповноважений орган у ЗСУ призначений для організації спеціального зв'язку та захисту інформації у сферах ЕДП та електронної ідентифікації у ЗСУ. До його повноважень належить забезпечення:

- відомчого контролю за дотриманням вимог законодавства у сфері ЕДП;
- установлення вимог з безпеки та захисту інформації КНЕДП «ЦСК ЗСУ» та його відокремлених пунктів реєстрації;
- погодження регламентів КНЕДП «ЦСК ЗСУ»;
- взаємодії з контролюючим органом національної системи ЕДП;

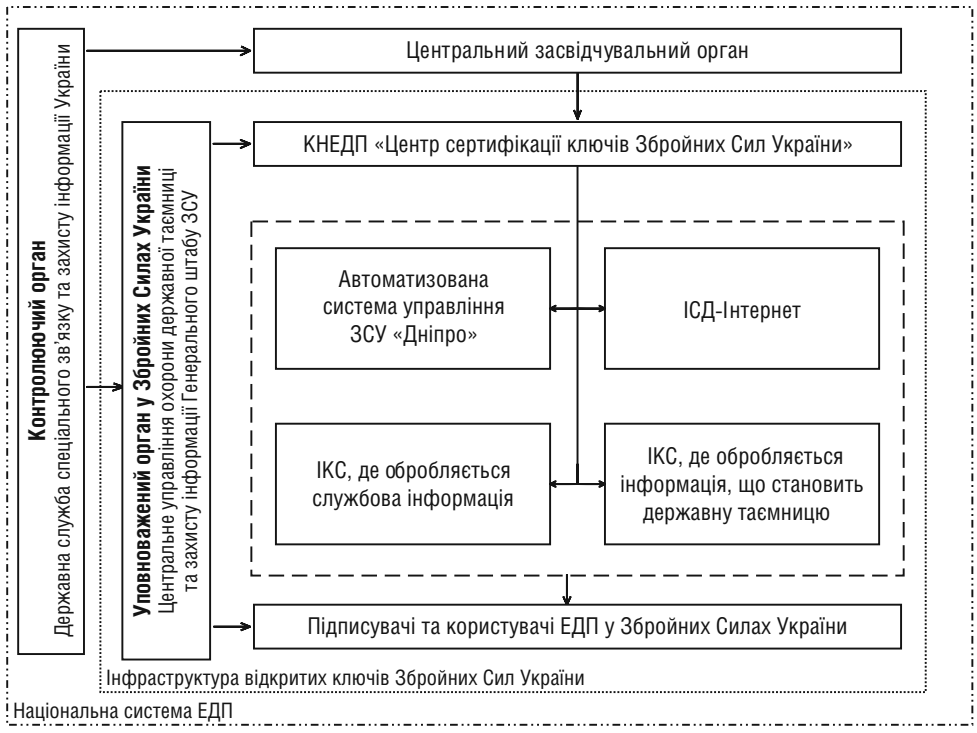

Рис. 1. Інфраструктура відкритих ключів у Збройних Силах України

• видання приписів щодо усунення порушень вимог законодавства у сфері ЕДП;

• відомчого регулювання з питань електронної ідентифікації з використанням ЕДП у ЗСУ;

• визначення стандартів, що застосовуються при наданні довірчих послуг у сфері спеціального зв'язку та під час установлення довіреної ідентифікації у федеративній мережі місій.

Кваліфікований надавач ЕДП у ЗСУ – визначений підрозділ, який надає одну або більше кваліфікованих ЕДП в автоматизованій системі управління повсякденною діяльністю ЗСУ, в ІСД-Інтернет та в ІКС, де обробляється службова інформація та інформація, що становить державну таємницю.

Підписувачі та користувачі ЕДП у ЗСУ – створювачі електронних печаток, відправники та отримувачі електронних даних, які одержують ЕДП у кваліфікованих надавачів ЕДП у ЗСУ.

Безпосередньо функції довірчої сторони виконують програмно-технічні комплекси, які використовуються під час надання ЕДП і являють собою апаратні, апаратно-програмні та програмні засоби КНЕДП «ЦСК ЗСУ».

Додатково в ІВК ЗСУ повинні виконуватись такі вимоги щодо забезпечення режиму секретності під час обміну секретною інформацією в ІКС ЗСУ:

1. Передача інформації з ІКС вищого рівня секретності до нижчої має відбуватися за умови наявності в ІКС нижчого рівня секретності апаратури, що може бути підключена до мережі спеціального зв'язку ІКС вищого рівня секретності. Необхідною умовою є також забезпечення неможливості потрапляння секретних електронних документів з вищим грифом секретності до ІКС, де обробляються секретні електронні документи з нижчим грифом секретності.

2. Взаємодія між ІКС різного рівня секретності повинна бути організована з використанням серверів взаємодії, які мають чинний атестат відповідності Державної служби спеціального зв'язку та захисту інформації України.

