1. ІДЕНТИФІКАЦІЯ ОБ'ЄКТА ЕКСПЕРТИЗИ

Об’єктом експертизи є комплекс засобів захисту програмної системи корпоративної електронної пошти «FossDocMail» версії 6.x (x – ціле невід’ємне число). Склад програмних модулів, що входять до складу програмного забезпечення об’єкту експертизи наведено в п. 6.2 до цього документу.

Враховуючи, що відповідно до ГОСТ 19.101-77 програмна система корпоративної електронної пошти «FossDocMail» відноситься до програмних комплексів, в подальшому викладі для її позначення використовується скорочення «комплекс».

Дія експертного висновку розповсюджується на зразки програмної системи корпоративної електронної пошти «FossDocMail», які мають версію збірки 6.x (x – ціле невід’ємне число), мають склад програмного забезпечення якого відповідає даним, наведеним в п. 6.2 цього документу, та які виготовлені ТОВ «ФОСС-Он-Лайн» протягом терміну його дії, з урахуванням умов, зазначених у розділі 8 до цього документу.

2. ЗАГАЛЬНІ ВІДОМОСТІ ЩОДО ОБ'ЄКТА ЕКСПЕРТИЗИ

2.1 Найменування та відомості про розробника

Повне найменування об’єкту експертизи: комплекс засобів захисту програмної системи корпоративної електронної пошти «FossDocMail».

Розробник та виробник об’єкту експертизи: товариство з обмеженою відповідальністю «ФОСС-Он-Лайн» (фізична адреса: м. Харків, вул. Дарвіна, 20).

2.2 Призначення та стислий опис об’єкту експертизи

Комплекс являє собою програмну платформу для організації корпоративних систем обміну електронними поштовими повідомленнями між співробітниками організаціями.

Комплекс забезпечує сумісну роботу користувачів та можливість розсилки всієї необхідної інформації між користувачами системи та зовнішніми абонентами.

Комплекс надає наступні функціональні можливості:

- відправлення та гарантоване отримання користувачами електронних поштових повідомлень;
- можливість отримання сповіщень про доставку та перегляд електронних поштових повідомлень;
- централізоване керування та адміністрування системи;
- особисті каталоги користувачів;
- загальні каталоги з розмежуванням доступу користувачів;
- делегування прав доступу користувачів до поштових скриньок та особистих каталогів;
- встановлення черговості (пріоретизацію) доставки електронних поштових повідомлень в залежності від групи (категорії) користувачів.

Комплекс забезпечує обмін поштовими повідомленнями як всередині організації, так і з зовнішніми абонентами в мережі Інтернет.

Комплекс надає механізми доставки та повідомлень про доставку / перегляд повідомлень, які пересилаються між зареєстрованими користувачами.

Комплекс забезпечує підтримку протоколів та програмних інтерфейсів SMTP, MIME, S/MIME, X.509 та POP3.

Комплекс підтримує присвоєння індивідуальної електронної поштової адреси кожному співробітнику.

Передбачена можливість ведення облікових даних користувачів в адресній книзі на українській мові.

Інтерфейс адміністрування надає можливість захищеного віддаленого управління всіма компонентами системи.

Комплекс забезпечує:

- можливість квотування розміру пересланого повідомлення за різними групами користувачів;
- можливість застосування квот на розмір поштових скриньок користувачів;
- можливість блокування та / або видалення користувачів;
- можливість застосування профілів при реєстрації користувачів;
- можливість роботи з групами користувачів.

Загальна архітектура комплексу наведена на рис. 2.1. Комплекс складається з двох взаємопов’язаних прикладних систем «FossMail» та «FossDoc».

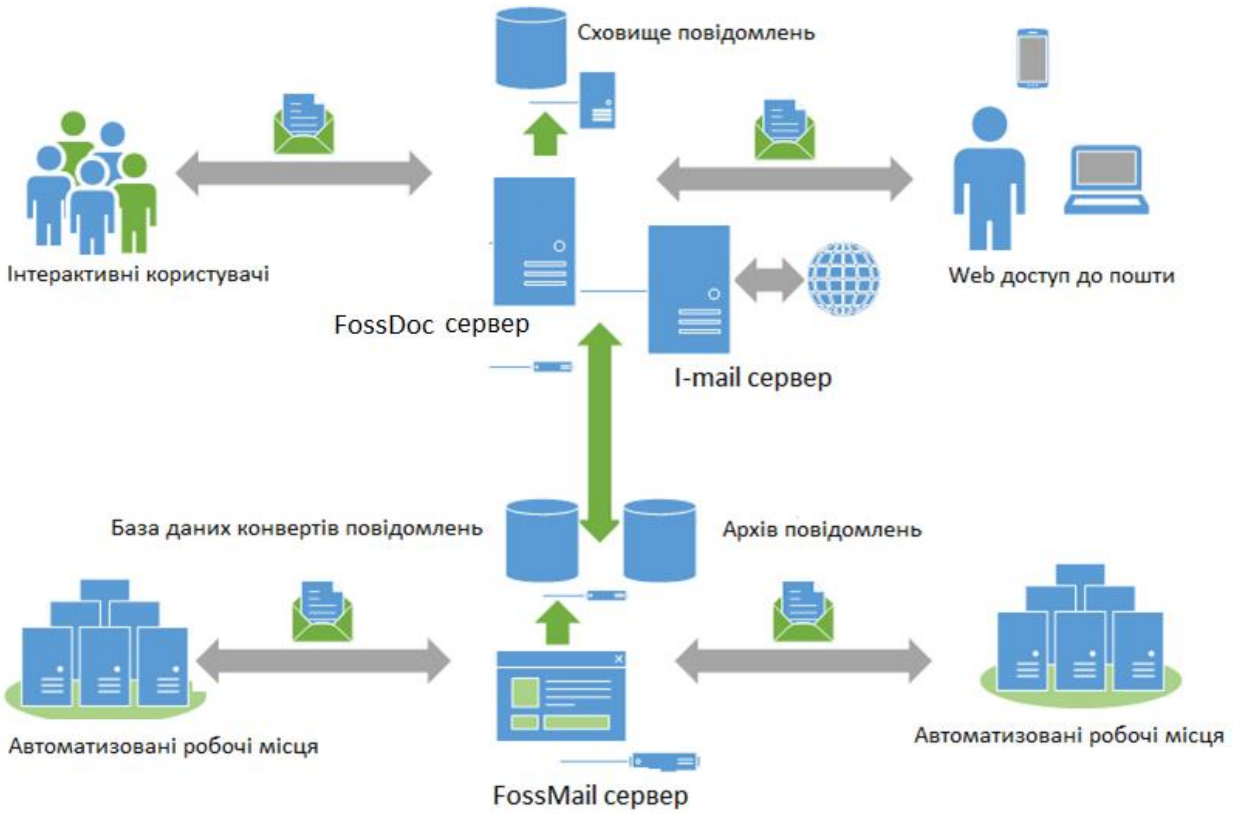

Рис. 2.1. Загальна архітектура комплексу

Прикладна система «FossMail» призначена для забезпечення реалізації транспортного рівня обміну електронними поштовими повідомленнями.

Прикладна система «FossDoc» призначена для реалізації функцій управління комплексом.

Прикладна система «FossMail» (FossMail-сервер на рис. 2.1) призначена для забезпечення реалізації транспортного рівня обміну електронними поштовими повідомленнями та реалізує наступні функції:

- гарантована передача електронних поштових повідомлень;
- формування звітів про доставку електронних поштових повідомлень;
- маршрутизація електронних поштових повідомлень;
- ведення бази даних електронних поштових повідомлень;
- архівація електронних поштових повідомлень;
- робота з автоматизованими робочими місцями користувачів;
- ведення черги електронних поштових повідомлень на відправку;
- налаштування алгоритму передачі електронних поштових повідомлень;
- захист від дублювання електронних поштових повідомлень;
- обмін адресними книгами.

