НОРМАТИВНИЙ ДОКУМЕНТ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

Департамент спеціальних телекомунікаційних систем та захисту інформації
Служби безпеки України

Київ 2016

Передмова

РОЗРОБЛЕНО Товариством з обмеженою відповідальністю "Інститут комп'ютерних технологій".

ВНЕСЕНО Департаментом технічного захисту інформації Адміністрації Держспецзв’язку.

ВВЕДЕНО ВПЕРШЕ.

НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Затверджено
наказом Департаменту спеціальних
телекомунікаційних систем та захисту інформації
Служби безпеки України

від “ 27 ” квітня 2016 року № 293

Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

НД ТЗІ 2.6-002-2015

ДСТСЗІ СБ України

Київ

Зміст

ПОРЯДОК ЗІСТАВЛЕННЯ ФУНКЦІОНАЛЬНИХ КОМПОНЕНТІВ БЕЗПЕКИ, ВИЗНАЧЕНИХ ISO/IEC 15408, З ВИМОГАМИ НД ТЗІ 2.5-004-99

Чинний від 2016-24-07

1 Галузь використання

Цей нормативний документ визначає відповідність між вимогами, встановленими стандартом ISO/IEC 15408 щодо функціональних компонентів безпеки, та вимогами, встановленими НД ТЗІ 2.5-004-99 щодо функціональних послуг безпеки (ФПБ), а також містить опис загальних положень та порядку проведення робіт із зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, які виконуються в процесі створення засобів технічного захисту інформації (ЗТЗІ) від несанкціонованого доступу (НСД), захищених від НСД компонентів обчислювальної системи та захищених інформаційно-телекомунікаційних систем (ІТС) або в процесі проведення державної експертизи в сфері технічного захисту інформації (ТЗІ).

НД призначено для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, а також юридичних та фізичних осіб усіх форм власності, які виконують роботи зі створення ЗТЗІ від НСД, захищених від НСД компонентів обчислювальної системи та комплексних систем захисту інформації (КСЗІ) в ІТС, а також проведення їх державної експертизи на відповідність вимогам нормативних документів (НД) системи ТЗІ в Україні.

2 Нормативні посилання

У цьому НД наведено посилання на такі нормативні документи:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни і визначення.

Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087.

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах 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.

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

ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 1. Вступ і загальна модель).

ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components (Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 2. Функціональні компоненти безпеки).

ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components (Інформаційні технології. Методи захисту. Критерії оцінювання ІТ-безпеки. Частина 3. Компоненти довіри до безпеки).

3 Визначення

У цьому НД використано терміни та визначення, встановлені ДСТУ 3396.2-97 та НД ТЗІ 1.1-003-99.

Крім цього, використано такі терміни та визначення.

Завдання з безпеки – сукупність вимог безпеки та специфікацій, призначена для використання як основи для оцінювання конкретного об’єкта оцінювання.

Засіб технічного захисту інформації від несанкціонованого доступу – програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт виробництва, має необхідну проектну та/або експлуатаційну документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз несанкціонованого доступу для інформації, оброблюваної в інформаційно-телекомунікаційній системі.

Захищений від несанкціонованого доступу компонент обчислювальної системи – програмний, апаратний або програмно-апаратний засіб, у якому додатково до основного призначення передбачено функції захисту інформації від загроз несанкціонованого доступу.

Інформаційна система – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які в процесі оброблення інформації діють як єдине ціле.

Об'єкт експертизи – засіб технічного захисту інформації від несанкціонованого доступу або захищений від несанкціонованого доступу компонент обчислювальної системи, стосовно якого проводиться експертиза в сфері технічного захисту інформації.

Об'єкт оцінювання – продукт інформаційних технологій або система із настановами адміністратора та користувача, що підлягають оцінюванню (сертифікації) на відповідність ISO/IEC 15408.

Область дії функцій безпеки об’єкта оцінювання – сукупність можливих взаємодій з об’єктом оцінювання або у його межах, що підпорядковані правилам політики безпеки об’єкта оцінювання.

Оцінювання – визначення міри відповідності характеристик об'єкта заданим критеріям та вимогам.

Політика безпеки об’єкта оцінювання – сукупність правил, що регулюють керування активами, їх захист та розподіл у межах об’єкта оцінювання.

Політика функції безпеки – політика безпеки, що реалізується функцією безпеки.

Профіль захисту – незалежна від реалізації сукупність вимог безпеки для певної категорії об’єктів оцінювання, що відповідає певним вимогам споживача.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Функція безпеки – функціональні можливості частини або частин об’єкта оцінювання, які забезпечують виконання підмножини взаємозв’язаних правил політики безпеки об’єкта оцінювання.

Функції безпеки об’єкта оцінювання – сукупність усіх функцій об’єкта оцінювання, спрямованих на реалізацію політики безпеки об’єкта оцінювання.

Функціональна послуга безпеки – сукупність функцій, що визначені відповідно до вимог НД ТЗІ 2.5-004-99 та забезпечують захист інформації від певної загрози або від множини загроз.

Функціональна специфікація об'єкта експертизи – упорядкований перелік реалізованих в об’єкті експертизи функціональних послуг безпеки згідно з НД ТЗІ 2.5-004-99 разом з описом їх політики або іншим чином визначений перелік функцій захисту з описом їх політик згідно з вимогами міжнародних стандартів.

4 Позначення та скорочення

У цьому НД використано такі позначення та скорочення:

ЗБ – завдання з безпеки;
ЗТЗІ – засіб технічного захисту інформації;
ІТ – інформаційна технологія;
ІТС – інформаційно-телекомунікаційна система;
КЗЗ – комплекс засобів захисту;
КСЗІ – комплексна система захисту інформації;
НД – нормативний документ;
НСД – несанкціонований доступ;
ОВЗ – особа, що виконує зіставлення;
ОДФ – область дії функцій безпеки об’єкта оцінювання;
ОЕ – об'єкт експертизи;
ОО – об’єкт оцінювання;

ПБО – політика безпеки об’єкта оцінювання;
ПЗ – профіль захисту;
ПФБ – політика функцій безпеки;
ТЗІ – технічний захист інформації;
ФБ – функція безпеки;
ФБО – функції безпеки об’єкта оцінювання;
ФПБ – функціональна послуга безпеки.

5 Загальні положення щодо зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

5.1 Відповідно до положень НД ТЗІ 1.1-002-99 у проблемі захисту від НСД інформації, оброблюваної в ІТС, виокремлюються два напрями:

- забезпечення захищеності інформації у функціонуючих та/або створюваних ІТС;
- створення ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи поза конкретним середовищем експлуатації.

При цьому як у першому, так і в другому випадку доцільним, а якщо в ІТС планується оброблення інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформації, яка становить державну таємницю або віднесена до державних інформаційних ресурсів), то обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів і заходів захисту встановленим вимогам і нормам. Результатами проведеного оцінювання має бути відповідний висновок, на підставі якого власники ІТС та оброблюваних у них інформаційних ресурсів можуть приймати рішення щодо прийнятності та достатності вжитих заходів і реалізованих засобів.

5.2 Згідно з вимогами Положення про державну експертизу в сфері технічного захисту інформації, на підставі якого в Україні функціонує система оцінювання відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам, об'єктами експертизи (ОЕ) можуть бути як КСЗІ, які є невід'ємною складовою ІТС, так і окремі ЗТЗІ від НСД, у тому числі захищені від НСД компоненти обчислювальної системи.

5.3 Відповідно до положень НД ТЗІ 2.6-001-11 обсяг і тривалість експертних робіт із державної експертизи КСЗІ в ІТС суттєво скорочуються у випадку, якщо у складі комплексу засобів захисту (КЗЗ) КСЗІ використовуються ЗТЗІ від НСД або захищені від НСД компоненти обчислюваної системи, стосовно яких уже було проведено державну експертизу в сфері ТЗІ та наявні чинні експертні висновки, що містять її результати та відображають відповідність цих засобів вимогам НД ТЗІ. Наявність і можливість використання таких ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) дозволяють також суттєво скоротити тривалість робіт зі створення КСЗІ.

5.4 На цей час поширеною у світі є практика оцінювання (сертифікації) ЗТЗІ від НСД та захищених від НСД компонентів обчислюваної системи на відповідність вимогам Єдиних критеріїв оцінки безпеки інформаційних

технологій, встановлених міжнародним стандартом ISO/IEC 15408. Такі засоби та компоненти обчислювальної системи широко використовуються в Україні при побудові ІТС різного призначення. З метою спрощення процедури експертних робіт при проведенні експертизи цих засобів та компонентів (у вигляді як окремих ОЕ, так і складових КЗЗ КСЗІ) експерти повинні мати можливість визначення множини та політики ФПБ, що реалізуються відповідним засобом (компонентом), не тільки шляхом дослідження ОЕ у порядку, визначеному НД ТЗІ 2.7-009-09, а і шляхом зіставлення наявних результатів оцінювання функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. З іншого боку, розробники ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) та захищених ІТС (КСЗІ в ІТС) повинні мати можливість визначення відповідності між вимогами НД ТЗІ 2.5-004-99 та вимогами ISO/IEC 15408, що дозволить суттєво спростити та прискорити процес підготовки створюваних ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) до оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408 або процес аналізу та прийняття рішення щодо можливого використання певного засобу (компонента обчислювальної системи) у складі захищеної ІТС (у складі КЗЗ КСЗІ).

5.5 Зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 може проводитись під час виконання робіт:

- з оцінювання ФПБ, які виконуються в процесі проведення державної експертизи в сфері ТЗІ, з метою визначення та підтвердження факту реалізації в ОЕ певної множини ФПБ, яка однозначно відповідає переліку функціональних компонентів безпеки, факт реалізації яких у відповідному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи, компоненті КЗЗ КСЗІ) підтверджено за результатами оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;
- зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою підготовки відповідних матеріалів (завдання з безпеки (ЗБ), опис об’єкта оцінювання (ОО) тощо), необхідних для оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;
- зі створення захищених ІТС (КСЗІ в ІТС) під час проведення аналізу можливості включення до складу відповідних ІТС (КЗЗ створюваних КСЗІ) певних ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи, для яких наявні результати оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408, але немає (на момент проведення аналізу) результатів державної експертизи в сфері ТЗІ;
- зі створення захищених ІТС (КСЗІ в ІТС) або ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою формулювання вимог до створюваних систем або засобів у термінах НД ТЗІ 2.5-004-99 з використанням існуючих профілів захисту (ПЗ) для аналогічних засобів або систем, визначених відповідно до вимог ISO/IEC 15408;
- в інших можливих випадках.

5.6 Зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується під час робіт з оцінювання ФПБ, проводиться особами, що виконують зіставлення (ОВЗ) – експертами на етапі попереднього аналізу ОЕ.

5.6.1 З урахуванням загальних вимог щодо порядку проведення робіт на етапі попереднього аналізу ОЕ, встановлених НД ТЗІ 2.6-001-11, зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 під час оцінювання ФПБ передбачає виконання на підставі вмісту наданих замовником експертизи вхідних матеріалів, у складі яких мають бути надані результати оцінювання ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність вимогам ISO/IEC 15408, зіставлення реалізованих у ОЕ функціональних компонентів безпеки із вимогами НД ТЗІ 2.5-004-99 щодо ФПБ та документування отриманих результатів.

5.6.2 Метою виконання такого зіставлення є:

- визначення (ідентифікація) множини ФПБ, що реалізовані в оцінюваному ОЕ, їх рівнів та політики, тобто визначення функціональної специфікації ОЕ згідно з НД ТЗІ 2.5-004-99;

- документування отриманих результатів та прийняття рішення щодо проведення подальших етапів експертних робіт або щодо їх припинення.

5.6.3 Визначення функціональної специфікації ОЕ згідно з НД ТЗІ 2.5-004-99 здійснюється ОВЗ шляхом виконання прямого зіставлення реалізованих у ОЕ функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 щодо ФПБ у порядку, наведеному у розділі 6.

Примітка. Наявність можливості визначення функціональної специфікації ОЕ згідно з НД ТЗІ 2.5-004-99 шляхом зіставлення реалізованих у ОЕ функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 щодо ФПБ не означає, що роботи з ідентифікації певних або всіх ФПБ, уточнення їх рівнів і політики не можуть бути виконані шляхом дослідження відповідного ОЕ у порядку, визначеному НД ТЗІ 2.7-009-09.

5.6.4 З урахуванням положень НД ТЗІ 2.7-009-09 визначена за результатами виконаного зіставлення функціональна специфікація ОЕ має бути перевірена на її формальну коректність шляхом:

- перевірки наявності у визначеній функціональній специфікації ОЕ ФПБ "Цілісність КЗЗ" рівня НЦ-1 або вище;

- перевірки наявності у визначеній функціональній специфікації ОЕ ФПБ певного рівня, наявність яких, згідно з вимогами НД ТЗІ 2.5-004-99 є необхідною умовою для реалізації інших ФПБ.

Якщо ФПБ «Цілісність КЗЗ» рівня НЦ-1 або вище відсутня, має бути прийнято рішення про припинення подальших експертних робіт. Якщо у визначеній функціональній специфікації ОЕ немає ФПБ певного рівня, наявність яких є необхідною умовою для реалізації інших ФПБ, із функціональної специфікації ОЕ мають бути вилучені ФПБ, необхідних умов реалізації яких немає.

5.6.5 Результати зіставлення, виконаного під час робіт із оцінювання ФПБ, документуються у порядку, визначеному у розділі 11.

5.7 Зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується під час робіт зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою підготовки матеріалів, необхідних для оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408, проводиться ОВЗ – розробниками відповідних засобів.

5.7.1 Зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 під час робіт зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) передбачає виконання аналізу проектної документації, що містить опис переліку та політики реалізованих ФПБ, з подальшим виконанням зіставлення реалізованих ФПБ із вимогами ISO/IEC 15408 щодо функціональних компонентів безпеки та документування отриманих результатів.

5.7.2 Метою аналізу проектної документації є чітке визначення ОВЗ переліку, політики та порядку реалізації у створюваному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи) певних ФПБ відповідних рівнів згідно з НД ТЗІ 2.5-004-99, вимоги щодо яких мають бути зіставлені з вимогами щодо функціональних компонентів безпеки згідно з ISO/IEC 15408. При цьому з метою спрощення виконання зіставлення доцільним є формулювання опису порядку реалізації певних ФПБ у вигляді, максимально наближеному до вимог, встановлених НД ТЗІ 2.5-004-99, із визначенням для кожної ФПБ користувачів, процесів та об’єктів різного типа, а також правил, згідно з якими функціонують механізми, що реалізують відповідні ФПБ.

Результатом проведеного аналізу має бути або сформульований опис порядку реалізації ФПБ, або чітко визначені складові проектної документації, що містять відповідні відомості.

5.7.3 Зіставлення реалізованих у створюваному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи) ФПБ з вимогами ISO/IEC 15408 щодо функціональних компонентів безпеки здійснюється ОВЗ шляхом виконання зворотного зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 щодо ФПБ у порядку, наведеному у розділі 6.