Під сервером взаємодії слід розуміти окремо виділені спеціальні апаратні та програмно-апаратні засоби, призначені для унеможливлення витоку секретних електронних документів під час їх передачі між ІКС різного рівня секретності, у тому числі й у федеративній мережі місій. Сервер взаємодії може виконувати такі функції:

• автоматизована перевірка секретного електронного документа щодо можливості його відправки до ІКС вищого (нижчого) рівня секретності;

• створення маршруту проходження секретного електронного документа між ІКС різних рівнів секретності.

З урахуванням наведеного та результатів науково-дослідних робіт [8, 9] на *рисунку 2* зображено перспективну схему організації ІВК у ЗСУ. Структура і склад кожної мережі визначається відповідно до загальних вимог до ІКС ЗСУ різного рівня секретності (обмеження доступу).

Інформаційно-комунікаційна мережа (ІКМ) ІКС, де обробляються секретні електронні документи з грифом

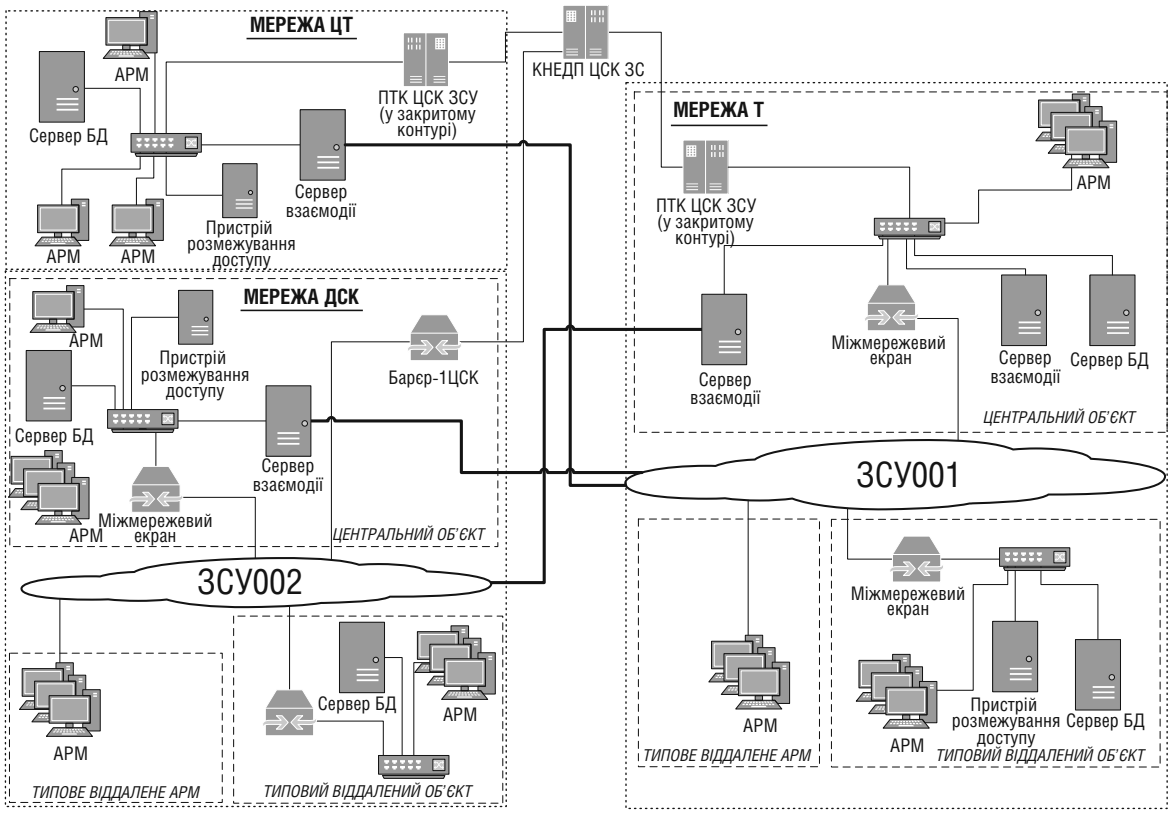

Рис. 2. Перспективна схема організації ІВК у ЗСУ

секретності «Цілком таємно» (далі – ІКС-ЦТ), може бути представлена як ІКС класу 2.

ІКМ ІКС, де обробляються секретні електронні документи з грифом секретності «Таємно» (далі – ІКС-Т), може бути виконана як розподілена ІКС класу 3 з каналами зв'язку, які використовуються ЗСУ. На даний час для обміну інформацією з грифом секретності «Таємно» у ЗСУ використовується захищена система обміну інформацією ЗСУ001.

ІКМ ІКС, де обробляються електронні документи з грифом обмеження доступу «Для службового користування» (далі – ІКС-ДСК), може бути виконана як ІКС класу 3. На даний час для обміну інформацією з грифом обмеження доступу «Для службового користування» у ЗСУ використовується мережа обміну службовою інформацією ЗСУ002. В ІКМ ІКС передбачається можливість надання кваліфікованих ЕДП з використанням шлюзу мережного типу «Бар'єр», котрий забезпечує запобігання витоку інформації, що обробляється в закритому сегменті ІКМ, у підключений до нього відкритий сегмент, в якому розміщений центр сертифікації ключів.