До складу прикладної системи «FossMail» входять наступні окремі модулі (див. рис. 2.2), які реалізують такі функціональні завдання:

- модуль *FMRP*, який реалізує процесор запитів FossMail та здійснює розсилку адресних книг, а також перевірку коректності доставки електронних поштових повідомлень від/до користувачів, зареєстрованих в системі;
- модуль *Mserver*, який реалізує механізм реєстрації електронних поштових повідомлень у базі даних;
- модуль *Router*, який реалізує механізм маршрутизації електронних поштових повідомлень (розбір вхідної черги і перекладка електронних поштових повідомлень у відповідні поштові скриньки);
- модуль *Fmqueue*, який реалізує механізм управління чергою електронних поштових повідомлень за напрямками залежно від пріоритетів поштових скриньок і пріоритетів повідомлень;
- модуль *АПФ*, який реалізує механізм прийому / передачі електронних поштових повідомлень по каналах зв'язку;
- модуль *Fmarc*, який реалізує механізм архівації електронних поштових повідомлень в ZIP-файли для подальшого їх зберігання;
- модуль *Fbarc*, який реалізує механізм архівації баз даних та перенесення інформації з робочих баз даних в архівні;
- модуль *Fmstat*, який реалізує механізми перегляду робочих і архівних баз даних, розпакування електронних поштових повідомлень з архівів і файлів з повідомлень;
- модуль *Fshell*, який є відповідним програмним інтерпретатором, за допомогою якого забезпечується створення та управління сценаріями роботи з електронними поштовими повідомленнями зі створення, розпакування, додавання полів тощо;
- модуль *CfgClient*, який реалізує механізм віддаленого управління конфігурацією вузла;
- модуль *Exmon*, який призначений для запуску і зупинки серверу системи, а також відображення його поточного стану.

Прикладна система «FossDoc» (FossDoc-сервер на рис. 2.1) призначена для реалізації функцій управління комплексом та реалізує наступні функції:

- формування даних щодо організаційної структури організації;
- підтримку списку користувачів;

- автентифікацію користувачів;
- роботу з Web-клієнтами;
- зберігання електронних поштових повідомлень користувачів в базі даних;
- формування електронних поштових повідомлень;
- роботу з адресними книгами;
- формування груп розсилки;
- розмежування та делегування прав доступу;
- роботу з електронними поштовими повідомленнями на рівні окремих працівників та на рівні функціональних підрозділів організації.

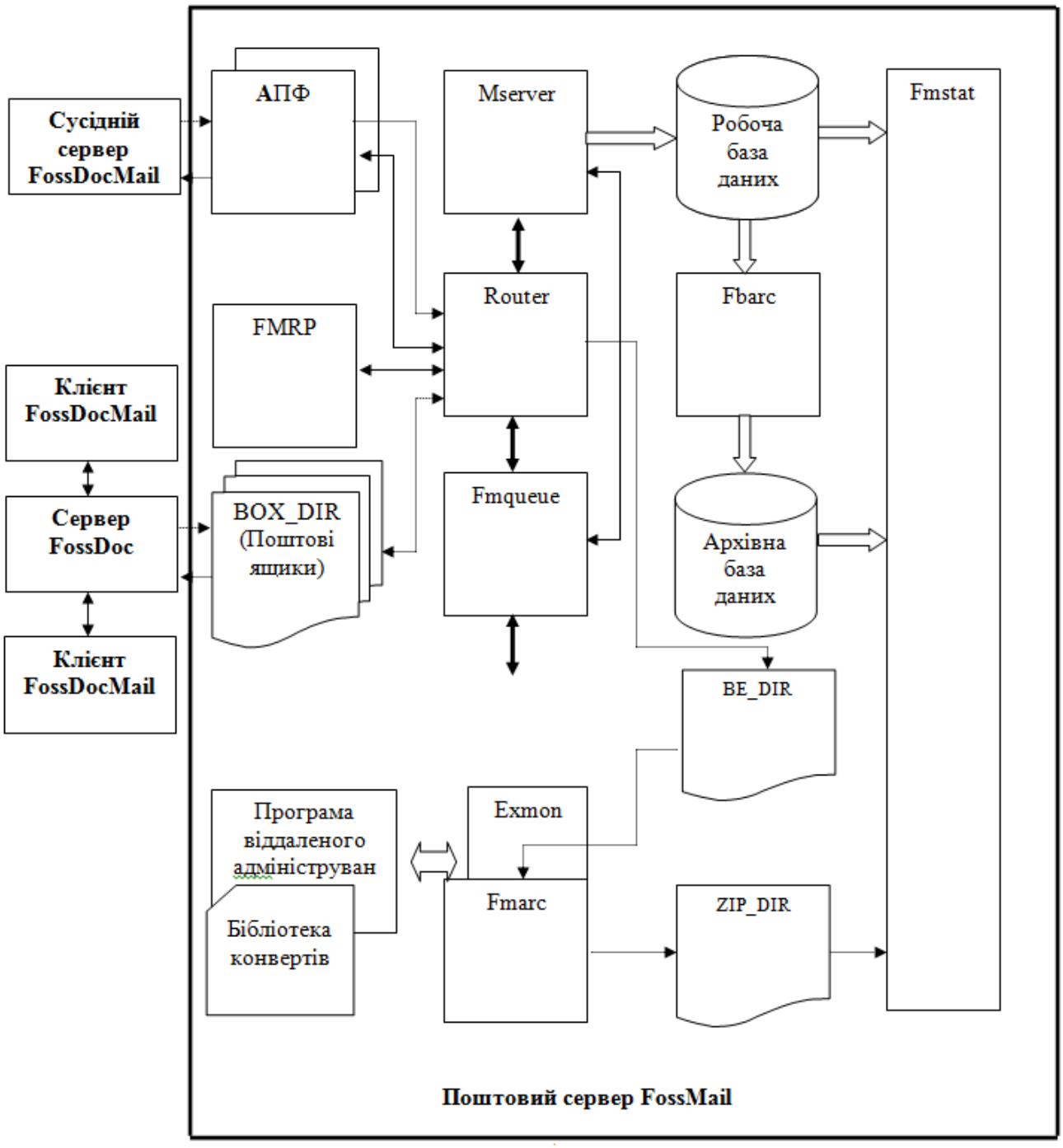

Рис. 2.2. Склад та порядок функціонування прикладної системи «FossMail»

До складу прикладної системи «FossDoc» входять наступні окремі

модулі (див. рис. 2.3), які реалізують такі функціональні завдання:

- *модуль «Провайдер бази даних»*, який призначений для взаємодії серверу додатків з системою управління базами даних (набір програмних бібліотек, що реалізують відповідний прикладний програмний інтерфейс); автоматизоване робоче місце користувачів має доступ до бази даних лише через відповідний провайдер;