5.7.4 Результатом виконаного зіставлення мають бути документовані у довільній формі відомості щодо функціональних компонентів безпеки згідно з ISO/IEC 15408, які за результатами зіставлення визнані такими, що реалізуються створюваним ЗТЗІ від НСД (захищеним від НСД компонентом обчислювальної системи). Обсяг зазначених відомостей має бути достатнім для підготовки відповідних матеріалів (ЗБ, опис ОО тощо), необхідних для оцінювання (сертифікації) створюваного ЗТЗІ від НСД на відповідність вимогам ISO/IEC 15408.

5.8 Зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується в ході робіт зі створення захищених ІТС (КСЗІ в ІТС) під час проведення аналізу можливості включення до складу відповідних ІТС (КЗЗ створюваних КСЗІ)

певних ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи, проводиться ОВЗ – розробниками відповідних систем. Метою відповідного зіставлення є визначення множини ФПБ, які можуть бути реалізовані певним ЗТЗІ від НСД (захищеним від НСД компонентом обчислювальної системи) у випадку його використання у складі відповідної захищеної ІТС (КЗЗ створюваної КСЗІ). Зіставлення має проводитись аналогічно до того, як це виконується під час робіт із оцінювання ФПБ, шляхом виконання дій, зазначених у пп. 5.6.3, 5.6.4. Після аналізу результатів зіставлення, отриманих для різних ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи), ОВЗ – розробником системи може бути прийнято рішення щодо доцільності або недоцільності включення певного засобу до складу створюваної ІТС (КСЗІ в ІТС) з метою виконання певних функцій із захисту інформації.

5.9 Зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99, яке виконується під час робіт зі створення захищених ІТС (КСЗІ в ІТС) або ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою формулювання вимог до створюваних систем або засобів у термінах НД ТЗІ 2.5-004-99, проводиться ОВЗ – розробниками відповідних систем або засобів. Метою відповідного зіставлення є визначення функціональних специфікацій створюваних засобів або систем згідно з НД ТЗІ 2.5-004-99 у вигляді вимог щодо множини ФПБ, які мають бути реалізовані, та вимог щодо їх політики на основі існуючих ПЗ для аналогічних засобів або систем, визначених відповідно до вимог ISO/IEC 15408. Зіставлення має проводитись аналогічно до того, як це виконується під час робіт із оцінювання ФПБ, шляхом виконання дій, зазначених у пп. 5.6.3, 5.6.4. Вимоги щодо функціональних специфікацій створюваних засобів або систем формулюються ОВЗ на основі отриманих результатів зіставлення.

5.10 В інших випадках зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 може проводитись шляхом виконання прямого або зворотного зіставлення у порядку, наведеному у розділі 6.

6 Порядок виконання зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

6.1 Пряме зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 проводиться під час виконання робіт:

- з оцінювання ФПБ, які виконуються в процесі проведення державної експертизи в сфері ТЗІ, з метою визначення та підтвердження факту реалізації в ОЕ певної множини ФПБ, яка однозначно відповідає переліку функціональних компонентів безпеки, факт реалізації яких у відповідному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи, компоненті КЗЗ КСЗІ) підтверджено за результатами оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;

- зі створення захищених ІТС (КСЗІ в ІТС) під час проведення аналізу можливості включення до складу відповідних ІТС (КЗЗ створюваних КСЗІ) певних ЗТЗІ від НСД або захищених від НСД компонентів обчислювальної системи, для яких наявні результати оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408, але немає (на момент проведення аналізу) результатів державної експертизи в сфері ТЗІ;

- зі створення захищених ІТС (КСЗІ в ІТС) або ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою формулювання вимог до створюваних систем або засобів у термінах НД ТЗІ 2.5-004-99 з використанням існуючих ПЗ, визначених відповідно до вимог ISO/IEC 15408;

- в інших аналогічних випадках.

6.2 Пряме зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 передбачає виконання зіставлення функціональних компонентів безпеки згідно з ISO/IEC 15408, реалізованих у відповідному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи) або визначених у відповідному ПЗ, з вимогами критеріїв конфіденційності, цілісності, доступності та спостережності, встановленими НД ТЗІ 2.5-004-99, з метою визначення переліку відповідних ФПБ, які відповідають зазначеним функціональним компонентам безпеки, їх рівнів та політики.

6.3 Зіставлення функціональних компонентів безпеки згідно з ISO/IEC 15408, реалізованих у певному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи) або визначених у певному ПЗ, з вимогами критеріїв конфіденційності, цілісності, доступності та спостережності, встановленими НД ТЗІ 2.5-004-99, з метою визначення переліку відповідних ФПБ, їх рівнів та політики виконується у такому порядку.

6.3.1 На підставі вмісту матеріалів щодо результатів оцінювання (сертифікації) відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність вимогам ISO/IEC 15408 (ЗБ, опис ОО, звіт за результатами оцінювання тощо) або на підставі вмісту опису відповідного ПЗ визначається перелік усіх функціональних компонентів безпеки та усіх їх функціональних елементів, які мають бути зіставлені з вимогами НД ТЗІ 2.5-004-99.

6.3.2 У визначеному за результатами виконання пп. 6.3.1 переліку функціональних елементів функціональних компонентів безпеки на підставі відомостей, наведених у колонках 3 таблиць 7.1 - 10.9, визначається наявність певних груп функціональних елементів, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99, наведені у колонках 2, щодо певних ФПБ певних рівнів, зазначених у колонках 1 відповідних таблиць.

Примітка. З метою спрощення визначення груп функціональних елементів, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо певних ФПБ певних рівнів, рекомендується користуватися таблицею А.1 Додатка А.

6.3.3 Для кожної групи функціональних елементів, визначеної за результатами виконання пп. 6.3.2, перевіряється факт дотримання умов задоволення функціональними елементами, що входять у відповідну групу, вимог НД ТЗІ 2.5-004-99 щодо певної ФПБ певного рівня, наведених у колонках 4 відповідних таблиць.

6.3.4 У випадку встановлення факту дотримання умов задоволення функціональними елементами, що входять у певну групу, вимог НД ТЗІ 2.5-004-99 щодо певної ФПБ певного рівня, на підставі вмісту матеріалів щодо результатів оцінювання (сертифікації) відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність вимогам ISO/IEC 15408 (ЗБ, опис ОО, звіт за результатами оцінювання тощо) або на підставі вмісту опису відповідного ПЗ та з урахуванням результатів перевірки дотримання умов задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99 щодо відповідної ФПБ відповідного рівня визначаються:

- перелік користувачів, процесів та об’єктів різного типу, що мають відношення до політики відповідної ФПБ;

- політика, механізми і засоби реалізації відповідної ФПБ.

Примітка. Якщо за результатами виконання пп. 6.3.4 для певної ФПБ встановлено, що при її реалізації використовуються механізми та засоби криптографічного захисту інформації, ці механізми та засоби мають відповідати вимогам нормативних документів системи криптографічного захисту інформації в Україні.

6.3.5 Характеристики ФПБ (рівень ФПБ, перелік об’єктів, політика, механізми і засоби реалізації), для яких встановлено факти задоволення певними групами функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимог НД ТЗІ 2.5-004-99 щодо відповідних ФПБ відповідних рівнів, документуються, відповідні ФПБ долучаються до визначеного за результатами зіставлення переліку ФПБ.

6.4 Зворотне зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 проводиться:

- під час робіт зі створення ЗТЗІ від НСД (захищених від НСД компонентів обчислювальної системи) з метою підготовки відповідних матеріалів (ЗБ, опис ОО тощо), необхідних для оцінювання (сертифікації) на відповідність вимогам ISO/IEC 15408;

- в інших аналогічних випадках.

6.5 Зворотне зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 передбачає виконання зіставлення характеристик функціональних послуг забезпечення конфіденційності, цілісності, доступності та спостережності згідно з НД ТЗІ 2.5-004-99, реалізованих у відповідному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи), з вимогами до функціональних компонентів безпеки згідно з ISO/IEC 15408, з метою визначення переліку функціональних компонентів безпеки та їх функціональних елементів, які відповідають реалізованим функціональним послугам.

6.6 Зіставлення характеристик функціональних послуг забезпечення конфіденційності, цілісності, доступності та спостережності згідно з НД ТЗІ 2.5-004-99, реалізованих у певному ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи), з вимогами до функціональних компонентів безпеки згідно з ISO/IEC 15408 виконується у такому порядку.

6.6.1 На підставі матеріалів, що входять до складу проектної документації відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) (технічне завдання, матеріали ескізного, технічного та робочого проектів тощо), у яких наведено опис політики та порядку реалізації ФПБ, визначається перелік усіх ФПБ, які мають бути зіставлені з вимогами ISO/IEC 15408.

6.6.2 Для кожної ФПБ, що міститься у визначеному за результатами виконання пп. 6.6.1 переліку ФПБ, на підставі відомостей, наведених у колонках 1 - 2 таблиць 7.1 - 10.9, визначаються вимоги щодо груп функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408, наведені у колонках 3 відповідних таблиць, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо реалізації політики відповідної ФПБ відповідного рівня.

6.6.3 Для функціональних елементів, що входять до складу кожної визначеної за результатами виконання пп. 6.6.2, групи функціональних елементів, на підставі вмісту матеріалів, у яких наведено опис політики та порядку реалізації ФПБ, зазначених у пп. 6.6.1, та з урахуванням умов задоволення функціональними елементами, що входять у відповідні групи, вимог НД ТЗІ 2.5-004-99 щодо певних ФПБ певних рівнів, наведених у колонках 4 відповідних таблиць, визначаються їхні характеристики (список суб’єктів, список об’єктів, список операцій тощо).

6.6.4 З урахуванням положень ISO/IEC 15408 формулюються вимоги та визначаються характеристики решти функціональних елементів, які разом із визначеними при виконанні пп. 6.6.2 входять до складу відповідних функціональних компонентів безпеки.

6.6.5 Для всіх функціональних елементів, які входять до складу визначених при виконанні пп. 6.6.2 - 6.6.4 функціональних компонентів безпеки, перевіряється дотримання умов ISO/IEC 15408 щодо їх залежності від інших функціональних елементів. Функціональні компоненти безпеки, для функціональних елементів яких дотримання умов ISO/IEC 15408 щодо їх залежності від інших функціональних елементів не забезпечено, вилучаються із переліку, визначеного при виконанні пп. 6.6.2 - 6.6.4.

6.6.6 Характеристики функціональних компонентів безпеки згідно з ISO/IEC 15408, які складаються із характеристик усіх їх функціональних елементів, визначених при виконанні пп. 6.6.2 - 6.6.5 та задовольняють вимоги НД ТЗІ 2.5-004-99 щодо всіх ФПБ, які реалізовані у ЗТЗІ від НСД (захищеному від НСД компоненті обчислювальної системи), документуються, відповідні функціональні компоненти безпеки долучаються до визначеного за результатами зіставлення ПЗ.

7 Відомості щодо відповідності функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам критеріїв конфіденційності, встановленим НД ТЗІ 2.5-004-99

У підрозділах цього розділу у таблицях 7.1 – 7.5 викладено відомості щодо відповідності функціональних елементів функціональних компонентів безпеки відповідних функціональних класів безпеки, встановлених стандартом ISO/IEC 15408, вимогам критеріїв конфіденційності, встановленим НД ТЗІ 2.5-004-99, для різних ФПБ. Відомості викладено у табличному вигляді, окремо для кожної ФПБ та її рівнів, визначених НД ТЗІ 2.5-004-99, із зазначенням у кожній таблиці: рівня ФПБ; вимог НД ТЗІ 2.5-004-99 щодо політики відповідної ФПБ відповідного рівня; вимог стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких у процесі виконання зіставлення функціональних компонентів безпеки згідно з ISO/IEC 15408, реалізованих у певному ЗТЗІ від НСД, з вимогами НД ТЗІ 2.5-004-99 можна приймати рішення про те, що певна сукупність функціональних елементів функціональних компонентів безпеки задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.

7.1 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ «Довірча конфіденційність»

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ «Довірча конфіденційність» наведено у таблиці 7.1.

Таблиця 7.1

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
1	2	3	4
КД-1	Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: Функції безпеки об’єкта (ФБО) повинні реалізовувати [призначення: політика функцій безпеки (ПФБ) керування доступом] для [призначення: список суб’єктів, об’єктів та операцій суб’єктів на об’єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів, інформації та операцій переміщення керованої інформації до керованих суб’єктів, на які поширюється ПФБ, та від них]	У списку суб’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів та всі типи процесів, на які поширюється політика ФПБ. У списку об’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від об’єктів відповідних типів до процесів відповідних типів (операції читання інформації), на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об’єктів, що ґрунтується на [призначення: список суб’єктів та об’єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб’єкта на керованому об’єкті: [призначення: правила керування доступом керованих суб’єктів до керованих об’єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб’єктів до об’єктів, що ґрунтується на таких додаткових	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від об’єктів відповідних типів до процесів відповідних типів (операціями читання інформації). У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів

		правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від об'єктів відповідних типів до процесів відповідних типів (операціями читання інформації), на які поширюється політика ФПБ
	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захи-щеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об'єктів усіх типів, на які поширюється політика ФПБ, з урахуванням належності об'єктів до доменів певних користувачів керувати операціями переміщення інформації від об'єктів відповідних типів до процесів відповідних типів (операціями читання інформації). ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу,

			асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни *атрибутів безпеки* об'єктів відповідних типів, що належать його домену
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об'єктів, на які поширюється політика ФПБ, що відповідають об'єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі області дії функцій (ОДФ). FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об'єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об'єктів, на які поширюється політика ФПБ

		реалізовувати [призначення: політики функцій безпеки (ФБ) керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
КД-2 16	Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб’єктів, об’єктів та операцій суб’єктів на об’єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів, інформації та операцій переміщення керованої інформації до керованих суб’єктів, на які поширюється ПФБ, та від них]	У списку суб’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів, на які поширюється політика ФПБ. У списку об’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об’єктів та процесів, на які поширюється політика ФПБ. У списку операцій функціональних елементів

			FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від об’єктів до користувачів відповідних типів (операції читання інформації) та всі операції ініціювання процесів, на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об’єктів, що ґрунтується на [призначення: список суб’єктів та об’єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб’єкта на керованому об’єкті: [призначення: правила керування доступом керованих суб’єктів до керованих об’єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб’єктів до об’єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб’єктів до об’єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб’єкта та інформації: [призначення: список суб’єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.1.2: ФБО повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб’єктів та інформації (для кожної операції)]. FDP_IFF.1.5: ФБО повинні явно дозволяти інформаційний потік, що	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути користувачів, процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від об’єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від об’єктів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів, на які поширюється політика ФПБ

		ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	
	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: *ФБО повинні реалізовувати [призначення:* ПФБ керування доступом, ПФБ керування інформаційними потоками], *що надає можливість [вибір:* змінювати значення за замовченням, запитувати, модифікувати, видаляти *[призначення:* інші операції]] *атрибути безпеки [призначення:* список атрибутів безпеки] *тільки [призначення:* уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об’єктів та процесів усіх типів, на які поширюється політика ФПБ, з урахуванням належності об’єктів та процесів до доменів певних користувачів керувати операціями переміщення інформації від об’єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни *атрибутів безпеки* об’єктів та процесів відповідних типів, що належать його домену
	КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта		
	КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів

		за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	об’єктів та процесів, на які поширюється політика ФПБ, що відповідають об’єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
КД-3	Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів та об'єктів] та всіх операцій суб'єктів на об'єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб'єкта з ОДФ на будь-якому об'єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку суб'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів, які підтримуються ОЕ. У списку об'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об'єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від об'єктів відповідних типів до користувачів відповідних типів (операції читання інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та

	користувача і захищеного об'єкта	для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах:	об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від об'єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 усіма операціями переміщення інформації від об'єктів до користувачів відповідних типів (операціями читання інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ

		[призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	
22	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: *ФБО повинні реалізовувати [призначення:* ПФБ керування доступом, ПФБ керування	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об'єктів та процесів усіх типів, які підтримуються ОЕ, з урахуванням належності об'єктів та процесів до доменів певних користувачів керувати

	об'єкта, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта	інформаційними потоками], *що надає можливість [вибір:* змінювати значення за замовченням, запитувати, модифікувати, видаляти *[призначення:* інші операції]] *атрибути безпеки [призначення:* список атрибутів безпеки] *тільки [призначення:* уповноважені ідентифіковані ролі]	операціями переміщення інформації від об’єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни *атрибутів безпеки* об’єктів та процесів, що належать його домену, таким чином, щоб мати можливість визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта або ініціювати процес
	КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1
	Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які

	експорту та імпорту	даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ
КД-4	Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб’єктів та об’єктів] та всіх операцій суб’єктів на об’єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб’єкта з ОДФ на будь-якому об’єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб’єктів та від них, на які	У списку суб’єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів та процесів, які підтримуються ОЕ. У списку об’єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об’єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від об’єктів при

		поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	посередництві процесів відповідних типів до користувачів відповідних типів (операції читання інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача, процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2 - FDP_ACF.1.4 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування, на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1, усіма операціями переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операціями читання інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ

		необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. *FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки].* FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. *FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]*	
26	Запити на зміну прав доступу до об'єкта повинні	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення:	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1

	оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта	список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: *ФБО повинні реалізовувати [призначення:* ПФБ керування доступом, ПФБ керування інформаційними потоками], *що надає можливість [вибір:* змінювати значення за замовченням, запитувати, модифікувати, видаляти *[призначення:* інші операції]] *атрибути безпеки [призначення:* список атрибутів безпеки] *тільки [призначення:* уповноважені ідентифіковані ролі]	наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об'єктів та процесів усіх типів, які підтримуються ОЕ, з урахуванням належності об'єктів та процесів до доменів певних користувачів керувати операціями переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни *атрибутів безпеки* об'єктів та процесів усіх типів, що належать його домену, таким чином, щоб мати можливість визначати конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта, а також визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес
	КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта		
	КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні,	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або

		дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1
	Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

7.2 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ «Адміністративна конфіденційність»

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Адміністративна конфіденційність" наведено у таблиці 7.2.

Таблиця 7.2

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
1	2	3	4
КА-1	Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів, об'єктів та операцій суб'єктів на об'єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]	У списку суб'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи процесів, на які поширюється політика ФПБ. У списку об'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об'єктів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від об'єктів відповідних типів до процесів відповідних типів (операції читання інформації), на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути процесів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від об'єктів відповідних типів до процесів відповідних типів (операціями читання інформації).

		операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від об'єктів відповідних типів до процесів відповідних типів (операціями читання інформації), на які поширюється політика ФПБ
30	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів усіх типів, на які поширюється політика ФПБ, керувати операціями переміщення інформації від

	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта	керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	об’єктів відповідних типів до процесів відповідних типів (операціями читання інформації). ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни *атрибутів безпеки* об’єктів відповідних типів
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів, на які поширюється політика ФПБ, що відповідають об’єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних

32		користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих	користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
КА-2	Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів, об'єктів та операцій суб'єктів на об'єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]	У списку суб'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів, на які поширюється політика ФПБ. У списку об'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об'єктів та процесів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від об'єктів до користувачів відповідних типів (операції читання інформації) та всі операції ініціювання процесів, на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення:	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від об'єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів

		правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від об'єктів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів, на які поширюється політика ФПБ
34	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів та процесів усіх типів, на які поширюється політика ФПБ, керувати операціями переміщення інформації від об'єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента

	об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта	ідентифіковані ролі]	FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни *атрибутів безпеки* об’єктів та процесів відповідних типів
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, на які поширюється політика ФПБ, що відповідають об’єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина	FDP_ETC.1.1: ФБО повинні	ПФБ керування доступом

	політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних	та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
КА-3	Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів та об'єктів] та всіх операцій суб'єктів на об'єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб'єкта з ОДФ на будь-якому об'єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку суб'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів, які підтримуються ОЕ. У списку об'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об'єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від об'єктів відповідних типів до користувачів відповідних типів (операції читання інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів,

	доступу користувача і захищеного об'єкта	під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки,	процесів та об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від об'єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 усіма операціями переміщення інформації від об'єктів до користувачів відповідних типів (операціями читання інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ
38			

		які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	
	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для

	користувачів, яким надані відповідні повноваження	повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	об’єктів та процесів усіх типів, які підтримуються ОЕ, керувати операціями переміщення інформації від об’єктів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів усіх типів таким чином, щоб мати можливість визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта або ініціювати процес
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта		
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес		
40	Права доступу до	FMT_MSA.2.1: ФБО повинні	Реалізовані

	кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1
	Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	*FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ.* *FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача.* *FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибут*и безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ, які реалізуються функціональними елементами FDP_ETC.2.1 - FDP_ETC.2.4, визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

		атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
КА-4	Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів та об'єктів] та всіх операцій суб'єктів на об'єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб'єкта з ОДФ на будь-якому об'єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку суб'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів та процесів, які підтримуються ОЕ. У списку об'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об'єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операції читання інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача, процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них].	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2 -

		FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та	FDP_ACF.1.4 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування, на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1, усіма операціями переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операціями читання інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ

		інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	
44	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів та процесів усіх типів, які підтримуються ОЕ, керувати операціями переміщення інформації від об'єктів при посередництві процесів відповідних типів до користувачів відповідних типів (операціями читання інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками

	об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта	ідентифіковані ролі]	функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів усіх типів таким чином, щоб мати можливість визначати конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта, а також визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів

		ПФБ	FDP_ACC.2.1 та/або FDP_IFC.2.1
46	Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

7.3 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ «Повторне використання об'єктів»

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ «Повторне використання об'єктів» наведено у таблиці 7.3.

Таблиця 7.3

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
КО-1	Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_RIP.1.1: ФБО повинні забезпечувати недоступність будь-якого попереднього інформаційного вмісту ресурсів при [вибір: виділення ресурсу, звільнення ресурсу] для таких об’єктів: [призначення: список об’єктів]. FDP_RIP.2.1: ФБО повинні забезпечувати недоступність будь-якого попереднього інформаційного вмісту ресурсів при [вибір: виділення ресурсу, звільнення ресурсу] для всіх об’єктів. FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	У списку об’єктів функціональних елементів FDP_RIP.1.1 чи FDP_RIP.2.1 наявні всі типи об’єктів, на які поширюється політика ФПБ "Довірча конфіденційність" або "Адміністративна конфіденційність". Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують скасування прав доступу до об’єкта, встановлених для попереднього користувача або процесу, перш ніж інший користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт
	Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані		
	Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною		

7.4 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Аналіз прихованих каналів"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Аналіз прихованих каналів" наведено у таблиці 7.4.

Таблиця 7.4

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
КК-1	Повинен бути виконаний аналіз прихованих каналів		Відповідні вимоги задоволені елементами довіри AVA_CCA.1.1C, AVA_CCA.1.2C, AVA_CCA.1.3C, AVA_CCA.1.4C, AVA_CCA.1.5C, визначеними стандартом ISO/IEC 15408-3
	Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані		
	Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів		
	Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність		
КК-2	Повинен бути виконаний аналіз прихованих каналів		Відповідні вимоги задоволені елементами довіри AVA_CCA.1.1C, AVA_CCA.1.2C, AVA_CCA.1.3C, AVA_CCA.1.4C, AVA_CCA.1.5C, визначеними стандартом ISO/IEC 15408-3
	Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані		
	Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів		

	Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність		
	КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів	FDP_IFF.6.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], щоб відстежувати [призначення: типи недозволених інформаційних потоків], коли вони перевищують [призначення: максимальна інтенсивність]	У списку типів недозволених інформаційних потоків функціонального елемента FDP_IFF.6.1 наявні всі потоки, що відповідають затвердженій підмножині знайдених прихованих каналів, для яких повинна забезпечуватися реєстрація використання
КК-3	Повинен бути виконаний аналіз прихованих каналів		Відповідні вимоги задоволені елементами довіри AVA_CCA1.1D, AVA_CCA1.2D, AVA_CCA.1.1C, AVA_CCA.1.2C, AVA_CCA.1.3C, AVA_CCA.1.4C, AVA_CCA.1.5C, визначеними стандартом ISO/IEC 15408-3
	Всі (затверджена підмножина) знайдені під час аналізу приховані канали повинні бути усунені	FDP_IFF.5.1: ФБО повинні забезпечувати, щоб не існувало недозволених інформаційних потоків, здатних порушити [призначення: ім'я ПФБ керування інформаційними потоками]	У ПФБ керування інформаційними потоками функціонального елемента FDP_IFF.5.1 наявні всі потоки, що відповідають затвердженій підмножині знайдених прихованих каналів, які повинні бути усунені

7.5 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Конфіденційність при обміні"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Конфіденційність при обміні" наведено у таблиці 7.5.

Таблиця 7.5

Рівень ФПБ	Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ	Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99	Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99
КВ-1	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуютьс я, і спроможність користувачів і/або процесів керувати рівнем захищеності	FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]. FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UCT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від несанкціонованого розкриття. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	У списку суб'єктів функціонального елемента FDP_IFC.1.1 наявні всі типи інтерфейсних процесів, на які поширюється політика ФПБ. У списку об'єктів функціонального елемента FDP_IFC.1.1 наявні всі типи об'єктів, на які поширюється політика ФПБ. У ПФБ керування інформаційними потоками функціональних елементів FDP_IFC.1.1, FDP_ETC.1.1 та FDP_ITC.1.1 наявні всі потоки, що відповідають операціям переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. ПФБ керування інформаційними потоками функціонального елемента FDP_UCT.1.1 надає можливість відправлення та одержання даних користувача у спосіб, захищений від несанкціонованого розкриття, при виконанні всіх операцій переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об'єктів усіх типів, на які поширюється політика ФПБ

	КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається	FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу	В атрибутах безпеки функціонального елемента FDP_IFF.1.1 наявні атрибути інтерфейсних процесів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.1.2 наявні правила забезпечення на підставі атрибутів безпеки функціонального елемента FDP_IFF.1.1 та з використанням криптографічних операцій функціонального елемента FCS_COP.1.1 захисту від безпосереднього ознайомлення з інформацією, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ

		криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
КВ-2	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуютьс я, і спроможність користувачів і/або процесів керувати рівнем захищеності	FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UCT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування	У списку суб'єктів функціонального елемента FDP_IFC.1.1 наявні всі типи інтерфейсних процесів, на які поширюється політика ФПБ. У списку об'єктів функціонального елемента FDP_IFC.1.1 наявні всі типи об'єктів, на які поширюється політика ФПБ. У ПФБ керування інформаційними потоками функціональних елементів FDP_IFC.1.1, FDP_ETC.2.1 та FDP_ITC.2.1 наявні всі потоки, що відповідають операціям переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. ПФБ керування інформаційними потоками функціонального елемента FDP_UCT.1.1 надає можливість відправлення та одержання даних користувача у спосіб, захищений від несанкціонованого розкриття, при виконанні всіх операцій переміщення об'єктів відповідних типів між

		інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від несанкціонованого розкриття. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об’єктів усіх типів, на які поширюється політика ФПБ
	КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу	FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб’єкта та інформації: [призначення: список суб’єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб’єктів та інформації (для кожної операції)]. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила	В атрибутах безпеки функціональних елементів FDP_IFF.1.1 наявні атрибути інтерфейсних процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.1.2 наявні правила забезпечення, на підставі атрибутів безпеки функціонального елемента FDP_IFF.1.1, з використанням атрибутів інтерфейсних процесів, однозначно асоційованих із переданими об'єктами функціональними елементами FDP_ETC.2.2 - FDP_ETC.2.4 та FDP_ITC.2.2 - FDP_ITC.2.5, та за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1, захисту від безпосереднього ознайомлення з інформацією, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ

		при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні	
54			

		розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
	Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, керувати рівнем захищеності об’єктів усіх типів, на які поширюється політика ФПБ. ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із зміни рівня захищеності об’єктів відповідних типів, на які поширюється політика ФПБ

КВ-3	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів	FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UCT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від несанкціонованого розкриття. FDP_ITT.1.1, FDP_ITT.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], щоб запобігати [вибір:	У списку суб'єктів функціонального елемента FDP_IFC.2.1 наявні всі типи користувачів та інтерфейсних процесів, які існують в ОЕ. У списку об'єктів функціонального елемента FDP_IFC.2.1 наявні всі типи об'єктів, які підтримуються ОЕ. У ПФБ керування інформаційними потоками функціональних елементів FDP_IFC.2.1, FDP_ETC.2.1 та FDP_ITC.2.1 наявні всі потоки, що відповідають операціям переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), які підтримуються ОЕ. ПФБ керування інформаційними потоками функціональних елементів FDP_UCT.1.1 та FDP_ITT.1.1 чи FDP_ITT.2.1 надають можливість відправлення та одержання даних користувача у спосіб, захищений від несанкціонованого розкриття, при виконанні всіх операцій переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), які підтримуються ОЕ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об'єктів усіх типів, які підтримуються ОЕ
	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуютьс я, і спроможність користувачів і/або процесів керувати рівнем захищеності		

		розкриття, модифікація, недоступність] даних користувача при їх передачі між фізично розділеними частинами ОО. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	
	КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і приймальника об'єкта Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і джерела об'єкта Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника	FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні	В атрибутах безпеки функціональних елементів FDP_IFF.2.1 наявні атрибути користувачів, інтерфейсних процесів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єктах відповідних типів, які передаються між ініційованими певними користувачами інтерфейсними процесами відповідних типів. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.2.2 наявні правила забезпечення на підставі атрибутів безпеки функціонального елемента FDP_IFF.2.1 з використанням атрибутів користувачів – джерел, користувачів - приймальників об'єктів та атрибутів інтерфейсних процесів, однозначно асоційованих із переданими об'єктами функціональними елементами FDP_ETC.2.2 - FDP_ETC.2.4 та FDP_ITC.2.2 - FDP_ITC.2.5, та за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1, захисту від безпосереднього ознайомлення з інформацією, що міститься в об'єктах усіх типів, що передаються між ініційованими певними користувачами інтерфейсними процесами усіх типів, які підтримуються ОЕ. При цьому представлення захищеного

		реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів].	об'єкта є функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника

		FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
	Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, керувати рівнем захищеності об’єктів усіх типів, які підтримуються ОЕ. ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із зміни рівня захищеності об’єктів усіх типів, які підтримуються ОЕ