Під сервером баз даних слід розуміти захищений електронно-обчислювальний засіб у серверному виконанні з установленим спеціалізованим програмним забезпеченням, який виконує функції сервера додатків на базі Web-технологій для забезпечення обміну секретними електронними документами між користувачами ІКС, їх зберігання, розмежування доступу до секретних електронних документів користувачів та обробки секретних електронних документів відповідно до політки безпеки інформації в ІКС за допомогою пристрою розмежування доступу.

Пристрій розмежування доступу – електронно-обчислювальний засіб з установленим спеціалізованим програмним забезпеченням, призначений для:

- створення бази користувачів ІКС;
- створення бази електронно-обчислювальних засобів ІКС;
- створення бази комутаторів;
- авторизації користувачів ІКС;
- розмежування доступу до ресурсів серверу баз даних.

Комутатор – пристрій, призначений для з'єднання декількох АРМ у межах одного об'єкта (центрального або віддаленого).

Автоматизоване робоче місце – електронно-обчислювальний засіб на основі персональної електронної обчислювальної машини чи засобу спеціального зв'язку, на якому встановлений мінімально потрібний комплект програмного забезпечення з обов'язковою наявністю Інтернет-браузера. Кожен електронно-обчислювальний засіб повинен мати свій ідентифікатор у базі даних електронно-обчислювальних засобів ІКС.

Відповідно до політики безпеки в ІКС на автоматизованих робочих місцях за допомогою програмних засобів, розміщених на сервері даних, передбачений особистий кабінет користувача ІКС. Передбачається, що авторизований користувач ІКС може мати доступ до свого особистого кабінету з будь-якого електронно-обчислювального засобу ІКС. При цьому гриф секретності інформації, яку може обробляти користувач ІКС, буде обмежений максимально дозволеним грифом секретності (грифом обмеження доступу) інформації, котру можна обробляти на відповідному електронно-обчислювальному засобі.

Міжмережевий екран – програмно-апаратний комплекс, який реалізує функцію контролю вхідного і вихідного трафіку в ІКМ ІКС одного рівня секретності.

Програмно-технічний комплекс КНЕДП «ЦСК ЗСУ» в закритому контурі – апаратні, апаратно-програмні та програмні засоби, призначені для:

- надання кваліфікованих ЕДП в ІКС ЗСУ відповідного рівня секретності;
- оновлення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;
- цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів.

Висновки. У запропонованій інфраструктурі відкритих ключів Збройних Сил України кваліфікований надавач електронних довірчих послуг «Центр сертифікації ключів Збройних Сил України» генерує пару ключів для всіх військовослужбовців та працівників ЗСУ, сертифікати відкритих ключів яких використовуватимуться в усіх інформаційно-комунікаційних системах ЗСУ.

Надання електронних довірчих послуг користувачам інформаційно-комунікаційних систем Збройних Сил України здійснюватиметься за грифами секретності секретних електронних документів та за рівнем допуску до роботи з державною таємницею відповідного користувача інформаційно-комунікаційної системи ЗСУ.

Застосування серверів взаємодії дасть змогу реалізувати взаємодію інфраструктури відкритих ключів ЗСУ з інфраструктурами відкритих ключів збройних сил держав – членів НАТО для здійснення обміну інформацією та розвідувальними даними під час спільних операцій держав – членів НАТО.

Перелік літератури

1. Про електронні довірчі послуги [Електронний ресурс] : Закон України № 2155-VIII від 5 жовтня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2155-19#Text.

2. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності [Електронний ресурс] : постанова Кабінету Міністрів України № 749 від 19 вересня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/749-2018-п#Text.

3. Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг [Електронний ресурс] : постанова Кабінету Міністрів України від 7 листопада 2018 р. № 992 // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/992-2018-п#Text.

4. Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів [Електронний ресурс] : постанова Кабінету Міністрів України № 193 від 3 березня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/193-2020-п#Text.

5. Кваліфікований надавач електронних довірчих послуг «Центр сертифікації ключів Збройних Сил України» для Міністерства оборони України та Збройних Сил України [Електронний ресурс] // КНЕДП «Центр сертифікації ключів Збройних Сил України». – Режим доступу : https://ca.mil.gov.ua/main.

6. Довірчий список [Електронний ресурс] // Центральний засвідчувальний орган. Міністерство цифрової трансформації України. – Режим доступу : https://www.czo.gov.ua/trustedlist.

7. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : постанова Кабінету Міністрів України № 180 від 16 лютого 1998 р. // Верховна Рада України. Законодавство України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/180-98-п#Text.

8. Науково-дослідна робота, шифр «Фундамент» : звіт про НДР (остаточний) / Житомирський військовий інститут імені С. П. Корольова ; кер. О. Бойченко. – Житомир, 2019. – 119 с.

9. Науково-дослідна робота, шифр «Фундамент-ТТЗ» : звіт про НДР (остаточний) / Житомирський військовий інститут імені С. П. Корольова ; кер. О. Бойченко. – Житомир, 2020. – 103 с.