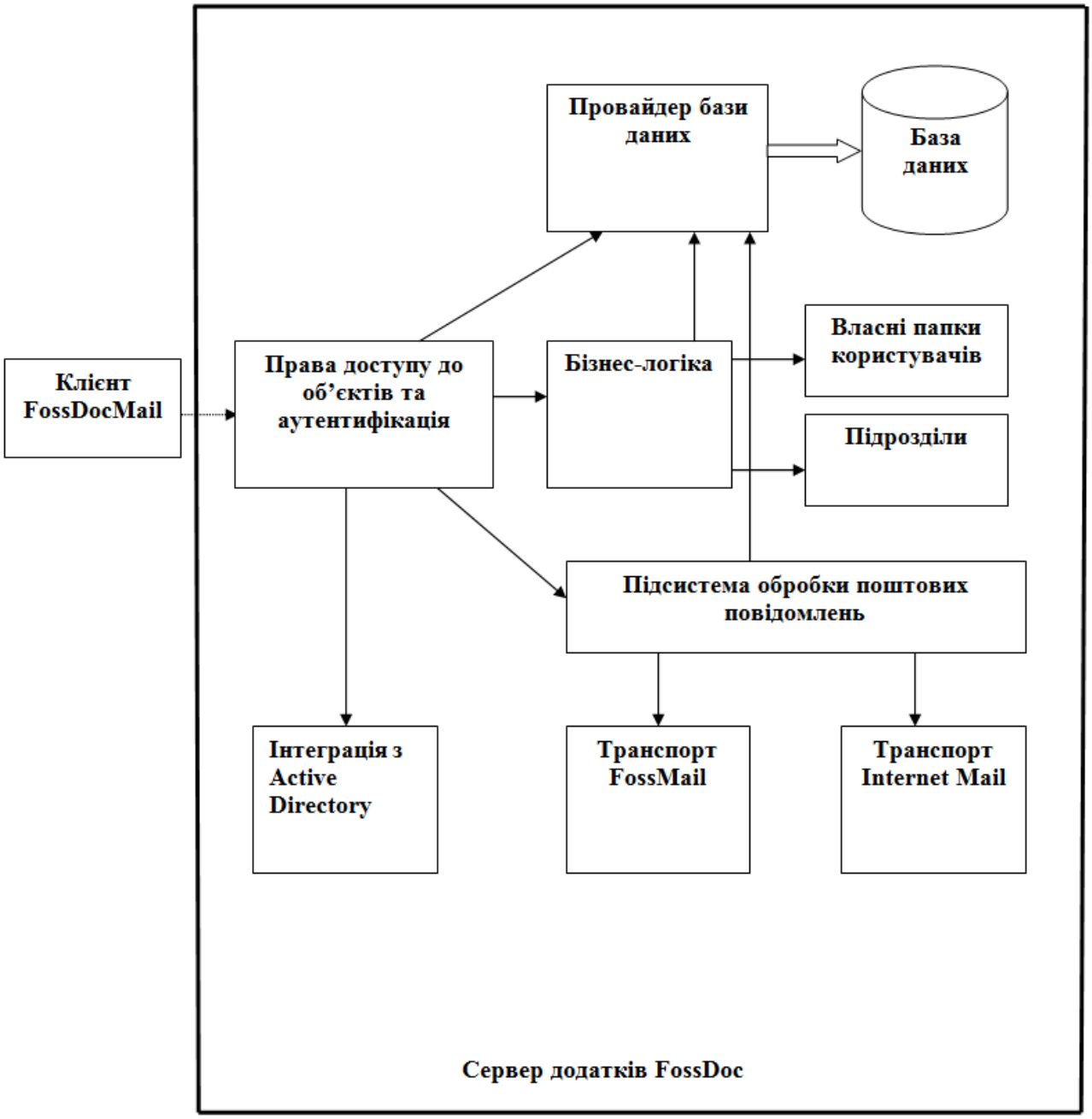

Рис. 2.3. Склад та порядок функціонування прикладної системи «FossDoc»

- *модуль «База даних»*, який побудований на базі системи управління базами даних Microsoft SQL Server, MySQL або Oracle та використовується для збереження документів, поштових повідомлень, даних щодо організаційної структури організації, списку користувачів, прав доступу, а також усіх інших технологічних даних, необхідних для роботи комплексу;

- *модуль «Права доступу до об'єктів та автентифікація»*, який забезпечує автентифікацію користувачів в системі, перевірки прав доступу до будь-яких документів, папок, поштових скриньок тощо; у разі використання

режиму автентифікації Windows співпрацює з модулем «Інтеграція з Active Directory»;

- *модуль «Бізнес-логіка»*, який відповідає за підтримку даних щодо організаційної структури організації, роботи користувачів, та надає можливості роботи з бібліотеками документів;
- *модуль «Власні папки користувачів»*, який зберігає електронні поштові повідомлення та персональні контакти для кожного користувача;
- *модуль «Підрозділи»*, який містить опис структури організації та забезпечує організацію роботи користувачів та поштових скриньок на рівні функціональних підрозділів організації;
- *модуль «Підсистема обробки поштових повідомлень»*, який відповідає за взаємодію з модулями «Транспорт FossMail» та «Транспорт InternetMail»;
- *модуль «Транспорт FossMail»*, який відповідає за взаємодію системи з поштовим вузлом FossMail, виконує отримання та відправку поштових повідомлень з поштового серверу;
- *модуль «Транспорт InternetMail»*, який відповідає за взаємодію системи з поштовим вузлом InternetMail, а також дозволяє працювати як самостійний поштовий сервер;
- *модуль «Інтеграція з Active Directory»*, який забезпечує взаємодію з існуючим доменом Microsoft Windows з метою ідентифікації та автентифікації користувачів.

I-mail-сервер забезпечує обмін електронними поштовими повідомленнями за протоколом SMTP/POP3 та дозволяє користувачам працювати з ними.

Автоматизоване робоче місце користувачів забезпечує:

- перегляд електронної поштової кореспонденції;
- підготовка електронної поштової кореспонденції;
- пошук електронної поштової кореспонденції;
- пересилку електронної поштової кореспонденції;
- роботу з контактами;
- управління налаштуваннями робочого місця;
- автентифікацію користувача;
- криптографічний захист конфіденційності, цілісності та автентичності електронних поштових повідомлень.

Комплекс розроблений ТОВ «ФОСС-Он-Лайн» (фізична адреса: м. Харків, вул. Дарвіна, 20) згідно технічного завдання («Технічне завдання на створення програмної системи корпоративної електронної пошти «FossDocMail»).

Комплекс структурно складається з *наступних компонентів*:

- серверний компонент комплексу;
- клієнтський компонент комплексу.

Серверний компонент комплексу призначений для централізованої обробки та зберігання всіх даних, що циркулюють в комплексі, в рамках виконання зазначених вище операцій, а також надання користувачам комплексу графічного інтерфейсу для введення, перегляду та обробки даних в комплексі.

Клієнтський компонент комплексу призначений для введення, перегляду та обробки даних в комплексі.

Комплекс призначений для застосування в складі інформаційно-телекомунікаційних систем (ІТС) класу 2 та 3 (згідно НД ТЗІ 2.5-005-99), побудованих за клієнт-серверною технологією. При цьому серверний компонент комплексу використовується на серверній частині таких систем, а клієнтський компонент – на клієнтській частині ІТС відповідно.

При передачі інформації між компонентами комплексу через неконтрольоване середовище обміну (глобальну мережу Інтернет) забезпечується захист конфіденційності та цілісності інформації, що передається, а також взаємна автентифікація компонент комплексу перед початком обміну даними між ними.

2.4 Умови застосування

Клієнтський компонент комплексу функціонує на робочій станції, яка складається з обчислювальної машини на платформі Intel X86 або еквівалентній з наступними параметрами:

- процесор Intel Pentium / Celeron 1800 МГц та вище;
- обсяг оперативного запам’ятовуючого пристрою не менш за 256 Мб;
- обсяг вільного місця на накопичувачі на жорсткому магнітному диску (НЖМД) не менш за 70 Гб.

Серверний компонент комплексу функціонує на ЕОМ серверного типу, яка складається з обчислювальної машини на платформі Intel X86 або еквівалентній з наступними параметрами:

- процесор Intel Pentium / Xeon 2400 МГц та вище;
- обсяг оперативного запам’ятовуючого пристрою не менш за 512 Мб;
- обсяг вільного місця на НЖМД не менш за 250 Гб.

Для функціонування комплексу потрібна наявність такого системного та прикладного програмного забезпечення:

- клієнтська або серверна операційна система Microsoft Windows версії від XP SP3 або вище;
- система управління базами даних Microsoft SQL Server (версії від 2008 або вище), Oracle (версії від 10g або вище) або PostgreSQL (версії від 9.1.13 або вище).

3. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ЕКСПЕРТИЗИ

До складу комплексу входить комплекс засобів захисту інформації від несанкціонованого доступу (далі – КЗЗ), який призначений для забезпечення захисту інформації, яка зберігається, обробляється та передається в комплексі.

Вимоги до КЗЗ комплексу викладені в частковому технічному завданні («Програмна система корпоративної електронної пошти «FossDocMail». Часткове технічне завдання. Вимоги щодо забезпечення захисту інформації від несанкціонованого доступу»), погодженому з Адміністрацією Держспецзв’язку.

КЗЗ комплексу забезпечує виконання наступних функцій:

- забезпечення цілісності програмного забезпечення комплексу;
- реєстрація подій, пов’язаних із діями користувачів в комплексі, а також зі зміною даних, що обробляються та зберігаються в комплексі;

– ідентифікація та автентифікація користувачів комплексу;

– розмежування доступу користувачів до об’єктів захисту комплексу;

– створення та управління обліковими записами користувачів;

– можливість доступу до об’єктів захисту комплексу лише за умови введення коректних атрибутів доступу користувача.