КВ-4	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів	FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UCT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від несанкціонованого розкриття. FDP_ITT.1.1, FDP_ITT.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], щоб запобігати [вибір:	У списку суб'єктів функціонального елемента FDP_IFC.2.1 наявні всі типи користувачів та інтерфейсних процесів, які існують в ОЕ. У списку об'єктів функціонального елемента FDP_IFC.2.1 наявні всі типи об'єктів, які підтримуються ОЕ. У ПФБ керування інформаційними потоками функціональних елементів FDP_IFC.2.1, FDP_ETC.2.1 та FDP_ITC.2.1 наявні всі потоки, що відповідають операціям переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), які підтримуються ОЕ. ПФБ керування інформаційними потоками функціональних елементів FDP_UCT.1.1 та FDP_ITT.1.1 чи FDP_ITT.2.1 надають можливість відправлення та одержання даних користувача у спосіб, захищений від несанкціонованого розкриття, при виконанні всіх операцій переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), які підтримуються ОЕ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об'єктів усіх типів, які підтримуються ОЕ
	Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуютьс я, і спроможність користувачів і/або процесів керувати рівнем захищеності		

		розкриття, модифікація, недоступність] даних користувача при їх передачі між фізично розділеними частинами ОО. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	
	КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і приймальника об'єкта Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і джерела об'єкта Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника	FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних	В атрибутах безпеки функціональних елементів FDP_IFF.2.1 наявні атрибути користувачів, інтерфейсних процесів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єктах відповідних типів, які передаються між ініційованими певними користувачами інтерфейсними процесами відповідних типів. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.2.2 наявні правила забезпечення на підставі атрибутів безпеки функціонального елемента FDP_IFF.2.1 з використанням атрибутів користувачів – джерел, користувачів - приймальників об'єктів та атрибутів інтерфейсних процесів, однозначно асоційованих із переданими об'єктами функціональними елементами FDP_ETC.2.2 - FDP_ETC.2.4 та FDP_ITC.2.2 - FDP_ITC.2.5, та за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1, захисту від безпосереднього ознайомлення з інформацією, що міститься в об'єктах усіх типів, що передаються між ініційованими певними користувачами інтерфейсними процесами усіх типів, які підтримуються ОЕ. При цьому представлення захищеного

62		користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні	об'єкта є функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника

		ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
	Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, керувати рівнем захищеності об’єктів усіх типів, які підтримуються ОЕ. ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із зміни рівня захищеності об’єктів усіх типів, які підтримуються ОЕ

	Політика конфіденційності при обміні повинна включати опис інформації, яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів		Відповідні вимоги задоволені елементами довіри AVA_CCA1.1D, AVA_CCA1.2D, AVA_CCA.1.1C, AVA_CCA.1.2C, AVA_CCA.1.3C, AVA_CCA.1.4C, AVA_CCA.1.5C, визначеними стандартом ISO/IEC 15408-3
	Повинен бути виконаний аналіз прихованих каналів обміну		
	Всі знайдені приховані канали обміну і максимальна пропускна здатність кожного із них мають бути документовані		
	Повинна бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення	FDP_IFF.4.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], щоб обмежити інтенсивність [призначення: типи недозволених інформаційних потоків] до [призначення: максимальна інтенсивність]. FDP_IFF.4.2: ФБО повинні запобігати [призначення: типи недозволених інформаційних потоків]. FDP_IFF.5.1: ФБО повинні забезпечувати, щоб не існувало недозволених інформаційних потоків, здатних порушити [призначення: ім’я ПФБ керування інформаційними потоками]. FDP_IFF.6.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], щоб відстежувати [призначення: типи недозволених інформаційних потоків], коли вони перевищують [призначення: максимальна інтенсивність]	У ПФБ керування інформаційними потоками функціональних елементів FDP_IFF.4.1, FDP_IFF.4.2, FDP_IFF.5.1, FDP_IFF.6.1 наявні всі потоки, що відповідають затвердженій підмножині знайдених прихованих каналів, для яких повинна бути забезпечена реєстрація використання, часткове перекриття або усунення

8 Відомості щодо відповідності функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам критеріїв цілісності, встановленим НД ТЗІ 2.5-004-99

У підрозділах цього розділу у таблицях 8.1 – 8.4 викладені відомості щодо відповідності функціональних елементів функціональних компонентів безпеки відповідних функціональних класів безпеки, встановлених стандартом ISO/IEC 15408, вимогам критеріїв цілісності, встановленим НД ТЗІ 2.5-004-99, для різних ФПБ. Відомості викладено у табличному вигляді, окремо для кожної ФПБ та її рівнів, визначених НД ТЗІ 2.5-004-99, із зазначенням у кожній таблиці: рівня ФПБ; вимог НД ТЗІ 2.5-004-99 щодо політики відповідної ФПБ відповідного рівня; вимог стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких у процесі виконання зіставлення функціональних компонентів безпеки згідно з ISO/IEC 15408, реалізованих у певному ЗТЗІ від НСД, з вимогами НД ТЗІ 2.5-004-99, можна приймати рішення про те, що певна сукупність функціональних елементів функціональних компонентів безпеки задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.

8.1 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Довірча цілісність"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Довірча цілісність" наведено у таблиці 8.1.

Таблиця 8.1

Рівень ФПБ	Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ	Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99	Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99
ЦД-1	Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб’єктів, об’єктів та операцій суб’єктів на об’єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ	У списку суб’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів, на які поширюється політика ФПБ. У списку об’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або

		керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]	FDP_IFC.1.1 наявні всі операції переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операції модифікації інформації), на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них -	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути користувачів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації). У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації), на які поширюється політика ФПБ

		атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	
	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об'єктів усіх типів, на які поширюється політика ФПБ, з урахуванням належності об'єктів до доменів певних користувачів керувати операціями переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації). ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об'єктів відповідних типів, що належать його домену

		ідентифіковані ролі]	
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів, на які поширюється політика ФПБ, що відповідають об’єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача.	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів	

		безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
ЦД-2	Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб’єктів, об’єктів та операцій суб’єктів на об’єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів, інформації та операцій переміщення керованої інформації до керованих суб’єктів, на які поширюється ПФБ, та від них]	У списку суб’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів та процесів, на які поширюється політика ФПБ. У списку об’єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об’єктів та процесів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від процесів до об’єктів відповідних типів (операції модифікації інформації) та всі операції ініціювання процесів, на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об’єктів, що ґрунтується на [призначення: список суб’єктів та об’єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб’єкта на керованому об’єкті: [призначення: правила керування доступом	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути користувачів, процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від процесів відповідних типів до об’єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від

		керованих суб’єктів до керованих об’єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб’єктів до об’єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб’єктів до об’єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб’єкта та інформації: [призначення: список суб’єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.1.2: ФБО повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб’єктів та інформації (для кожної операції)]. FDP_IFF.1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	процесів відповідних типів до об’єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів, на які поширюється політика ФПБ
	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення:	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами

	на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес	список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об'єктів та процесів усіх типів, на які поширюється політика ФПБ, з урахуванням належності об'єктів та процесів до доменів певних користувачів керувати операціями переміщення інформації від процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об'єктів та процесів відповідних типів, що належать його домену
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об'єктів та процесів, на які поширюється політика ФПБ, що відповідають об'єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина політики довірчої цілісності мають	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних

	бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-	користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
ЦД-3 74	Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб’єктів та об’єктів] та всіх операцій суб’єктів на об’єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні	У списку суб’єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів та процесів, які підтримуються ОЕ. У списку об’єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об’єктів та процесів, які підтримуються ОЕ.

		забезпечувати, щоб на операції будь-якого суб’єкта з ОДФ на будь-якому об’єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб’єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб’єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від процесів відповідних типів до об’єктів відповідних типів (операції модифікації інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об’єктів, що ґрунтується на [призначення: список суб’єктів та об’єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб’єкта на керованому об’єкті: [призначення: правила керування доступом керованих суб’єктів до керованих об’єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб’єктів до об’єктів, що ґрунтується на таких	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та об’єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від процесів відповідних типів до об’єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування, на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1, усіма операціями переміщення інформації від процесів до об’єктів відповідних типів (операціями модифікації інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ

76		додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що	

		ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	

	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об’єктів та процесів усіх типів, які підтримуються ОЕ, з урахуванням належності об’єктів та процесів до доменів певних користувачів керувати операціями переміщення інформації від процесів відповідних типів до об’єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів, що належать його домену, таким чином, щоб мати можливість визначати конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт, та визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес
	КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт		
	КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1

		використовуються для реалізації ПФБ	
	Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

		передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
ЦД-4	Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів та об'єктів] та всіх операцій суб'єктів на об'єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб'єкта з ОДФ на будь-якому об'єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку суб'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів та процесів, які підтримуються ОЕ. У списку об'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об'єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від користувачів при посередництві процесів відповідних типів до об'єктів відповідних типів (операції модифікації інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від користувачів при посередництві процесів

		атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах	відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2 - FDP_ACF.1.4 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 усіма операціями переміщення інформації від користувачів при посередництві процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ

		безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти	
82			

		інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	
	Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам для об’єктів та процесів усіх типів, які підтримуються ОЕ, з урахуванням належності об’єктів та процесів до доменів певних користувачів керувати операціями переміщення інформації від користувачів при посередництві процесів відповідних типів до об’єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з будь-якою роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів усіх типів, що належать його домену, таким чином, щоб мати можливість визначати конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт, та визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес

	КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1
	Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

		реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	

8.2 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Адміністративна цілісність"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Адміністративна цілісність" наведено у таблиці 8.2.

Таблиця 8.2

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
ЦА-1	Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів, об'єктів та операцій суб'єктів на об'єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]	У списку суб'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів, на які поширюється політика ФПБ. У списку об'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об'єктів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операції модифікації інформації), на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них].	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути користувачів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації). У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або

		FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 операціями переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації), на які поширюється політика ФПБ
	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу,	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів усіх типів, на які поширюється політика ФПБ, керувати операціями переміщення інформації від користувачів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації).

	що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт	атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів відповідних типів
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів, на які поширюється політика ФПБ, що відповідають об’єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
	Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3

		атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні	або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
ЦА-2	Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FDP_ACC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів, об'єктів та операцій суб'єктів на об'єктах, на які поширюється ПФБ]. FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]	У списку суб'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи користувачів та процесів, на які поширюється політика ФПБ. У списку об'єктів функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі типи об'єктів та процесів, на які поширюється політика ФПБ. У списку операцій функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1 наявні всі операції переміщення інформації від процесів до об'єктів відповідних типів (операції модифікації інформації) та всі операції ініціювання процесів, на які поширюється політика ФПБ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2, FDP_IFF.1.5 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1

		дозволяють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]	та/або FDP_IFF.1.1 операціями переміщення інформації від процесів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів, на які поширюється політика ФПБ
	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів та процесів усіх типів, на які поширюється політика ФПБ, керувати операціями переміщення інформації від процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають

	користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт		можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів відповідних типів
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, на які поширюється політика ФПБ, що відповідають об’єктам функціональних елементів FDP_ACC.1.1 та/або FDP_IFC.1.1
92	Як частина політики адміністративної цілісності мають бути представлені	FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ

	правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.1.2: ФБО повинні експортувати дані користувача без атрибутів безпеки, асоційованих із даними користувача. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.1.2: ФБО повинні ігнорувати будь-які атрибути безпеки, асоційовані з даними користувача, при імпорті із-за меж ОДФ. FDP_ITC.1.3: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки,	функціональних елементів FDP_ETC.1.1 та FDP_ETC.1.2 або FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.1.1 - FDP_ITC.1.3 або FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, на які поширюється політика ФПБ

		асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
ЦА-3	Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів та об'єктів] та всіх операцій суб'єктів на об'єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб'єкта з ОДФ на будь-якому об'єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку суб'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів та процесів, які підтримуються ОЕ. У списку об'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об'єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від процесів відповідних типів до об'єктів відповідних типів (операції модифікації інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ].	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями

		FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах:	переміщення інформації від процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2, FDP_ACF.1.3 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 усіма операціями переміщення інформації від процесів до об'єктів відповідних типів (операціями модифікації інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ

		[призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF.2.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	
96	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів та процесів усіх типів, які підтримуються ОЕ, керувати операціями переміщення інформації

	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт	інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	від процесів відповідних типів до об’єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів усіх типів таким чином, щоб мати можливість визначати конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт, та визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують

	ініціалізації	інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1
	Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні	ПФБ керування доступом та/або ПФБ керування інформаційними потоками при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

		реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	
ЦА-4	Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ОЕ	FDP_ACC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] для [призначення: список суб'єктів та об'єктів] та всіх операцій суб'єктів на об'єктах, на які поширюється ПФБ. FDP_ACC.2.2: ФБО повинні забезпечувати, щоб на операції будь-якого суб'єкта з ОДФ на будь-якому об'єкті з ОДФ поширювалась будь-яка ПФБ керування доступом. FDP_IFC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів та інформації] та всіх операцій переміщення керованої інформації до керованих суб'єктів та від них, на які поширюється ПФБ. FDP_IFC.2.2: ФБО повинні забезпечувати, щоб у межах ОДФ на всі операції переміщення керованої інформації до керованих суб'єктів та від них поширювалась будь-яка ПФБ керування інформаційними потоками	У списку суб'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи користувачів та процесів, які підтримуються ОЕ. У списку об'єктів функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі типи об'єктів та процесів, які підтримуються ОЕ. У списку операцій функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1 наявні всі операції переміщення інформації від користувачів при посередництві процесів відповідних типів до об'єктів відповідних типів (операції модифікації інформації) та всі операції ініціювання процесів, які підтримуються ОЕ
	КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача і захищеного об'єкта	FDP_ACF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом] до об'єктів, що ґрунтується на [призначення: список суб'єктів та об'єктів, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки або іменовані групи атрибутів безпеки, що відносяться до цієї ПФБ]. FDP_ACF.1.2: ФБО повинні реалізовувати такі правила визначення того, чи дозволена операція керованого суб'єкта на керованому об'єкті: [призначення: правила керування доступом керованих суб'єктів до керованих об'єктів із використанням керованих операцій на них]. FDP_ACF.1.3: ФБО повинні явно дозволяти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно	В атрибутах безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 наявні атрибути користувачів, процесів та об'єктів усіх типів, які підтримуються ОЕ, що дозволяють керувати операціями переміщення інформації від користувачів при посередництві процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. У правилах керування доступом функціональних елементів FDP_ACF.1.2 - FDP_ACF.1.4 та/або FDP_IFF.1.2 - FDP_IFF.1.6 чи FDP_IFF.2.2 - FDP_IFF.2.6 наявні

		дозволяють доступ суб'єктів до об'єктів]. FDP_ACF.1.4: ФБО повинні явно забороняти доступ суб'єктів до об'єктів, що ґрунтується на таких додаткових правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють доступ суб'єктів до об'єктів]. FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF. 1.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.1.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]. FDP_IFF.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб'єкта та інформації: [призначення: список суб'єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки].	правила керування на підставі атрибутів безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1 чи FDP_IFF.2.1 усіма операціями переміщення інформації від користувачів при посередництві процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та усіма операціями ініціювання процесів, які підтримуються ОЕ
100		FDP_IFF.2.2: ФБО повинні дозволяти	