Для реалізації функцій криптографічного захисту інформації в комплексі використовується засіб криптографічного захисту інформації «Бібліотека криптографічних перетворень «UALib» (UA.АЭЛА.0000-01 90 01) виробництва ТОВ «НВЦ «Безпека інформаційних технологій і систем», який має позитивний чинний (на момент проведення експертизи) експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації, на момент проходження експертизи є чинним та містить відомості щодо правильності реалізації механізмів шифрування та електронного цифрового підпису, відповідності засобу нормативним документам в сфері криптографічного захисту інформації, а також можливості його використання для криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю, та службової інформації), а також відкритої інформації, вимогу щодо захисту якої встановлено законом від 18.02.2014 № 05/02/02-549.

Об'єктом експертних випробувань є КЗЗ комплексу. Експертним випробуванням підлягає сукупність програмних засобів, які входять до складу КЗЗ комплексу та призначені для реалізації політики безпеки інформації згідно вимог часткового технічного завдання («Програмна система корпоративної електронної пошти «FossDocMail». Часткове технічне завдання. Вимоги щодо забезпечення захисту інформації від несанкціонованого доступу», далі – ЧТЗ).

Державна експертиза в сфері технічного захисту інформації комплексу проводиться на виконання рішення Експертної ради з питань державної експертизи в сфері технічного захисту інформації Адміністрації Держспецзв’язку (протокол засідання від 25.05.2015 № 6-2015).

4. ВИМОГИ НОРМАТИВНИХ ДОКУМЕНТІВ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, НА ВІДПОВІДНІСТЬ ЯКИМ ЗДІЙСНЮЄТЬСЯ ОЦІНКА ОБ'ЄКТА ЕКСПЕРТИЗИ

Експертні роботи здійснювалися на відповідність наступним нормативним документам з технічного захисту інформації:

– часткове технічне завдання «Програмна система корпоративної електронної пошти «FossDocMail». Часткове технічне завдання. Вимоги щодо забезпечення захисту інформації від несанкціонованого доступу»;

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;

– НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;

– НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

5. МЕТОДИКА ПРОВЕДЕННЯ РОБІТ

Державна експертиза в сфері технічного захисту інформації комплексу проводилась ТОВ «Мале підприємство «Дина» згідно погоджених Департаментом технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України програми та методики державної експертизи у сфері технічного захисту інформації.

6. ПЕРЕЛІК ДОКУМЕНТІВ І СПЕЦИФІКАЦІЙ ПРОГРАМНИХ ТА ТЕХНІЧНИХ ЗАСОБІВ, ЯКІ НАДАНО ЗАМОВНИКОМ ОРГАНІЗАТОРУ ЕКСПЕРТИЗИ

6.1 Перелік документів, наданих для проведення експертних випробувань:

1. «Технічне завдання на створення програмної системи корпоративної електронної пошти «FossDocMail».
2. «Програмна система корпоративної електронної пошти «FossDocMail». Часткове технічне завдання. Вимоги щодо забезпечення захисту інформації від несанкціонованого доступу».
3. Матеріали проектування програмної системи корпоративної електронної пошти «FossDocMail»:
   - 3.1 «Электронная почта «FossMail». Краткое описание FossMail».
   - 3.2 «Электронная почта «FossMail». Общее описание».
   - 3.3 «Электронная почта «FossMail». Описание динамической библиотеки fservdll.dll».
4. Матеріали внутрішніх (попередніх) випробувань програмної системи корпоративної електронної пошти «FossDocMail».
5. Експлуатаційна документація на програмну систему корпоративної електронної пошти «FossDocMail»:
   - 5.1 «Электронная почта «FossMail». Рабочее место абонента почты FossMail32 (MAPI транспорт для почты FossMail32)».
   - 5.2 «Электронная почта «FossMail». Инсталляция и настройка узла».
   - 5.3 «Электронная почта «FossMail». Руководство администратора узла».
   - 5.4 «Электронная почта «FossMail». Требования к аппаратному и программному обеспечению».
   - 5.5 «Электронная почта «FossMail». FBArc. Программа архивирования рабочей базы данных электронной почты FossMail».
   - 5.6 «Электронная почта «FossMail». FBArc. Программа архивации сообщений FMarc».
   - 5.7 «Электронная почта «FossMail». FBArc. Процессор запросов».

5.8 «Электронная почта «FossMail». FBArc. Программа просмотра баз данных FMStat».
5.9 «Электронная почта «FossMail». FBArc. Чистильщик каталогов».
5.10 «Электронная почта «FossMail». FBArc. Программа Mserver».
5.11 «Электронная почта «FossMail». FBArc. Менеджер очереди сообщений FMQueueMngr».
5.12 «Электронная почта «FossMail». FBArc. Агент передачи файлов TCPAPF».
5.13 «Электронная почта «FossMail». FBArc. Интерпретатор сценариев FShell».

Далі за текстом документу наводяться посилання на окремі документи з наведеного переліку.

6.2 Специфікації програмних засобів, наданих для проведення експертних випробувань:

Серверна частина	
Каталог `ru`	Файли локалізації на російську мову
Каталог `uk`	Файли локалізації на українську мову
Каталог `Deployment`	Файли оновлень клієнтської частини
Каталог `EM`	Зовнішні модулі сервера
Каталог `Instances`	Технологічні налаштування сервера
Каталог `MySQL`	Файли бази MySQL
Каталог `WebTemplates`	Файли сторінок для веб-сервера
Каталог `XSP`	Веб-сервер
`Foss.FossDoc.Updater.exe`	Основний виконуваний файл для оновлення програмного забезпечення комплексу
`Ionic.Zip.Host.exe`	Виконуваний файл розпакування оновлень
`Foss.FossDoc.ApplicationServer.Connection.dll`	Бібліотека для підключення до сервера
`Foss.FossDoc.ApplicationServer.Interfaces.dll`	Бібліотека інтерфейсів сервера
`Foss.FossDoc.Archiver.dll`	Бібліотека для роботи з архівом оновлень
`Foss.FossDoc.Messaging.Mail MessageAdapting.Interfaces.dll`	Бібліотека інтерфейсів по роботі з поштовими повідомленнями
`Foss.FossDoc.PluginsUpdater.dll`	Бібліотека по роботі з клієнтськими оновленнями
`Foss.FossDoc.ThreadManagement.dll`	Бібліотека по роботі з потоками
`Foss.FUIS.dll`	Бібліотека елементів користувацького інтерфейсу
`Foss.FUIS.Localization.dll`	Бібліотека по роботі з локалізацією
`Foss.ServiceAdvertising.dll`	Бібліотека пошуку служб серверів
`Foss.TemplateLibrary.dll`	Бібліотека алгоритмів і шаблонних функцій
`FossDocApplicationServerDotNet ProxyStubs.dll`	Бібліотека-проксі для інтерфейсів сервера

IIOPChannel.dll	Бібліотека протоколу CORBA
Interop.DSOFramer.dll	Бібліотека по роботі з HTML-повідомленнями
Ionic.Zip.dll	Бібліотека по роботі з zip-архівами
Foss.FossDoc.Updater.exe.config	Конфігураційний файл клієнта
Сайт FossDocMail.url	Ярлик сайту продукту
Форум FossDocMail.url	Ярлик форуму продукту
FossDoc Application Server.exe	Основний виконуваний файл серверу
FossDoc Application Server.exe.config	Конфігураційний файл серверу
FossDoc Application Server Configurator.exe	Конфігуратор серверу
FossDoc Application Server Configurator.exe.config	Конфігураційний файл конфігуратору серверу
FossDoc Solution Deployer.exe	Виконуваний файл імпорту та експорту даних
FossDoc Solution Deployer.exe.config	Конфігураційний файл для імпорту та експорту даних
FossDoc Solution Deployer MYSQL.exe	Виконуваний файл імпорту та експорту даних на MySQL
FossDoc.Monitor.exe	Виконуваний файл моніторингу потоків сервера
Foss.Deployment.InstallRetinue.dll	Бібліотека інсталяції
Foss.Diagnostics.Loggers.dll	Бібліотека реєстрації подій
Foss.DualServiceModel.dll	Бібліотека роботи з сервісами
Foss.FAB.FossDocManagement.dll	Бібліотека роботи з адресними книгами
Foss.FAB.Management.dll	Бібліотека роботи з адресними книгами
Foss.FossDoc.ApplicationServer.dll	Головна бібліотека серверу
Foss.FossDoc.ApplicationServer.ApplicationConfigurationFile Upgrade.dll	Бібліотека оновлення файлів конфігурацій
Foss.FossDoc.ApplicationServer.Cryptography.Microsoft.dll	Провайдер цифрового підпису Microsoft
Foss.FossDoc.ApplicationServer.DatabaseProvider.dll	Бібліотека провайдеру баз даних
Foss.FossDoc.ApplicationServer.DatabaseProvider.Configurator.dll	Бібліотека конфігуратору провайдерів баз даних
Foss.FossDoc.ApplicationServer.DatabaseProvider.MSSQL.dll	Бібліотека провайдеру бази MS SQL Server
Foss.FossDoc.ApplicationServer.DatabaseProvider.MSSQL.Configurator.dll	Бібліотека конфігуратору MS SQL Server
Foss.FossDoc.ApplicationServer.DatabaseProvider.MySQL.dll	Бібліотека провайдеру бази MySQL
Foss.FossDoc.ApplicationServer.DatabaseProvider.MySQL.Configurator.dll	Бібліотека MySQL Server
Foss.FossDoc.ApplicationServer.ExternalModules.Implementation.dll	Бібліотека реалізації модулів сервера

Foss.FossDoc.ApplicationServer.Licensing.dll	Бібліотека для управління ліцензіями на використання комплексу
Foss.FossDoc.ApplicationServer.Messaging.Interfaces.dll	Бібліотека інтерфейсів по роботі з повідомленнями
Foss.FossDoc.ApplicationServer.Messaging.TextFormatConversion.dll	Бібліотека по роботі з текстом
Foss.FossDoc.Cryptography.dll	Бібліотека криптографії
Foss.FossDoc.Cryptography.Inter.dll	Бібліотека інтерфейсів криптографії
Foss.FossDoc.Cryptography.Microsoft.dll	Бібліотека криптографії Microsoft
Foss.FossDoc.ExternalModules.EDMS.Components.dll	Бібліотека компоненту EDMS
Foss.FossDoc.Messaging.Mail MessageAdapting.dll	Бібліотека по роботі з повідомленнями
Foss.GoogleAnalytics.dll	Бібліотека Google Analytics
Foss.InternetMail.dll	Бібліотека по роботі з поштою email
Foss.InternetMail.Interfaces.dll	Бібліотека інтерфейсів по роботі з поштою email
fservdll.dll	Бібліотека пакетів FossMail
generic_provider_nbu.dll	Бібліотека провайдеру НБУ
Microsoft.Exchange.Data.Common.dll	Бібліотека утиліт для MS Exchange
MySql.Data.dll	Бібліотека для роботи з MySQL

Клієнтська частина	
Каталог `ru`	Файли локалізації на російську мову
Каталог `uk`	Файли локалізації на українську мову
Foss.FossDoc.Updater.exe	Основний виконуваний файл клієнтської частини
Ionic.Zip.Host.exe	Виконуваний файл для розпакування оновлень
Foss.FossDoc.ApplicationServer.Connection.dll	Бібліотека для підключення до сервера
Foss.FossDoc.ApplicationServer.Interfaces.dll	Бібліотека інтерфейсів сервера
Foss.FossDoc.Archiver.dll	Бібліотека для роботи з архівом оновлень
Foss.FossDoc.Messaging.MailMessageAdapting.Interfaces.dll	Бібліотека інтерфейсів по роботі з поштовими повідомленнями
Foss.FossDoc.PluginsUpdater.dll	Бібліотека по роботі з клієнтськими оновленнями
Foss.FossDoc.ThreadManagement.dll	Бібліотека по роботі з потоками
Foss.FUIS.dll	Бібліотека елементів користувацького інтерфейсу
Foss.FUIS.Localization.dll	Бібліотека по роботі з локалізацією
Foss.ServiceAdvertising.dll	Бібліотека пошуку служб серверів
Foss.TemplateLibrary.dll	Бібліотека алгоритмів і шаблонних функцій
FossDocApplicationServerDotNet ProxyStubs.dll	Бібліотека-проксі для інтерфейсів сервера

IIOPChannel.dll	Бібліотека протоколу CORBA
Interop.DSOFramer.dll	Бібліотека по роботі з HTML-повідомленнями
Ionic.Zip.dll	Бібліотека по роботі з zip-архівами
Foss.FossDoc.Updater.exe.config	Конфігураційний файл клієнта
Сайт FossDocMail.url	Ярлик сайту продукту
Форум FossDocMail.url	Ярлик форуму продукту

7. РЕЗУЛЬТАТИ РОБІТ ЩОДО КОЖНОГО ПУНКТУ ОКРЕМОЇ МЕТОДИКИ ЕКСПЕРТИЗИ ОБ'ЄКТА

7.1 За результатами перевірки вимог до рівня гарантій експерти зробили висновок, що:

– комплекс відповідає вимогам до архітектури рівня гарантій Г-2;

– комплекс відповідає вимогам до середовища розробки рівня гарантій Г-2;

– комплекс відповідає вимогам до послідовності розробки рівня гарантій Г-2;

– комплекс відповідає вимогам до середовища функціонування рівня гарантій Г-2;

– комплекс відповідає вимогам до документації рівня гарантій Г-2;

– комплекс відповідає вимогам до випробувань рівня гарантій Г-2.

– програмне забезпечення комплексу, яке використовується, відповідає безпечній конфігурації та містить всі необхідні механізми захисту інформації, які реалізують визначену в детальному проекті політику безпеки (заходи відображені в документах [5.2, 5.3]).

7.2 За результатами перевірки комплексу на відповідність вимогам по захисту інформації від загроз несанкціонованого доступу експерти зробили такі висновки:

– КЗЗ комплексу коректно реалізує послуги безпеки КА-2, КО-1, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДР-1, ДЗ-1, ДВ-1, НР-2, НИ-1, НИ-2, НК-1, НО-1, НЦ-1, НТ-2, НА-1, НП-1 відповідно до вимог ЧТЗ та НД ТЗІ 2.5-004-99;

– КЗЗ комплексу відповідає вимогам п. 6.2, 6.3, 6.5, 7.2 – 7.4, 8.1, 8.3, 8.4, 9.1 – 9.6, 9.8, 9.9 НД ТЗІ 2.5-004-99 та п. 4.5.5 ЧТЗ.

7.3 Висновки щодо відповідності об'єкта експертизи вимогам нормативних документів системи ТЗІ за результатами експертних випробувань по кожному пункту методики державної експертизи у сфері технічного захисту інформації викладені в документі «Програмна система корпоративної електронної пошти «FossDocMail». Протокол виконання робіт відповідно до розділів 5, 6 методики державної експертизи у сфері технічного захисту інформації».

7.4 Характеристика функціональних послуг безпеки, що реалізуються комплексом

7.4.1 В рамках реалізації *функціональних послуг безпеки «КА-2» та «ЦА-1»* комплекс забезпечує розмежування доступу користувачів до даних, наведених в табл. 7.1.