		інформаційний потік між керованим суб'єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила, що ґрунтуються на впорядкованих зв'язках між атрибутами безпеки: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб'єктів та інформації (для кожної операції)]. FDP_IFF.2.5: ФБО повинні явно дозволяти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно дозволяють інформаційні потоки]. FDP_IFF.2.6: ФБО повинні явно забороняти інформаційний потік, що ґрунтується на таких правилах: [призначення: правила, що ґрунтуються на атрибутах безпеки, які явно забороняють інформаційні потоки]	
	Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FDP_ACF.1.1 та/або FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, для об'єктів та процесів усіх типів, які підтримуються ОЕ, керувати операціями переміщення інформації від користувачів при посередництві процесів відповідних типів до об'єктів відповідних типів (операціями модифікації інформації) та операціями ініціювання процесів. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних

	визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт		елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із призначення/ зміни атрибутів безпеки об’єктів та процесів усіх типів таким чином, щоб мати можливість визначати конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт, та визначати конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес
	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес		
	Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації	FMT_MSA.2.1: ФБО повинні забезпечувати призначення атрибутам безпеки тільки безпечних значень. FMT_MSA.3.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що передбачає [вибір: обмежувальні, дозволяючі, інші властивості] значень за замовченням для атрибутів безпеки, що використовуються для реалізації ПФБ	Реалізовані функціональними елементами FMT_MSA.2.1 та FMT_MSA.3.1 правила та використовувані властивості атрибутів безпеки забезпечують встановлення цих атрибутів у момент створення або ініціалізації всіх типів об’єктів та процесів, що підтримуються ОЕ та відповідають об’єктам функціональних елементів FDP_ACC.2.1 та/або FDP_IFC.2.1
	Як частина політики адміністративної	FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ	ПФБ керування доступом та/або ПФБ керування інформаційними потоками

	цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту	керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]	при експорті даних користувача за межі ОДФ функціональних елементів FDP_ETC.2.1 - FDP_ETC.2.4 визначені для всіх типів об’єктів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками при імпорті даних користувача із-за меж ОДФ функціональних елементів FDP_ITC.2.1 - FDP_ITC.2.5 визначені для всіх типів об’єктів, які підтримуються ОЕ

8.3 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Відкат"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Відкат" наведено у таблиці 8.3.

Таблиця 8.3

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
ЦО-1	Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу	FDP_ROL.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] щоб дозволяти відкат [призначення: список операцій] на [призначення: список об’єктів]. FDP_ROL.1.2: ФБО повинні дозволяти відкат в межах [призначення: обмеження виконання відкату]	У списку об’єктів функціонального елемента FDP_ROL.1.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. У списку операцій функціонального елемента FDP_ROL.1.1 наявні всі типи операції над об’єктами відповідних типів, на які поширюється політика ФПБ. У обмеженнях виконання відкату функціонального елемента FDP_ROL.1.2 визначені ті проміжки часу, для яких можливий відкат (відміна) певних множин операцій, виконаних над об’єктами відповідних типів
ЦО-2	Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу	FDP_ROL.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] щоб дозволяти відкат усіх операцій на [призначення: список об’єктів]. FDP_ROL.2.2: ФБО повинні дозволяти відкат в межах [призначення: обмеження виконання відкату]	У списку об’єктів функціонального елемента FDP_ROL.2.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. У обмеженнях виконання відкату функціонального елемента FDP_ROL.2.2 визначені ті проміжки часу, для яких можливий відкат (відміна) всіх операцій, виконаних над об’єктами відповідних типів

8.4 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Цілісність при обміні"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Цілісність при обміні" наведено у таблиці 8.4.

Таблиця 8.4

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
ЦВ-1	Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовувани ми механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності	FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб'єктів, інформації та операцій переміщення керованої інформації до керованих суб'єктів, на які поширюється ПФБ, та від них]. FDP_ETC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ITC.1.1: ФБО повинні реалізовувати [призначення: політики ФБ керування доступом та/або політики ФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UIT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від таких помилок [вибір: модифікація, видалення, вставка, повтор]. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	У списку суб'єктів функціонального елемента FDP_IFC.1.1 наявні всі типи інтерфейсних процесів, на які поширюється політика ФПБ. У списку об'єктів функціонального елемента FDP_IFC.1.1 наявні всі типи об'єктів, на які поширюється політика ФПБ. У ПФБ керування інформаційними потоками функціональних елементів FDP_IFC.1.1, FDP_ETC.1.1 та FDP_ITC.1.1 наявні всі потоки, що відповідають операціям переміщення об'єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією) або операціям експорту об'єктів відповідних типів за межі ОДФ та імпорту інформації із-за меж ОДФ, на які поширюється політика ФПБ. ПФБ керування інформаційними потоками

			функціонального елемента FDP_UIT.1.1 надає можливість відправлення та одержання даних користувача у спосіб, захищений від порушення цілісності інформації внаслідок її несанкціонованої модифікації, при виконанні всіх операцій переміщення об’єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об’єктів усіх типів, на які поширюється політика ФПБ
	КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається	FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб’єкта та інформації: [призначення: список суб’єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб’єктів та інформації (для кожної операції)]. FDP_UIT.1.2: ФБО повинні бути здатними визначати після одержання даних користувача, чи виникли такі помилки [вибір: модифікація, видалення, вставка, повтор].	В атрибутах безпеки функціонального елемента FDP_IFF.1.1 наявні атрибути інтерфейсних процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють засобам функціонального елемента FDP_UIT.1.2 забезпечувати захист від порушення цілісності інформації, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ, внаслідок її несанкціонованої модифікації. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.1.2

		FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	наявні правила забезпечення функціональним елементом FDP_UIT.1.2 на підставі атрибутів безпеки функціонального елемента FDP_IFF.1.1 та з використанням криптографічних операцій функціонального елемента FCS_COP.1.1 захисту від порушення цілісності інформації, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ
ЦВ-2	Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовувани	FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів, інформації та операцій переміщення керованої інформації до керованих суб’єктів, на які поширюється ПФБ, та від них]. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ.	У списку суб’єктів функціонального елемента FDP_IFC.1.1 наявні всі типи інтерфейсних процесів, на які поширюється політика ФПБ. У списку об’єктів функціонального елемента FDP_IFC.1.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. У ПФБ керування інформаційними

	ми механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності	FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UIT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від таких помилок [вибір: модифікація, видалення, вставка, повтор]. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	потоками функціональних елементів FDP_IFC.1.1, FDP_ETC.2.1 та FDP_ITC.2.1 наявні всі потоки, що відповідають операціям переміщення об’єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією) або операціям експорту об’єктів відповідних типів за межі ОДФ та імпорту інформації із-за меж ОДФ, на які поширюється політика ФПБ. ПФБ керування інформаційними потоками функціонального елемента FDP_UIT.1.1 надає можливість відправлення та одержання даних користувача у спосіб, захищений від порушення цілісності інформації внаслідок її несанкціонованої модифікації, видалення, вставки, повтору при виконанні всіх операцій переміщення об’єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об’єктів усіх типів, на які поширюється політика ФПБ
	КЗЗ повинен забезпечувати можливість виявлення порушення	FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб’єкта та	В атрибутах безпеки функціонального елемента FDP_IFF.1.1 наявні атрибути інтерфейсних процесів та

	цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання	інформації: [призначення: список суб’єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб’єктів та інформації (для кожної операції)]. FDP_UIT.1.2: ФБО повинні бути здатними визначати після одержання даних користувача, чи виникли такі помилки [вибір: модифікація, видалення, вставка, повтор]. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача,	об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють засобам функціонального елемента FDP_UIT.1.2 забезпечувати захист від порушення цілісності інформації, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ, внаслідок її несанкціонованої модифікації, видалення, вставки, повтору. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.1.2 наявні правила забезпечення функціональним елементом FDP_UIT.1.2 на підставі атрибутів безпеки функціонального елемента FDP_IFF.1.1 з використанням атрибутів інтерфейсних процесів, однозначно асоційованих із переданими об'єктами функціональними елементами FDP_ETC.2.2 - FDP_ETC.2.4 та FDP_ITC.2.2 - FDP_ITC.2.5, та за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 захисту від порушення цілісності інформації, що міститься в об'єктах відповідних типів, які передаються між інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ
	Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу		
	Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу		

		контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
110	Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів,	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями.	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, керувати

	яким надані відповідні повноваження	FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	рівнем захищеності об’єктів усіх типів, на які поширюється політика ФПБ. ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із зміни рівня захищеності об’єктів відповідних типів, на які поширюється політика ФПБ
ЦВ-3	Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовувани ми механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності	FDP_IFC.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками] для [призначення: список суб’єктів, інформації та операцій переміщення керованої інформації до керованих суб’єктів, на які поширюється ПФБ, та від них]. FDP_ETC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при експорті даних користувача, контрольованому ПФБ, за межі ОДФ. FDP_ITC.2.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками] при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ. FDP_UIT.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом та/або ПФБ керування інформаційними потоками], що надає можливість [вибір: відправлення, одержання] даних користувача у спосіб, захищений від таких помилок [вибір: модифікація, видалення, вставка, повтор]. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	У списку суб’єктів функціонального елемента FDP_IFC.1.1 наявні всі типи користувачів та інтерфейсних процесів, на які поширюється політика ФПБ. У списку об’єктів функціонального елемента FDP_IFC.1.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. У ПФБ керування інформаційними потоками функціональних елементів FDP_IFC.1.1, FDP_ETC.2.1 та FDP_ITC.2.1 наявні всі потоки, що відповідають операціям переміщення об’єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією) або операціям експорту об’єктів відповідних типів за межі ОДФ та імпорту інформації із-за меж ОДФ, на які поширюється політика ФПБ. ПФБ керування інформаційними

			потоками функціонального елемента FDP_UIT.1.1 надає можливість відправлення та одержання даних користувача у спосіб, захищений від порушення цілісності інформації внаслідок її несанкціонованої модифікації, видалення, вставки, повтору при виконанні всіх операцій переміщення об’єктів відповідних типів між інтерфейсними процесами відповідних типів (операції обміну інформацією), на які поширюється політика ФПБ. Функції керування безпекою функціонального елемента FMT_SMF.1.1 забезпечують можливість керування рівнем захищеності об’єктів усіх типів, на які поширюється політика ФПБ
	КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і приймальника об'єкта	FDP_IFF.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування інформаційними потоками], що ґрунтується на таких типах атрибутів безпеки суб’єкта та інформації: [призначення: список суб’єктів та типів інформації, що знаходяться під керуванням зазначеної ПФБ, та для кожного із них - атрибути безпеки]. FDP_IFF. 1.2: ФБО повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції, якщо виконуються такі правила: [призначення: співвідношення, що ґрунтуються на атрибутах безпеки, які необхідно підтримувати між атрибутами безпеки суб’єктів та інформації (для кожної операції)]. FDP_UIT.1.2: ФБО повинні бути здатними визначати після одержання даних користувача, чи	В атрибутах безпеки функціонального елемента FDP_IFF.1.1 наявні атрибути користувачів, інтерфейсних процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють засобам функціонального елемента FDP_UIT.1.2 забезпечувати захист від порушення цілісності інформації, що міститься в об'єктах відповідних типів, які передаються між ініційованими певними користувачами інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ, внаслідок її несанкціонованої

	Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу і джерела об'єкта Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника	виникли такі помилки [вибір: модифікація, видалення, вставка, повтор]. FDP_ETC.2.2: ФБО повинні експортувати дані користувача з атрибутами безпеки, асоційованими з даними користувача. FDP_ETC.2.3: ФБО повинні забезпечувати, щоб при експорті за межі ОДФ атрибути безпеки однозначно асоціювались із експортованими даними користувача. FDP_ETC.2.4: ФБО повинні реалізовувати такі правила при експорті даних користувача з ОДФ: [призначення: додаткові правила керування експортом інформації]. FDP_ITC.2.2: ФБО повинні використовувати атрибути безпеки, асоційовані з імпортованими даними користувача. FDP_ITC.2.3: ФБО повинні забезпечувати, щоб використовуваний протокол передбачав однозначну асоціацію між атрибутами безпеки та одержаними даними користувача. FDP_ITC.2.4: ФБО повинні забезпечувати, щоб інтерпретація атрибутів безпеки імпортованих даних користувача була такою, як передбачено джерелом даних користувача. FDP_ITC.2.5: ФБО повинні реалізовувати такі правила при імпорті даних користувача, контрольованому ПФБ, із-за меж ОДФ: [призначення: додаткові правила керування імпортом]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина	модифікації, видалення, вставки, повтору. У правилах керування інформаційними потоками функціонального елемента FDP_IFF.1.2 наявні правила забезпечення функціональним елементом FDP_UIT.1.2 на підставі атрибутів безпеки функціонального елемента FDP_IFF.1.1 з використанням атрибутів користувачів – джерел, користувачів - приймальників об’єктів та атрибутів інтерфейсних процесів, однозначно асоційованих із переданими об'єктами функціональними елементами FDP_ETC.2.2 - FDP_ETC.2.4 та FDP_ITC.2.2 - FDP_ITC.2.5, та за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1, захисту від порушення цілісності інформації, що міститься в об'єктах відповідних типів, які передаються між ініційованими певними користувачами інтерфейсними процесами відповідних типів та на які поширюється політика ФПБ. При цьому представлення захищеного об'єкта є функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника

		криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
	Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FDP_IFF.1.1, що дозволяють користувачам, асоційованим із певними ролями, керувати рівнем захищеності об’єктів усіх типів, які підтримуються ОЕ. ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції зі зміни рівня захищеності об’єктів усіх типів, які підтримуються ОЕ

9 Відомості щодо відповідності функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам критеріїв доступності, встановленим НД ТЗІ 2.5-004-99

У підрозділах цього розділу у таблицях 9.1 – 9.4 викладено відомості щодо відповідності функціональних елементів функціональних компонентів безпеки відповідних функціональних класів безпеки, встановлених стандартом ISO/IEC 15408, вимогам критеріїв доступності, встановленим НД ТЗІ 2.5-004-99, для різних ФПБ. Відомості викладено у табличному вигляді, окремо для кожної ФПБ та її рівнів, визначених НД ТЗІ 2.5-004-99, із зазначенням у кожній таблиці: рівня ФПБ; вимог НД ТЗІ 2.5-004-99 щодо політики відповідної ФПБ відповідного рівня; вимог стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких у процесі виконання зіставлення функціональних компонентів безпеки згідно з ISO/IEC 15408, реалізованих у певному ЗТЗІ від НСД, з вимогами НД ТЗІ 2.5-004-99, можна приймати рішення про те, що певна сукупність функціональних елементів функціональних компонентів безпеки задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.

9.1 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Використання ресурсів"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Використання ресурсів" наведено у таблиці 9.1.