Таблиця 7.1

Об’єкт захисту	Умовне позначення
програмне забезпечення серверного компоненту	{SERV-SOFT}
програмне забезпечення клієнтського компоненту	{CLNT-SOFT}
електронні поштові повідомлення, які створюються користувачами (разом із вкладеннями)	{MAIL}
квитанції про отримання електронних поштових повідомлень	{RECEIPT}
база електронних поштових повідомлень	{DB-MAIL}
адресна книга користувачів	{ADDRESS}
вкладення до електронних поштових повідомлень, які зберігаються окремо від електронних поштових повідомлень	{ATTACH}
ключові дані, необхідні для формування електронного цифрового підпису на електронних поштових повідомлень	{KEY}
ключові дані, необхідні для перевіряння електронного цифрового підпису на електронних поштових повідомлень	{CERT}
журнали реєстрації подій, що ведуться в системі	{LOG}
конфігураційні та системні об’єкти серверного компоненту, що визначають параметри конфігурації, функціонування та правила розмежування доступу до компонент	{CONFIG}

Комплекс підтримує вбудовані групи (ролі) користувачів, наведені в табл. 7.2.

Таблиця 7.2

Суб’єкт доступу	Умовне позначення
Системний адміністратор (користувач, що має право управління системними налаштуваннями, обліковими записами користувачів та їх правами доступу до інформаційних об’єктів)	[К_СА]
Оператор (користувачі, що здійснюють підготовку та відправлення електронних поштових відправлень)	[К_О]

Атрибутами доступу користувачів є:

- умовний ідентифікатор (логін);
- пароль;
- набір ролей користувача.

Атрибутами інформаційних об’єктів є:

- найменування (ідентифікатор);
- список управління доступом (ідентифікатори користувачів / ролей користувачів та доступні їм для виконання операції: перегляд, модифікація, створення, видалення, експорт тощо).

Комплекс забезпечує реалізацію загальних правил розмежування доступу користувачів до інформаційних об’єктів, наведених в табл. 7.3, 7.4.

Таблиця 7.3

Об’єкт доступу	[К_СА]	[К_О]
{SERV-SOFT}	+	-

{CLNT-SOFT}	+	+
{MAIL}	+	+
{RECEIPT}	+	+
{DB-MAIL}	+	-
{ADDRESS}	+	+
{ATTACH}	+	+
{KEY}	-	+
{CERT}	+	+
{LOG}	+	-
{CONFIG}	+	-

Таблиця 7.4

Суб'єкт	Тип доступу			
	читання	модифікація	створення	видалення
[К_СА]	{SERV-SOFT} {CLNT-SOFT} {MAIL} {RECEIPT} {DB-MAIL} {ADDRESS} {ATTACH} {CERT} {LOG} {CONFIG}	{MAIL} {RECEIPT} {DB-MAIL} {ADDRESS} {ATTACH} {CONFIG}	{SERV-SOFT} {CLNT-SOFT} {MAIL} {RECEIPT} {DB-MAIL} {ADDRESS} {ATTACH} {LOG} {CONFIG}	{SERV-SOFT} {CLNT-SOFT} {MAIL} {RECEIPT} {DB-MAIL} {ADDRESS} {ATTACH} {LOG} {CONFIG}
[К_О]	{CLNT-SOFT} {MAIL} {RECEIPT} {ADDRESS} {ATTACH} {KEY} {CERT}	{MAIL} {RECEIPT} {ATTACH}	{MAIL} {RECEIPT} {ATTACH}	{MAIL} {RECEIPT} {ATTACH}

Права конкретного користувача визначаються правами, що визначені безпосередньо для групи (груп) користувачів, в яку (які) він входить. Додавання нових користувачів та груп користувачів, розподілення користувачів по групам та призначення прав користувачів по відношенню до об'єктів в комплексі здійснюється системним адміністратором.

Користувач, що створює певний інформаційний об'єкт, визначає його розташування в ієрархії об'єктів комплексу. Об'єкт, який містить в собі інші об'єкти, є батьківським по відношенню до цих об'єктів, а новий створюваний об'єкт визначається як дочірній в батьківському контейнері.

Успадковування полягає в тому, що за умовчанням створений (або скопійований) об'єкт успадковує права доступу від батьківського контейнеру. Для цього в дескрипторі батьківського об'єкта встановлюється відповідний керуючий прапор, як ознака успадкування його прав доступу. При змінюванні прав доступу або їх скасуванні в батьківському об'єкті, здійснені зміни застосовуються до всіх дочірніх об'єктів, що успадковують ці права доступу.

Комплекс передбачає можливість експорту інформаційних об'єктів у вигляді об'єктів файлової системи; при цьому встановлені в комплексі для експортованих інформаційних об'єктів атрибути доступу не зберігаються; для експортованих об'єктів автоматично встановлюються атрибути файлової

системи для директорії, в яку здійснено їх експорт; нормативно-розпорядча документація містить опис дій системного адміністратора щодо безпечного поводження з експортованими об’єктами [5.3].

Комплекс передбачає можливість імпорту інформаційних об’єктів відповідного типу, представлених у вигляді об’єктів файлової системи; при цьому при експорті об’єктів для них автоматично встановлюються атрибути доступу, налаштовані в комплексі для об’єктів цього типу; нормативно-розпорядча документація містить опис порядку налаштування прав доступу до інформаційних об’єктів комплексу при відновленні його працездатності системним адміністратором [5.3].

Додатково до наведених механізмів розмежування доступу КЗЗ комплексу забезпечує можливість довірчого управління доступом до електронних поштових повідомлень. Для цього користувач-відправник електронного повідомлення обирає відповідних адресатів, які можуть отримати зазначене повідомлення та переглянути його інформаційний зміст.

7.4.2 В рамках реалізації *функціональної послуги безпеки «КО-1»* КЗЗ комплексу забезпечує скасування прав доступу для користувачів (процесів), які вони можуть одержати при доступі до об’єктів захисту, звільнених іншим користувачем (процесом), а також очищення змісту об’єктів захисту перш ніж певний користувач (процес) зможе одержати їх в своє розпорядження після звільненням цих об’єктів іншим користувачем (процесом) [3.2].

Послуга стосується даних, що зберігаються в оперативному запам’ятовуючому пристрої ЕОМ під час сеансу роботи користувача.

Під час роботи при зміні поточного користувача КЗЗ комплексу здійснює очищення ділянок оперативної пам’яті ЕОМ, які виділялись для сеансу роботи користувача. Очищення ділянок оперативної пам’яті здійснюється в процесі завершення сеансу роботи користувача, вхід до комплексу нового користувача можливий лише за умови успішного завершення процедур очищення.

Додатково для очищення відповідних запам’ятовуючих пристроїв використовуються штатні засоби операційної системи (обнулення або перезапису сторінок пам'яті, відстеження покажчиків читання/запису для дискової пам'яті та захисту сторінкового файлу підкачки тощо).

Обнуління сторінок пам’яті при їхньому звільненні забезпечується потоком обнуління сторінок, який переводить очищенні сторінки в список, з якого потім проводиться їхнє видалення. Такий механізм гарантує обнуління звільненої пам’яті в визначений проміжок часу (цей проміжок залежить від завантаження системи), навіть у випадку відсутності запитів на виділення пам’яті.

Очищення пам’яті забезпечується вибіркою доступних сторінок пам’яті із списку очищених сторінок, а не із усієї множини.

Віртуальна пам'ять використовує системний файл підкачки для витіснення на диск сторінок пам'яті, що не використовуються. Цей файл підкачки відкривається виключно операційною системою і є захищеним від доступу до нього інших користувачів та процесів.

Об’єкти, що зберігаються на диску, мають право використовувати лише той дисковий простір, що необхідний для їхнього виконання. Механізм

використання покажчиків (Read/Write) запобігає читання інформації за межами області, що використовується об’єктом.

7.4.3 В рамках реалізації *функціональної послуги безпеки «ЦО-1»* КЗЗ комплексу забезпечує можливість відкату (відміни) операцій над об’єктами в комплексі. Політика відкату відноситься до об’єктів захисту, що зберігаються в базах даних. Для цього використовується механізм транзакцій, які можуть бути скасовані в повному обсязі, якщо при завершенні їх виконання не отримано відповідне підтвердження. Відкат здійснюється системним адміністратором комплексу в порядку, визначеному в експлуатаційній документації [5.10].

7.4.4 В рамках реалізації *функціональних послуг безпеки «КВ-1» та «ЦВ-1»* КЗЗ комплексу забезпечує конфіденційність та цілісність даних користувача при їх передачі між серверним та клієнтським компонентами, а також між абонентами поштових систем через незахищене середовище (телекомунікаційну мережу загального користування Internet). Для реалізації послуги до складу комплексу входить засіб криптографічного захисту інформації «Бібліотека криптографічних перетворень «UALib» (UA.АЭЛА.0000-01 90 01), який має позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації (від 18.02.2014 № 05/02/02-549).

Користувачі або процеси комплексу можуть керувати рівнем захищеності інформації; документи, що формуються в комплексі, можуть передаватись в захищеному (зашифрованому та підписаному електронним цифровим підписом) вигляді.

7.4.5. В рамках реалізації *функціональної послуги безпеки «ДР-1»* КЗЗ комплексу підтримує можливість обмеження обсягу ресурсів, що виділяються для роботи користувачам [5.2, 5.3]:

- розмір пересланого електронного поштового повідомлення;
- розмір поштових скриньок користувачів.

Оператор не має можливості змінити встановлені обмеження на розмір пересланого електронного поштового повідомлення та розмір поштових скриньок користувачів. Право управління встановленими обмеженнями належить лише системному адміністратору.

7.4.6 В рамках реалізації *функціональної послуги безпеки «ДЗ-1»* комплекс забезпечує можливість оновлення власного програмного забезпечення. Модернізація здійснюється системним адміністратором комплексу без переривання функцій із захисту інформації в порядку, наведеному в експлуатаційній документації.

Модернізація може бути проведена в будь-який момент часу для всіх програмних модулів комплексу. Для оновлення програмних модулів розробником комплексу створюються та розповсюджуються відповідні пакети оновлення. Комплекс має механізми, що дозволяють коректним чином здійснити інсталяцію пакетів оновлення.

Системний адміністратор може ініціювати виконання оновлення програмного забезпечення комплексу за наявності відповідних пакетів оновлення.

Проведення оновлень з використанням пакетів оновлень не викликає необхідності повторної інсталяції, і проводиться під контролем його КЗЗ. Після проведення оновлень є необхідним лише перезапуск програмного забезпечення серверного компоненту комплексу.

Дія цього експертного висновку розповсюджується на оновлене програмне забезпечення комплексу, яке має версію збірки 6.x (x – ціле невід'ємне число), має склад програмного забезпечення якого відповідає даним, наведеним в п. 6.2 цього документу, та яке виготовлено ТОВ «ФОСС-Он-лайн» протягом терміну його дії, з урахуванням умов, зазначених у розділі 8 до цього документу.

7.4.7 В рамках реалізації *функціональної послуги безпеки «ДВ-1»* комплекс забезпечує можливість відновлення роботи. Відновлення здійснюється системним адміністратором шляхом повторної інсталяції програмного забезпечення комплексу та відновлення необхідної інформації з резервної копії в порядку, наведеному в [5.3].

Відновлення після збоїв здійснюється в наступному обсязі:

– інформаційний зміст баз даних відновлюється з архівних копій, які регулярно з визначеною періодичністю створюються системним адміністратором налаштуваннями комплексу;

– файли програмного забезпечення комплексу та програмних комплексів, створених з його використанням, відновлюються шляхом переінсталяції з їх дистрибутивних носіїв; при цьому відновлене функціонування здійснюється з безпечного стану шляхом застосування раніше визначеної та реалізованої політики безпеки інформації.

Комплекс підтримує можливість створення резервних копій, розміщених як на локальних носіях даних ЕОМ, на якій він встановлений, так і на мережевих сховищах даних, до яких він може мати мережеве підключення.

Відновлення інформаційного змісту баз даних здійснюється у разі виходу з ладу апаратного або програмного забезпечення системи управління базами даних, збоїв в їх роботі, що спричинили втрату інформації в базах даних.

Відновлення програмного забезпечення комплексу здійснюється у разі виходу з ладу системного програмного або апаратного забезпечення ЕОМ, на яких воно було розгорнуто, що спричинило пошкодження програмних модулів та неможливість їх виконання [3.2, 5.3].

7.4.8 В рамках реалізації *функціональної послуги безпеки «НР-2»* комплекс забезпечує можливість реєстрації подій, які виконуються користувачами комплексу.

Для реєстрації операцій, що здійснюються користувачами в комплексі, використовується відповідний журнал реєстрації подій, до якого заносяться відомості про такі події [5.3]:

– запуск на виконання / завершення роботи компонент комплексу;

– вхід/вихід до комплексу відповідних користувачів;

– отримання користувачами комплексу доступу до відповідних об’єктів захисту;

– управління обліковими записами користувачів (ролями користувачів) комплексу та їх правами доступу;

– помилки, які виникають під час функціонування компонент комплексу.

Для реєстрації операцій, що здійснюються користувачами в комплексі використовується журнал реєстрації подій. Журнал реєстрації подій має наступні поля:

– об’єкт операції;
– ідентифікатор об’єкта;
– операція, що виконується над об’єктом;
– успішність виконання операції;
– ідентифікатор користувача, під яким здійснено вхід до комплексу;
– примітка (інша необхідна інформація).

В журналі реєстрації подій фіксується виконання всіх операцій, що визначаються класом об’єкта та для яких налаштований аудит в політиці безпеки. Кожна операція, що здійснюється з об’єктом, перевіряється та реєструється із занесенням результатів успішності (або неуспішності) перевірки доступності операції, із можливими додатковими коментарями.

Комплекс забезпечує захист журналу реєстрації подій від несанкціонованого доступу. Право перегляду журналу реєстрації подій має системний адміністратор.

7.4.9 В рамках реалізації *функціональних послуг безпеки «НИ-1», «НИ-2» та «НК-1»* комплекс забезпечує можливість однозначної ідентифікації та автентифікації адміністратора та користувачів.

Політика зовнішньої ідентифікації застосовується при реалізації механізмів ідентифікації та автентифікації з використанням поточного ідентифікатора користувача в операційній системі (домені).

Політика одиночної ідентифікації застосовується при реалізації механізмів ідентифікації та автентифікації з використанням пари атрибутів доступу «ідентифікатор і пароль».

Введення даних автентифікації користувачів здійснюється із забезпеченням неможливості їх перехоплення стороннім програмним забезпеченням. Управління даними облікових записів користувачів здійснюється адміністратором відповідно до [5.3].

7.4.10 В рамках реалізації *функціональної послуги безпеки «НО-1»* КЗЗ комплексу забезпечує виділення ролі системного адміністратора та ролі користувачів (оператори).

Системний адміністратор має право управління налаштуваннями комплексу. Користувачі мають право використовувати комплекс за призначенням для виконання покладених на них функціональних обов’язків.

Системний адміністратор має можливість створення будь-якої кількості ролей (груп) користувачів та налаштування для кожної з створених ролей правил управління доступом до інформаційних об’єктів.

Роль користувача визначається наступним способом [5.3]:

1) включенням користувача у групу користувачів, яка має певні повноваження;

2) присвоєнням обліковому запису групи користувачів, в яку включено користувача, певних повноважень з використанням механізму правил управління доступом.

Група користувачів комплексу є іменованою сукупністю облікових записів користувачів, яка дозволяє призначати повноваження і права доступу для групи користувачів, а не індивідуально для кожного користувача. КЗЗ комплексу дозволяє системному адміністратору створювати будь-які власні групи.

В комплексі за умовчанням передбачені вбудовані групи користувачів, які наведені у табл. 7.2.

КЗЗ комплексу надає можливість системному адміністратору керувати наступними функціональними компонентами безпеки [5.3]:

1) база даних облікових записів користувачів – дозволяє керувати атрибутами безпеки облікових записів користувачів і груп користувачів;

2) відкат – надає можливість керувати відкатом операцій із зміни технологічних даних комплексу;

3) модернізація – надає можливість здійснювати оновлення програмного забезпечення комплексу;

4) квоти – надає можливість управляти обмеженнями на ресурси, які виділяються користувачам.

Користувачі виступають в певній ролі тільки після того, як КЗЗ виконав процедури їх ідентифікації та автентифікації, визначені в п. 7.4.9.

Користувач, який успішно пройшов ідентифікацію та автентифікацію та авторизацію, може виконувати тільки дії, що дозволені для ролі, на яку він призначений.