Таблиця 9.1

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
ДР-1	Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів ОЕ, до яких вона відноситься	FRU_RSA.1.1: ФБО повинні реалізовувати максимальні квоти таких ресурсів: [призначення: керовані ресурси], які [вибір: окремі користувачі, окремі групи користувачів, суб’єкти] можуть використовувати [вибір: одночасно, протягом певного періоду часу]	У функціональному елементі FRU_RSA.1.1 визначені всі типи користувачів та поділюваних ресурсів, на які поширюється політика ФПБ. Функціональний елемент FRU_RSA.1.1 надає можливість встановлення максимальних обмежень (максимальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, на які поширюється політика ФПБ
	Політика використання ресурсів повинна визначати обмеження, які можна накладати,		

	на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу		
	Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FRU_RSA.1.1, що забезпечують встановлення максимальних обмежень (максимальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, на які поширюється політика ФПБ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із встановлення/ зміни максимальних обмежень (максимальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, на які поширюється політика ФПБ
ДР-2	Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів ОЕ	FRU_RSA.2.1: ФБО повинні реалізовувати максимальні квоти таких ресурсів: [призначення: керовані ресурси], які [вибір: окремі користувачі, окремі групи користувачів, суб’єкти] можуть використовувати [вибір: одночасно, протягом певного періоду часу]. FRU_RSA.2.2: ФБО повинні забезпечувати виділення мінімального числа кожного із [призначення: керовані ресурси], які є доступними для [вибір: окремі користувачі, окремі групи користувачів,	У функціональних елементах FRU_RSA.2.1 та FRU_RSA.2.2 визначені всі типи користувачів та поділюваних ресурсів, які підтримуються ОЕ. Функціональний елемент FRU_RSA.2.1 надає можливість встановлення максимальних обмежень (максимальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ. Функціональний елемент FRU_RSA.2.2 надає можливість встановлення
	Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються		

	окремому користувачу Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача	суб'єкти], щоб використовувати [вибір: одночасно, протягом певного періоду часу]	мінімальних обмежень (мінімальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ
	Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FRU_RSA.2.1 та FRU_RSA.2.2, що забезпечують встановлення максимальних обмежень (максимальних квот) та мінімальних обмежень (мінімальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із встановлення/ зміни максимальних обмежень (максимальних квот) та мінімальних обмежень (мінімальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ

ДР-3	Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів ОЕ	FRU_RSA.2.1: ФБО повинні реалізовувати максимальні квоти таких ресурсів: [призначення: керовані ресурси], які [вибір: окремі користувачі, окремі групи користувачів, суб'єкти] можуть використовувати [вибір: одночасно, протягом певного періоду часу]. FRU_RSA.2.2: ФБО повинні забезпечувати виділення мінімального числа кожного із [призначення: керовані ресурси], які є доступними для [вибір: окремі користувачі, окремі групи користувачів, суб'єкти], щоб використовувати [вибір: одночасно, протягом певного періоду часу]. FRU_PRS.2.1: ФБО повинні встановлювати пріоритет кожному суб'єкту в ФБО. FRU_PRS.2.2: ФБО повинні забезпечувати доступ до всіх спільно використовуваних ресурсів на підставі пріоритетів, призначених суб'єктам	У функціональних елементах FRU_RSA.2.1 та FRU_RSA.2.2 визначені всі типи користувачів, груп користувачів та поділюваних ресурсів, які підтримуються ОЕ. Функціональний елемент FRU_RSA.2.1 надає можливість встановлення максимальних обмежень (максимальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів та груп користувачів усіх типів, які підтримуються ОЕ. Функціональний елемент FRU_RSA.2.2 надає можливість встановлення мінімальних обмежень (мінімальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів та груп користувачів усіх типів, які підтримуються ОЕ. Функціональні елементи FRU_PRS.2.1 та FRU_PRS.2.2 надають можливість встановлення пріоритетів та забезпечення доступу на підставі встановлених пріоритетів до поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ
	Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу і довільним групам користувачів		
	Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача і довільних груп користувачів		
	Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціональних елементів FRU_RSA.2.1 та FRU_RSA.2.2, що забезпечують встановлення максимальних обмежень (максимальних квот) та мінімальних обмежень (мінімальних квот) на обсяг поділюваних ресурсів усіх

		ролями. FMT_MSA.1.1: ФБО повинні реалізовувати [призначення: ПФБ керування доступом, ПФБ керування інформаційними потоками], що надає можливість [вибір: змінювати значення за замовченням, запитувати, модифікувати, видаляти [призначення: інші операції]] атрибути безпеки [призначення: список атрибутів безпеки] тільки [призначення: уповноважені ідентифіковані ролі]	типів для користувачів та груп користувачів усіх типів, які підтримуються ОЕ. У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції керування атрибутами безпеки функціонального елемента FRU_PRS.2.1, що забезпечують встановлення пріоритетів доступу до поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із встановлення/ зміни максимальних обмежень (максимальних квот) та мінімальних обмежень (мінімальних квот) на обсяг поділюваних ресурсів усіх типів для користувачів та груп користувачів усіх типів, які підтримуються ОЕ. ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FMT_MSA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснювати операції із встановлення/ зміни пріоритетів доступу до поділюваних ресурсів усіх типів для користувачів усіх типів, які підтримуються ОЕ

9.2 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Стійкість до відмов"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Стійкість до відмов" наведено у таблиці 9.2.

Таблиця 9.2

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
ДС-1	Розробник повинен провести аналіз відмов компонентів ОЕ	FPT_FLS.1.1: ФБО повинні зберігати безпечний стан при таких типах збоїв: [призначення: список типів збоїв ФБО]. FRU_FLT.1.1: ФБО повинні забезпечувати виконання [призначення: список можливостей ОО], коли виникають такі збої [призначення: список типів збоїв]	У списках типів збоїв та можливостей ОО функціональних елементів FPT_FLS.1.1 та FRU_FLT.1.1 наявні всі типи відмов, після яких ОЕ в змозі продовжувати функціонування, визначені у політиці ФПБ. Список можливостей ОО, виконання яких забезпечується при виникненні певних збоїв, та список відповідних типів збоїв функціонального елемента FRU_FLT.1.1 забезпечують виконання вимог політики ФПБ щодо того, щоб відмова одного захищеного компонента не призводила до недоступності всіх послуг, а в гіршому випадку проявлялася у зниженні характеристик обслуговування
	Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів ОЕ, до яких вона відноситься, і типи їх відмов, після яких ОЕ в змозі продовжувати функціонування		
	Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги		
	Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в		

	зниженні характеристик обслуговування		
	КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента	FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAA.1.1: ФБО повинні бути здатними застосовувати набір правил моніторингу подій, що підлягають аудиту, та на підставі цих правил вказувати на можливе порушення політики безпеки об'єкта (ПБО)	Правила моніторингу подій функціонального елемента FAU_SAA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, одержувати інформацію про відмову будь-якого захищеного компонента
ДС-2	Розробник повинен провести аналіз відмов компонентів ОЕ	FPT_FLS.1.1: ФБО повинні зберігати безпечний стан при таких типах збоїв: [призначення: список типів збоїв ФБО]. FRU_FLT.1.1: ФБО повинні забезпечувати виконання [призначення: список можливостей ОО], коли виникають такі збої [призначення: список типів збоїв]	У списках типів збоїв та можливостей ОО функціональних елементів FPT_FLS.1.1 та FRU_FLT.1.1 наявні всі типи відмов всіх компонентів ОЕ. Список можливостей ОО, виконання яких забезпечується при виникненні певних збоїв, та список відповідних типів збоїв функціонального елемента FRU_FLT.1.1 забезпечують виконання вимог політики ФПБ щодо того, щоб відмова одного захищеного компонента не призводила до недоступності всіх послуг, а в гіршому випадку проявлялася у зниженні характеристик обслуговування
	Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів ОЕ		
	Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги		
	Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування		

	КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента	FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAA.1.1: ФБО повинні бути здатними застосовувати набір правил моніторингу подій, що підлягають аудиту, та на підставі цих правил вказувати на можливе порушення ПБО	Правила моніторингу подій функціонального елемента FAU_SAA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, одержувати інформацію про відмову будь-якого захищеного компонента
ДС-3	Розробник повинен провести аналіз відмов компонентів ОЕ	FPT_FLS.1.1: ФБО повинні зберігати безпечний стан при таких типах збоїв: [призначення: список типів збоїв ФБО]. FRU_FLT.2.1: ФБО повинні забезпечувати виконання всіх можливостей ОО, коли виникають такі збої [призначення: список типів збоїв]	У списках типів збоїв та можливостей ОО функціональних елементів FPT_FLS.1.1 та FRU_FLT.2.1 наявні всі типи відмов всіх компонентів ОЕ. Список можливостей ОО, виконання яких забезпечується при виникненні певних збоїв, та список відповідних типів збоїв функціонального елемента FRU_FLT.2.1 забезпечують виконання вимог політики ФПБ щодо того, щоб відмова одного захищеного компонента не призводила до недоступності всіх послуг або до зниження характеристик обслуговування
	Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів ОЕ		
	Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги		
	Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування		
	КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного	FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі].	Правила моніторингу подій функціонального елемента FAU_SAA.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів

	компонента	FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAA.1.1: ФБО повинні бути здатними застосовувати набір правил моніторингу подій, що підлягають аудиту, та на підставі цих правил вказувати на можливе порушення ПБО	FMT_SMR.1.1 чи FMT_SMR.2.1, одержувати інформацію про відмову будь-якого захищеного компонента

9.3 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Гаряча заміна"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Гаряча заміна" наведено у таблиці 9.3.

Таблиця 9.3

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
ДЗ-1	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації ОЕ		Відповідні вимоги задоволені елементами довіри AVA_FLR.1.4C, AVA_FLR.2.4C, AVA_FLR.3.4C, визначеними стандартом ISO/IEC 15408-3
	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) ОЕ. Модернізація ОЕ не повинна призводити до необхідності ще раз проводити	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, здійснити модернізацію (upgrade) ОЕ, яка не призводить до необхідності ще раз проводити інсталяцію ОЕ або до переривання виконання КЗЗ функцій захисту. Функціональний елемент FMT_MOF.1.1 надає можливість користувачу,

	інсталяцію ОЕ або до переривання виконання КЗЗ функцій захисту	ролями. FMT_MOF.1.1: ФБО повинні надавати можливість [вибір: визначати режим виконання; вимикати, вмикати, модифікувати режим виконання] тільки [призначення: уповноважені ідентифіковані ролі]	асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити модернізацію (upgrade) ОЕ, яка не призводить до необхідності ще раз проводити інсталяцію ОЕ або до переривання виконання КЗЗ функцій захисту
ДЗ-2	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів ОЕ, які можуть бути замінені без переривання обслуговування		Відповідні вимоги задоволені елементами довіри AVA_FLR.1.4C, AVA_FLR.2.4C, AVA_FLR.3.4C, визначеними стандартом ISO/IEC 15408-3
	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MOF.1.1: ФБО повинні надавати можливість [вибір: визначати режим виконання; вимикати, вмикати, модифікувати режим виконання*]* тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, здійснити заміну будь-якого захищеного компонента ОЕ, у тому числі визначених у політиці ФПБ компонентів – без переривання обслуговування. Функціональний елемент FMT_MOF.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити заміну будь-якого захищеного компонента ОЕ, у тому числі визначених у політиці ФПБ компонентів – без переривання обслуговування
ДЗ-3	Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування		Відповідні вимоги задоволені елементами довіри AVA_FLR.1.4C, AVA_FLR.2.4C, AVA_FLR.3.4C, визначеними стандартом ISO/IEC 15408-3
	Адміністратор або користувачі, яким	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі	У списку функцій керування безпекою функціонального

	надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MOF.1.1: ФБО повинні надавати можливість [вибір: визначати режим виконання; вимикати, вмикати, модифікувати режим виконання*]* тільки [призначення: уповноважені ідентифіковані ролі]	елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, здійснити заміну будь-якого захищеного компонента ОЕ без переривання обслуговування. Функціональний елемент FMT_MOF.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити заміну будь-якого захищеного компонента ОЕ без переривання обслуговування

9.4 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Відновлення після збоїв"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Відновлення після збоїв" наведено у таблиці 9.4.

Таблиця 9.4

Рівень ФПБ	Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ	Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99	Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99
ДВ-1	Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов ОЕ і переривань обслуговування, після яких можливе повернення у відомий	FPT_RCV.1.1: Після [призначення: список збоїв/ переривань обслуговування] ФБО повинні переходити в режим аварійної підтримки, який надає можливість повернення ОО до безпечного стану	У списку збоїв/ переривань обслуговування функціонального елемента FPT_RCV.1.1 наявні всі типи відмов і переривань обслуговування, визначені у політиці ФПБ, після яких можливе повернення ОЕ у відомий захищений стан без порушення політики безпеки. Функціональний елемент FPT_RCV.1.1 забезпечує при виникненні відповідних збоїв/ переривань обслуговування

	захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція ОЕ		можливість переведення ОЕ до режиму аварійної підтримки, із якого повернути його до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Режим аварійної підтримки функціонального елемента FPT_RCV.1.1 забезпечує при виникненні відповідних збоїв/ переривань обслуговування можливість повернення ОЕ, за допомогою відповідних ручних процедур, у відомий захищений стан без порушення політики безпеки та необхідності повторної інсталяції
	Після відмови ОЕ або переривання обслуговування КЗЗ повинен перевести ОЕ до стану, із якого повернути його до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження		
	Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути ОЕ до нормального функціонування	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MOF.1.1: ФБО повинні надавати можливість [вибір: визначати режим виконання; вимикати, вмикати, модифікувати режим виконання*]* тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, за допомогою відповідних ручних процедур безпечним чином повернути ОЕ до нормального функціонування. Функціональний елемент FMT_MOF.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, за допомогою відповідних ручних процедур безпечним чином повернути ОЕ до нормального функціонування
ДВ-2 126	Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов ОЕ і	FPT_RCV.2.1: Якщо автоматичне відновлення після [призначення: список збоїв/ переривань обслуговування] неможливе, ФБО повинні переходити в режим	У списках збоїв/ переривань обслуговування функціональних елементів FPT_RCV.2.1 та FPT_RCV.2.2 наявні всі типи відмов і переривань обслуговування, після яких можливе повернення ОЕ у

	переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція ОЕ	аварійної підтримки, який надає можливість повернення ОО до безпечного стану. FPT_RCV.2.2: Для [призначення: список збоїв/ переривань обслуговування] ФБО повинні забезпечити повернення ОО до безпечного стану з використанням автоматичних процедур	відомий захищений стан без порушення політики безпеки, визначені у політиці ФПБ. Функціональний елемент FPT_RCV.2.1 забезпечує, при виникненні відповідних збоїв/ переривань обслуговування та у випадку, якщо не можуть бути використані автоматизовані процедури для повернення ОЕ до нормального функціонування, можливість переведення ОЕ до режиму аварійної підтримки, із якого повернути його до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Режим аварійної підтримки функціонального елемента FPT_RCV.2.1 забезпечує при виникненні відповідних збоїв/ переривань обслуговування можливість повернення ОЕ, за допомогою відповідних ручних процедур, у відомий захищений стан без порушення політики безпеки та необхідності повторної інсталяції. Функціональний елемент FPT_RCV.2.2 забезпечує при виникненні відповідних збоїв/ переривань обслуговування можливість повернення ОЕ за допомогою відповідних автоматизованих процедур до нормального функціонування
	Після відмови ОЕ або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення ОЕ до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути ОЕ до нормального функціонування		
	Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести ОЕ до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження		

	Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути ОЕ до нормального функціонування	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MOF.1.1: ФБО повинні надавати можливість [вибір: визначати режим виконання; вимикати, вмикати, модифікувати режим виконання*]* тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, за допомогою відповідних ручних процедур безпечним чином повернути ОЕ до нормального функціонування. Функціональний елемент FMT_MOF.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, за допомогою відповідних ручних процедур безпечним чином повернути ОЕ до нормального функціонування
ДВ-3	Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов ОЕ і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція ОЕ	FPT_RCV.3.1: Якщо автоматичне відновлення після [призначення: список збоїв/ переривань обслуговування] неможливе, ФБО повинні переходити в режим аварійної підтримки, який надає можливість повернення ОО до безпечного стану. FPT_RCV.3.2: Для [призначення: список збоїв/ переривань обслуговування] ФБО повинні забезпечити повернення ОО до безпечного стану з використанням автоматичних процедур	У списках збоїв/ переривань обслуговування функціональних елементів FPT_RCV.3.1 та FPT_RCV.3.2 наявні всі типи відмов і переривань обслуговування, після яких можливе повернення ОЕ у відомий захищений стан без порушення політики безпеки, визначені у політиці ФПБ. Функціональний елемент FPT_RCV.3.1 забезпечує при виникненні відповідних збоїв/ переривань обслуговування та у випадку, якщо не можуть бути використані автоматизовані процедури для повернення ОЕ до нормального функціонування, можливість переведення ОЕ до режиму аварійної підтримки, із якого повернути його до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Режим аварійної підтримки функціонального елемента FPT_RCV.3.1 забезпечує при виникненні відповідних збоїв/ переривань обслуговування можливість повернення ОЕ за
	Після будь-якої відмови ОЕ або переривання обслуговування, що не призводить до необхідності заново інсталювати ОЕ,		

	КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути ОЕ до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування		допомогою відповідних ручних процедур у відомий захищений стан без порушення політики безпеки та необхідності повторної інсталяції. Функціональний елемент FPT_RCV.3.2 забезпечує при виникненні відповідних збоїв/ переривань обслуговування можливість повернення ОЕ за допомогою відповідних автоматизованих процедур до нормального функціонування або в гіршому випадку функціонування в режимі з погіршеними характеристиками обслуговування
	Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести ОЕ до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження		
	Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути ОЕ з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_MOF.1.1: ФБО повинні надавати можливість [вибір: визначати режим виконання; вимикати, вмикати, модифікувати режим виконання*]* тільки [призначення: уповноважені ідентифіковані ролі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, за допомогою відповідних ручних процедур безпечним чином повернути ОЕ з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування. Функціональний елемент FMT_MOF.1.1 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, за допомогою відповідних ручних процедур безпечним чином повернути ОЕ з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування

10 Відомості щодо відповідності функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам критеріїв спостережності, встановленим НД ТЗІ 2.5-004-99

У підрозділах цього розділу у таблицях 10.1 – 10.9 викладено відомості щодо відповідності функціональних елементів функціональних компонентів безпеки відповідних функціональних класів безпеки, встановлених стандартом ISO/IEC 15408, вимогам критеріїв спостережності, встановленим НД ТЗІ 2.5-004-99, для різних ФПБ. Відомості викладено у табличному вигляді, окремо для кожної ФПБ та її рівнів, визначених НД ТЗІ 2.5-004-99, із зазначенням у кожній таблиці: рівня ФПБ; вимог НД ТЗІ 2.5-004-99 щодо політики відповідної ФПБ відповідного рівня; вимог стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99; необхідних умов, за яких у процесі виконання зіставлення функціональних компонентів безпеки згідно з ISO/IEC 15408, реалізованих у певному ЗТЗІ від НСД, з вимогами НД ТЗІ 2.5-004-99, можна приймати рішення про те, що певна сукупність функціональних елементів функціональних компонентів безпеки задовольняє відповідні вимоги НД ТЗІ 2.5-004-99.

10.1 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Реєстрація"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Реєстрація" наведено у таблиці 10.1.

Таблиця 10.1

Рівень ФПБ	Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ	Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99	Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99
НР-1	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються	FAU_GEN.1.1: ФБО повинні бути здатними генерувати запис аудита для таких події, що потенційно підлягають аудиту: а) запуск і завершення виконання функцій аудита; б) усі події, що підлягають аудиту, на [вибір: мінімальний, базовий, деталізований, невизначений] рівні аудита; в) [призначення: інші спеціально визначені події, що потенційно підлягають аудиту]	У списку подій аудита функціонального елемента FAU_GEN.1.1 наявні всі події, що мають безпосереднє відношення до безпеки, визначені у політиці ФПБ
	КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє		

	відношення до безпеки		
	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.	FAU_GEN.1.2: ФБО повинні реєструвати в кожному записі аудита мінімум таку інформацію: а) дата і час події, тип події, ідентифікатор суб'єкта і результат події (успішний або неуспішний); б) для кожного типу подій, що потенційно підлягають аудиту, із числа визначених у функціональних компонентах, які включені до ПЗ/ ЗБ, [призначення: *інша інформація, що стосується аудита].* FAU_GEN.2.1: ФБО повинні бути здатними асоціювати кожну подію, що потенційно піддається аудиту, з ідентифікатором користувача, який був ініціатором цієї події	У переліку інформації, яка реєструється функціональним елементом FAU_GEN.1.2 у записах аудита, для кожної події наявна інформація про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події, а також інформація, достатня для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події
	КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту	FPT_ITA.1.1: ФБО повинні забезпечувати доступність [призначення: список типів даних ФБО] для віддаленого довіреного продукту інформаційних технологій (ІТ) у межах [призначення: задана метрика доступності] при виконанні таких умов [призначення: умови забезпечення доступності]. FPT_ITI.1.1, FPT_ITI.2.1: ФБО повинні надавати можливість виявляти модифікацію будь-яких даних ФБО при передачі між ФБО і віддаленим довіреним продуктом ІТ в межах такої метрики [призначення: метрика модифікації]	Функціональні елементи FPT_ITA.1.1, FPT_ITI.1.1, FPT_ITI.2.1 забезпечують можливість передачі інформації, зареєстрованої у записах аудита функціональним елементом FAU_GEN.1.2, до інших систем згідно з заданими правилами, а також захист переданих даних від несанкціонованої модифікації
НР-2	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються	FAU_GEN.1.1: ФБО повинні бути здатними генерувати запис аудита для таких події, що потенційно підлягають аудиту: а) запуск і завершення виконання функцій аудита; б) усі події, що підлягають аудиту, на [вибір: мінімальний, базовий, деталізований, невизначений] рівні аудита; в) [призначення: інші спеціально визначені події, що потенційно підлягають аудиту]	У списку подій аудита функціонального елемента FAU_GEN.1.1 наявні всі події, що мають безпосереднє відношення до безпеки, визначені у політиці ФПБ
	КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє		

	відношення до безпеки		
	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події	FAU_GEN.1.2: ФБО повинні реєструвати в кожному записі аудита мінімум таку інформацію: а) дата і час події, тип події, ідентифікатор суб'єкта і результат події (успішний або неуспішний); б) для кожного типу подій, що потенційно підлягають аудиту, із числа визначених у функціональних компонентах, які включені до ПЗ/ ЗБ, [призначення: *інша інформація, що стосується аудита].* FAU_GEN.2.1: ФБО повинні бути здатними асоціювати кожну подію, що потенційно піддається аудиту, з ідентифікатором користувача, який був ініціатором цієї події	У переліку інформації, яка реєструється функціональним елементом FAU_GEN.1.2 у записах аудита, для кожної події наявна інформація про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події, а також інформація, достатня для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події
	КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування	FAU_STG.1.1, FAU_STG.2.1: ФБО повинні захищати збережені записи аудита від несанкціонованого видалення. FAU_STG.1.2, FAU_STG.2.2: ФБО повинні бути здатними [вибір: запобігати, виявляти] несанкціоновану модифікацію збережених записів аудита в журналі аудита	Функціональні елементи FAU_STG.1.1 та FAU_STG.1.2 або FAU_STG.2.1 та FAU_STG.2.2 забезпечують захист збережених журналів реєстрації від несанкціонованого доступу з метою їх модифікації або руйнування
	Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAR.1.1: ФБО повинні надавати [призначення: уповноважені користувачі] можливість читати [призначення: список інформації аудита] із записів аудита. FAU_SAR.1.2: ФБО повинні представляти записи аудита у	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, здійснити перегляд і аналіз журналу реєстрації. Функціональні елементи FAU_SAR.1.1 та FAU_SAR.1.2 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити перегляд і аналіз журналу реєстрації

		вигляді, що дозволяє користувачу сприймати інформацію, яка в них міститься	
НР-3	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються	FAU_GEN.1.1: ФБО повинні бути здатними генерувати запис аудита для таких події, що потенційно підлягають аудиту: а) запуск і завершення виконання функцій аудита; б) усі події, що підлягають аудиту, на [вибір: мінімальний, базовий, деталізований, невизначений] рівні аудита; в) [призначення: інші спеціально визначені події, що потенційно підлягають аудиту]	У списку подій аудита функціонального елемента FAU_GEN.1.1 наявні всі події, що мають безпосереднє відношення до безпеки, визначені у політиці ФПБ
	КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки		
	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події	FAU_GEN.1.2: ФБО повинні реєструвати в кожному записі аудита мінімум таку інформацію: а) дата і час події, тип події, ідентифікатор суб’єкта і результат події (успішний або неуспішний); б) для кожного типу подій, що потенційно підлягають аудиту, із числа визначених у функціональних компонентах, які включені до ПЗ/ ЗБ, [призначення: *інша інформація, що стосується аудита].* FAU_GEN.2.1: ФБО повинні бути здатними асоціювати кожну подію, що потенційно піддається аудиту, з ідентифікатором користувача, який був ініціатором цієї події	У переліку інформації, яка реєструється функціональним елементом FAU_GEN.1.2 у записах аудита, для кожної події наявна інформація про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події, а також інформація, достатня для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події
	КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування	FAU_STG.1.1, FAU_STG.2.1: ФБО повинні захищати збережені записи аудита від несанкціонованого видалення. FAU_STG.1.2, FAU_STG.2.2: ФБО повинні бути здатними [вибір: запобігати, виявляти] несанкціоновану модифікацію збережених записів аудита в журналі аудита	Функціональні елементи FAU_STG.1.1 та FAU_STG.1.2 або FAU_STG.2.1 та FAU_STG.2.2 забезпечують захист збережених записів аудита від несанкціонованого доступу з метою їх модифікації або руйнування
	Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що

	своєму розпорядженні засоби перегляду і аналізу журналу реєстрації	надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAR.1.1: ФБО повинні надавати [призначення: уповноважені користувачі] можливість читати [призначення: список інформації аудита] із записів аудита. FAU_SAR.1.2: ФБО повинні представляти записи аудита у вигляді, що дозволяє користувачу сприймати інформацію, яка в них міститься FAU_SAA.1.1: ФБО повинні бути здатними застосовувати набір правил моніторингу подій, що підлягають аудиту, і вказувати на можливе порушення ПБО на основі цих правил. FAU_SAA.1.2: ФБО повинні реалізовувати такі правила при моніторингу подій, що підлягають аудиту: а) накопичення або об'єднання відомих [призначення: підмножина визначених подій, що потенційно підлягають аудиту] б) [призначення: *інші правила].* FAU_SAA.2.1: ФБО повинні бути здатними супроводжувати профілі використання системи, де кожен окремий профіль являє собою відомі шаблони передісторії використання, що виконувалась учасниками [призначення: специфікація цільової групи профілю]. FAU_SAA.2.2: ФБО повинні бути здатними супроводжувати рейтинг підозрілої активності для кожного користувача, чиї дії відображені у профілі, де рейтинг підозрілої активності відображає ступінь неузгодженості дій, що виконуються користувачем, із встановленими шаблонами використання, визначеними у профілі.	дозволяють користувачам, асоційованим із певними ролями, здійснити перегляд і аналіз журналу реєстрації, а також неруйнівні дії щодо припинення повторення небезпечних подій. Функціональні елементи FAU_SAR.1.1 та FAU_SAR.2.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити перегляд і аналіз журналу реєстрації. Правила моніторингу подій функціональних елементів FAU_SAA.1.1, FAU_SAA.1.2 забезпечують контроль одиничних або повторюваних реєстраційних подій, які можуть свідчити про прямі (істотні) порушення політики безпеки. Функціональні елементи FAU_SAA.2.1 – FAU_SAA.2.3 та FAU_ARP.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, одержати інформацію про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій
	КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій		

		FAU_SAA.2.3: ФБО повинні бути здатними вказувати на очікуване порушення ФБО, коли рейтинг підозрілої активності користувача перевищує такі порогові умови [призначення: умови, при яких ФБО повідомляють про аномальні дії]. FAU_ARP.1.1: ФБО повинні вжити [призначення: список найменш руйнівних дій] при виявленні можливого порушення безпеки	
НР-4	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються	FAU_GEN.1.1: ФБО повинні бути здатними генерувати запис аудита для таких події, що потенційно підлягають аудиту: а) запуск і завершення виконання функцій аудита; б) усі події, що підлягають аудиту, на [вибір: мінімальний, базовий, деталізований, невизначений] рівні аудита; в) [призначення: інші спеціально визначені події, що потенційно підлягають аудиту]. FAU_SEL.1.1: ФБО повинні бути здатними до залучення подій, що потенційно підлягають аудиту, до сукупності подій, що підлягають аудиту, або до їх вилучення із цієї сукупності за такими атрибутами: а) [вибір: ідентифікатор об’єкта, ідентифікатор користувача, ідентифікатор суб’єкта, ідентифікатор вузла мережі, тип події]; б) [призначення: список додаткових атрибутів, на яких ґрунтується вибірковість аудита]	У списку подій аудита функціонального елемента FAU_GEN.1.1 наявні всі події, що мають безпосереднє або непряме відношення до безпеки, визначені у політиці ФПБ
	КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки		
	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або	FAU_GEN.1.2: ФБО повинні реєструвати в кожному записі аудита мінімум таку інформацію: а) дата і час події, тип події, ідентифікатор суб’єкта і результат події (успішний або неуспішний); б) для кожного типу подій, що потенційно підлягають аудиту, із числа визначених у функціональних компонентах, які включені до ПЗ/ ЗБ, [призначення: *інша інформація, що стосується аудита].* FAU_GEN.2.1: ФБО повинні бути здатними асоціювати кожну	У переліку інформації, яка реєструється функціональним елементом FAU_GEN.1.2 у записах аудита, для кожної події наявна інформація про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події, а також інформація, достатня для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події