7.4.11 В рамках реалізації *функціональних послуг безпеки «НЦ-1» та «НТ-2»* КЗЗ комплексу забезпечує контроль цілісності власного програмного забезпечення та перевірку працездатності (за рахунок перевірки цілісності відповідних програмних модулів) компонент при запуску їх на виконання або за відповідним запитом системного адміністратора (шляхом повторного перезапуску програмного забезпечення). КЗЗ комплексу забезпечує реалізацію наступних механізмів із забезпечення власного захисту:

- захисту при старті;
- контролю доступу до об'єктів;
- захисту програмних модулів (файлів).

Захист комплексу при старті базується на завантаженні програмних модулів під контролем КЗЗ. Комплекс контролює процес завантаження та ініціалізації та зупиняє виконання при виникненні порушення цілісності програмних модулів або інших помилок, що можуть призвести до зниження рівня захисту інформації.

Механізм доступу процесів до об'єктів заснований на використанні дескрипторів об'єктів. Одержання дескриптора об’єкта процесом, якій запитує доступ до об’єкта, як правило відбувається при відкритті або створенні об'єкта. КЗЗ забезпечує підтвердження доступу перед створенням нового дескриптора

об’єкта. Дескриптори можуть бути також успадковані від батьківських процесів або прямо скопійовані (при наявності відповідних прав доступу) з іншого процесу.

Захист програмних модулів (файлів) здійснюється шляхом контролю їх цілісності. Для реалізації контролю цілісності КЗЗ реалізує механізм підрахунку контрольних сум для модулів, що використовуються комплексом. Для контролю цілісності файлів обчислюються та зберігаються відповідні контрольні суми.

При запуску для кожного модуля, що входить до складу КЗЗ комплексу, перевіряється співпадіння контрольної суми модуля із еталонним значенням. При неспівпадінні контрольних сум, або при відсутності модуля видається відповідне повідомлення про порушення контролю цілісності із зазначенням переліку файлів, цілісність яких порушена. Комплекс при цьому не запускається.

В процесі виконання комплексу системним адміністратором шляхом використання спеціальної утиліти надається можливість додатково перевірити цілісність окремих інформаційних баз даних комплексу.

При експлуатації комплексу повинні бути дотримані описані в розділі 8 цього документу обмеження, які дозволяють гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ комплексу і всі запити на доступ до захищених об'єктів контролюються цим КЗЗ.

7.4.12 В рамках реалізації *функціональної послуги безпеки «НА-1»* КЗЗ комплексу забезпечує автентифікацію користувачів, які формують та відправляють електронні поштові повідомлень; для накладання електронного цифрового підпису використовується відповідний особистий ключ особи – відправника електронного поштового повідомлення; для перевірки електронного цифрового підпису використовується його сертифікат відкритого ключа, створений відповідним центром сертифікації ключів [3.2].

Для однозначного підтвердження приналежності електронних документів їх відправникам використовуються сертифікати відкритих ключів відправника та центру сертифікації ключів, який сформував відповідні сертифікати.

Для реалізації послуги до складу комплексу засіб криптографічного захисту інформації «Бібліотека криптографічних перетворень «UALib» (UA.АЭЛА.0000-01 90 01), який поє позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації (від 18.02.2014 № 05/02/02-549).

Для забезпечення функціонування комплексу можуть використовуватись сертифікати відкритих ключів, які формуються зареєстрованими або акредитованими у відповідності до законодавства України центром сертифікації ключів. При використанні сертифікатів відкритих ключів, що формуються зареєстрованими центрами сертифікації ключів, функціональна послуга «НА» реалізується на рівні «НА-1». В разі використання посилених сертифікатів відкритих ключів, які формуються акредитованими центрами сертифікації ключів, при використанні комплексу у відповідних інформаційно-телекомунікаційних системах рівень реалізації функціональної послуги «НА» може бути збільшений до «НА-2».

7.4.13 В рамках реалізації *функціональної послуги безпеки «НП-1»* КЗЗ комплексу забезпечує автентифікацію користувачів, які отримують електронні документи; послуга стосується квитанцій (електронних підтверджень) про отримання електронних поштових повідомлень їх адресатами в комплексі; для накладання електронного цифрового підпису на квітанції (підтвердженні) використовується відповідний особистий ключ особи – отримувача електронного документу; для перевірки електронного цифрового підпису використовується його сертифікат відкритого ключа, створений відповідним центром сертифікації ключів [2 (п. 5.4.17)].

Для однозначного підтвердження приналежності електронних документів їх відправникам використовуються сертифікати відкритих ключів відправника та центру сертифікації ключів, який сформував відповідні сертифікати.

Для реалізації послуги до складу комплексу засіб криптографічного захисту інформації «Бібліотека криптографічних перетворень «UALib» (UA.АЭЛА.0000-01 90 01), який поє позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації (від 18.02.2014 № 05/02/02-549).

Для забезпечення функціонування комплексу можуть використовуватись сертифікати відкритих ключів, які формуються зареєстрованими або акредитованими у відповідності до законодавства України центром сертифікації ключів. При використанні сертифікатів відкритих ключів, що формуються зареєстрованими центрами сертифікації ключів, функціональна послуга «НП» реалізується на рівні «НП-1». В разі використання посилених сертифікатів відкритих ключів, які формуються акредитованими центрами сертифікації ключів, при використанні комплексу у відповідних інформаційно-телекомунікаційних системах рівень реалізації функціональної послуги «НП» може бути збільшений до «НП-2».

8. СФЕРА ВИКОРИСТАННЯ (ВИМОГИ ДО УМОВ ЕКСПЛУАТАЦІЇ) ОБ'ЄКТА ЕКСПЕРТИЗИ

Використання комплексу можливе лише за умови дотримання вимог та положень експлуатаційної документації, а також наступних положень:

– відсутність потенційно небезпечних програмних засобів на ЕОМ, на яких застосовується комплекс, до яких належать:

- засоби прямого доступу до інформації серверів;
- засоби розробки, відлагодження та тестування програмного забезпечення;
- засоби аналізу змісту оперативної пам’яті;
- засоби аналізу виконуємого коду програмного забезпечення;
- засоби злому комп’ютерних систем;

– заборона локального входу на сервери користувачів, які не є системними адміністраторами комплексу;

– фізична охорона серверів, на яких застосовується комплекс, зовнішніх пристроїв (накопичувачів), носіїв інформації та фізичних ліній зв’язку; фізична охорона повинна передбачати контроль доступу сторонніх осіб до

приміщення, де знаходяться об’єкти охорони, наявність надійних перешкод для несанкціонованого проникнення до приміщень та сховищ носіїв інформації, особливо в неробочий час;

– обмеження доступу користувачів до пристроїв введення інформації серверів, на яких застосовується комплекс, з зовнішніх джерел; в разі необхідності, введення інформації повинно здійснюватись під контролем системного адміністратора комплексу;

– дотримуються вимоги щодо умов застосування комплексу, наведені в технічному завданні [1, 2] та експлуатаційній документації [5];

– налаштування операційної системи та системи управління базами даних, спільно з якими використовується комплекс, відповідають вимогам експлуатаційної документації на комплекс [5.2];

– забезпечується надійне збереження атрибутів доступу користувачів комплексу, що унеможливлює несанкціонований доступ до них;

– при використанні комплексу для обробки службової інформації для забезпечення конфіденційності інформації, що передається через незахищене середовище, повинні використовуватись додаткові засоби криптографічного захисту інформації, що відповідають вимогам законодавства з питань криптографічного захисту службової інформації;

– дія експертного висновку розповсюджується на зразки комплексу, які мають версію 6.x (x – ціле невід’ємне число), мають склад програмного забезпечення якого відповідає даним, наведеним в п. 6.2 цього документу, та які виготовлені ТОВ «ФОСС-ОН-лайн» протягом терміну його дії, з урахуванням умов, зазначених у розділі 8 до цього документу.

9. ТЕРМІН ДІЇ ЕКСПЕРТНОГО ВИСНОВКУ

Термін дії висновку становить 3 роки за умови виконання вимог розділу 8 цього висновку.