	об'єкта, що мали відношення до кожної зареєстрованої події	подію, що потенційно піддається аудиту, з ідентифікатором користувача, який був ініціатором цієї події	
	КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування	FAU_STG.1.1, FAU_STG.2.1: ФБО повинні захищати збережені записи аудита від несанкціонованого видалення. FAU_STG.1.2, FAU_STG.2.2: ФБО повинні бути здатними [вибір: запобігати, виявляти] несанкціоновану модифікацію збережених записів аудита в журналі аудита	Функціональні елементи FAU_STG.1.1 та FAU_STG.1.2 або FAU_STG.2.1 та FAU_STG.2.2 забезпечують захист збережених записів аудита від несанкціонованого доступу з метою їх модифікації або руйнування
	Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAR.1.1: ФБО повинні надавати [призначення: уповноважені користувачі] можливість читати [призначення: список інформації аудита] із записів аудита. FAU_SAR.1.2: ФБО повинні представляти записи аудита у вигляді, що дозволяє користувачу сприймати інформацію, яка в них міститься FAU_SAA.1.1: ФБО повинні бути здатними застосовувати набір правил моніторингу подій, що підлягають аудиту, і вказувати на можливе порушення ПБО на основі цих правил. FAU_SAA.1.2: ФБО повинні реалізовувати такі правила при моніторингу подій, що підлягають аудиту: а) накопичення або об’єднання відомих [призначення: підмножина визначених подій, що потенційно підлягають аудиту];	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, здійснити перегляд і аналіз журналу реєстрації. Функціональні елементи FAU_SAR.1.1 та FAU_SAR.1.2 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити перегляд і аналіз журналу реєстрації. Правила моніторингу подій функціональних елементів FAU_SAA.1.1, FAU_SAA.1.2 забезпечують контроль одиничних або повторюваних реєстраційних подій, які можуть свідчити про прямі (істотні) порушення політики безпеки. Функціональні елементи FAU_SAA.2.1 – FAU_SAA.2.3 та FAU_ARP.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, одержати інформацію про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити
	КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки ОЕ. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій		

		б) [призначення: *інші правила].* FAU_SAA.2.1: ФБО повинні бути здатними супроводжувати профілі використання системи, де кожен окремий профіль являє собою відомі шаблони передісторії використання, що виконувалась учасниками [призначення: специфікація цільової групи профілю]. FAU_SAA.2.2: ФБО повинні бути здатними супроводжувати рейтинг підозрілої активності для кожного користувача, чиї дії відображені у профілі, де рейтинг підозрілої активності відображає ступінь неузгодженості дій, що виконуються користувачем, із встановленими шаблонами використання, визначеними у профілі. FAU_SAA.2.3: ФБО повинні бути здатними вказувати на очікуване порушення ФБО, коли рейтинг підозрілої активності користувача перевищує такі порогові умови [призначення: умови, при яких ФБО повідомляють про аномальні дії]. FAU_ARP.1.1: ФБО повинні вжити [призначення: список найменш руйнівних дій] при виявленні можливого порушення безпеки	неруйнівні дії щодо припинення повторення цих подій
НР-5	Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки	FAU_GEN.1.1: ФБО повинні бути здатними генерувати запис аудита для таких події, що потенційно підлягають аудиту: а) запуск і завершення виконання функцій аудита; б) усі події, що підлягають аудиту, на [вибір: мінімальний, базовий, деталізований, невизначений] рівні аудита; в) [призначення: інші спеціально визначені події, що потенційно підлягають аудиту]. FAU_SEL.1.1: ФБО повинні бути здатними до залучення подій, що потенційно підлягають аудиту, до сукупності подій, що підлягають аудиту, або до їх вилучення із цієї сукупності за такими атрибутами: а) [вибір: ідентифікатор об'єкта,	У списку подій аудита функціонального елемента FAU_GEN.1.1 наявні всі події, що мають безпосереднє або непряме відношення до безпеки, визначені у політиці ФПБ

		ідентифікатор користувача, ідентифікатор суб’єкта, ідентифікатор вузла мережі, тип події]; б) [призначення: список додаткових атрибутів, на яких ґрунтується вибірковість аудита]	
	Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події	FAU_GEN.1.2: ФБО повинні реєструвати в кожному записі аудита мінімум таку інформацію: а) дата і час події, тип події, ідентифікатор суб’єкта і результат події (успішний або неуспішний); б) для кожного типу подій, що потенційно підлягають аудиту, із числа визначених у функціональних компонентах, які включені до ПЗ/ ЗБ, [призначення: *інша інформація, що стосується аудита].* FAU_GEN.2.1: ФБО повинні бути здатними асоціювати кожну подію, що потенційно піддається аудиту, з ідентифікатором користувача, який був ініціатором цієї події	У переліку інформації, яка реєструється функціональним елементом FAU_GEN.1.2 у записах аудита, для кожної події наявна інформація про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події, а також інформація, достатня для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події
	КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування	FAU_STG.1.1, FAU_STG.2.1: ФБО повинні захищати збережені записи аудита від несанкціонованого видалення. FAU_STG.1.2, FAU_STG.2.2: ФБО повинні бути здатними [вибір: запобігати, виявляти] несанкціоновану модифікацію збережених записів аудита в журналі аудита	Функціональні елементи FAU_STG.1.1 та FAU_STG.1.2 або FAU_STG.2.1 та FAU_STG.2.2 забезпечують захист збережених записів аудита від несанкціонованого доступу з метою їх модифікації або руйнування
	Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації	FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FAU_SAR.1.1: ФБО повинні надавати [призначення: уповноважені користувачі]	У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні функції, що дозволяють користувачам, асоційованим із певними ролями, здійснити перегляд і аналіз журналу реєстрації. Функціональні елементи FAU_SAR.1.1 та FAU_SAR.2.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, здійснити перегляд і аналіз журналу
	КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть		

	свідчити про прямі (істотні) порушення політики безпеки ОЕ. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій	можливість читати [призначення: список інформації аудита] із записів аудита. FAU_SAR.1.2: ФБО повинні представляти записи аудита у вигляді, що дозволяє користувачу сприймати інформацію, яка в них міститься FAU_SAA.1.1: ФБО повинні бути здатними застосовувати набір правил моніторингу подій, що підлягають аудиту, і вказувати на можливе порушення ПБО на основі цих правил. FAU_SAA.1.2: ФБО повинні реалізовувати такі правила при моніторингу подій, що підлягають аудиту: а) накопичення або об'єднання відомих [призначення: підмножина визначених подій, що потенційно підлягають аудиту]; б) [призначення: *інші правила].* FAU_SAA.2.1: ФБО повинні бути здатними супроводжувати профілі використання системи, де кожен окремий профіль являє собою відомі шаблони передісторії використання, що виконувалась учасниками [призначення: специфікація цільової групи профілю]. FAU_SAA.2.2: ФБО повинні бути здатними супроводжувати рейтинг підозрілої активності для кожного користувача, чиї дії відображені у профілі, де рейтинг підозрілої активності відображає ступінь неузгодженості дій, що виконуються користувачем, із встановленими шаблонами використання, визначеними у профілі. FAU_SAA.2.3: ФБО повинні бути здатними вказувати на очікуване порушення ФБО, коли рейтинг підозрілої активності користувача перевищує такі порогові умови [призначення: умови, при яких ФБО повідомляють про аномальні дії]. FAU_SAA.3.1: ФБО повинні бути здатними супроводжувати внутрішнє представлення таких характерних подій [призначення: підмножина подій системи], які	реєстрації. Правила моніторингу подій функціональних елементів FAU_SAA.1.1, FAU_SAA.1.2 забезпечують контроль одиничних або повторюваних реєстраційних подій, які можуть свідчити про прямі (істотні) порушення політики безпеки, у реальному часі. Функціональні елементи FAU_SAA.2.1 – FAU_SAA.2.3, FAU_SAA.3.1 – FAU_SAA.3.3, FAU_SAA.4.1 – FAU_SAA.4.3 та FAU_ARP.1.1 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, у реальному часі одержати інформацію про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій
	КЗЗ має бути здатним виявляти і аналізувати несанкціоновані дії в реальному часі		

		можуть вказувати на порушення ПБО. FAU_SAA.3.2: ФБО повинні бути здатними порівнювати характерні події із записами показників функціонування системи, одержаних при обробленні [призначення: інформація, що використовується для визначення показників функціонування системи]. FAU_SAA.3.3: ФБО повинні бути здатними вказувати на очікуване порушення ФБО, коли подія системи відповідає характерній події, що вказує на можливе порушення ПБО. FAU_SAA.4.1: ФБО повинні бути здатними супроводжувати внутрішнє представлення таких послідовностей подій відомих сценаріїв проникнення [призначення: список послідовностей подій системи, збіг яких характерний для відомих сценаріїв проникнення] і таких характерних подій [призначення: підмножина подій системи], які можуть вказувати на порушення ПБО. FAU_SAA.4.2: ФБО повинні бути здатними порівнювати характерні події і послідовності подій із записами показників функціонування системи, одержаних при обробленні [призначення: інформація, що використовується для визначення показників функціонування системи]. FAU_SAA.4.3: ФБО повинні бути здатними вказувати на очікуване порушення ФБО, коли показники функціонування системи відповідають характерній події або послідовності подій, що вказують на можливе порушення ПБО. FAU_ARP.1.1: ФБО повинні вжити [призначення: список найменш руйнівних дій] при виявленні можливого порушення безпеки	

10.2 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Ідентифікація і автентифікація"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Ідентифікація і автентифікація" наведено у таблиці 10.2.

Таблиця 10.2

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
НИ-1	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ	FIA_ATD.1.1: ФБО повинні підтримувати для кожного користувача такий список атрибутів безпеки: [призначення: список атрибутів безпеки]. FIA_USB.1.1: ФБО повинні асоціювати відповідні атрибути безпеки користувача із суб'єктами, що діють від імені цього користувача: [призначення: список атрибутів безпеки користувача]. FIA_USB.1.2: ФБО повинні реалізовувати такі правила початкової асоціації атрибутів безпеки користувачів, асоційованих із суб'єктами, що діють від імені користувачів: [призначення: правила початкової асоціації атрибутів]. FIA_USB.1.3: ФБО повинні реалізовувати такі правила керування змінами атрибутів безпеки користувачів, асоційованих із суб'єктами, що діють від імені користувачів: [призначення: правила зміни атрибутів]	Атрибути безпеки функціональних елементів FIA_ATD.1.1, FIA_USB.1.1, правила початкової асоціації та керування зміною атрибутів функціональних елементів FIA_USB.1.2, FIA_USB.1.3 забезпечують однозначну ідентифікацію кожного користувача для всіх типів користувачів, на які поширюється політика ФПБ
	Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням	FIA_UID.2.1: ФБО повинні вимагати, щоб кожний користувач був успішно ідентифікований до дозволу будь-якої дії, що виконується за посередництва ФБО від імені цього користувача.	Поєднувані механізми автентифікації функціонального елемента FIA_UAU.5.1 та правила поєднання механізмів та забезпечення автентифікації

	захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача	FIA_UAU.2.1: ФБО повинні вимагати, щоб кожний користувач був успішно автентифікований до дозволу будь-якої дії, що виконується за посередництва ФБО від імені цього користувача. FIA_UAU.5.1: ФБО повинні надавати [призначення: список поєднуваних механізмів автентифікації] для підтримки автентифікації користувача. FIA_UAU.5.2: ФБО повинні автентифікувати будь-який наданий ідентифікатор користувача згідно [призначення: *правила, що описують, як поєднання механізмів автентифікації забезпечує автентифікацію]*	функціонального елемента FIA_UAU.5.2 забезпечують одержання від зовнішнього джерела автентифікованого ідентифікатора кожного користувача для всіх типів користувачів, на які поширюється політика ФПБ
НИ-2	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ	FIA_ATD.1.1: ФБО повинні підтримувати для кожного користувача такий список атрибутів безпеки: [призначення: список атрибутів безпеки]. FIA_USB.1.1: ФБО повинні асоціювати відповідні атрибути безпеки користувача із суб'єктами, що діють від імені цього користувача: [призначення: список атрибутів безпеки користувача]. FIA_USB.1.2: ФБО повинні реалізовувати такі правила початкової асоціації атрибутів безпеки користувачів, асоційованих із суб'єктами, що діють від імені користувачів: [призначення: правила початкової асоціації атрибутів]. FIA_USB.1.3: ФБО повинні реалізовувати такі правила керування змінами атрибутів безпеки користувачів, асоційованих із суб'єктами, що діють від імені користувачів: [призначення: правила зміни атрибутів].	Атрибути безпеки функціональних елементів FIA_ATD.1.1, FIA_USB.1.1, правила початкової асоціації та керування зміною атрибутів функціональних елементів FIA_USB.1.2, FIA_USB.1.3 забезпечують однозначну ідентифікацію кожного користувача для всіх типів користувачів, на які поширюється політика ФПБ
	Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен	FIA_UID.2.1: ФБО повинні вимагати, щоб кожний користувач був успішно ідентифікований до дозволу будь-якої дії, що виконується за посередництва ФБО від імені	Поєднувані механізми автентифікації функціонального елемента FIA_UAU.5.1 та правила поєднання механізмів та забезпечення

	автентифікувати цього користувача з використанням захищеного механізму	цього користувача. FIA_UAU.2.1: ФБО повинні вимагати, щоб кожний користувач був успішно автентифікований до дозволу будь-якої дії, що виконується за посередництва ФБО від імені цього користувача. FIA_UAU.5.1: ФБО повинні надавати [призначення: список поєднуваних механізмів автентифікації] для підтримки автентифікації користувача. FIA_UAU.5.2: ФБО повинні автентифікувати будь-який наданий ідентифікатор користувача згідно [призначення: *правила, що описують, як поєднання механізмів автентифікації забезпечує автентифікацію]*	автентифікації функціонального елемента FIA_UAU.5.2 забезпечують автентифікацію кожного користувача для всіх типів користувачів, на які поширюється політика ФПБ, з використанням захищеного механізму одного типу
	КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування	FPT_ITT.1.1, FPT_ITT.2.1: ФБО повинні захищати свої дані від [вибір: розкриття, модифікація] при їх передачі між окремими частинами ФБО	Функціональні елементи FPT_ITT.1.1, FPT_ITT.2.1 забезпечують захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування
НИ-3	Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ	FIA_ATD.1.1: ФБО повинні підтримувати для кожного користувача такий список атрибутів безпеки: [призначення: список атрибутів безпеки]. FIA_USB.1.1: ФБО повинні асоціювати відповідні атрибути безпеки користувача із суб'єктами, що діють від імені цього користувача: [призначення: список атрибутів безпеки користувача]. FIA_USB.1.2: ФБО повинні реалізовувати такі правила початкової асоціації атрибутів безпеки користувачів, асоційованих із суб'єктами, що діють від імені користувачів: [призначення: правила початкової асоціації атрибутів]. FIA_USB.1.3: ФБО повинні реалізовувати такі правила керування змінами атрибутів безпеки користувачів, асоційованих із суб'єктами, що	Атрибути безпеки функціональних елементів FIA_ATD.1.1, FIA_USB.1.1, правила початкової асоціації та керування зміною атрибутів функціональних елементів FIA_USB.1.2, FIA_USB.1.3 забезпечують однозначну ідентифікацію кожного користувача для всіх типів користувачів, на які поширюється політика ФПБ

		діють від імені користувачів: [призначення: правила зміни атрибутів]	
	Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищених механізмів двох або більше типів	FIA_UID.2.1: ФБО повинні вимагати, щоб кожний користувач був успішно ідентифікований до дозволу будь-якої дії, що виконується за посередництва ФБО від імені цього користувача. FIA_UAU.2.1: ФБО повинні вимагати, щоб кожний користувач був успішно автентифікований до дозволу будь-якої дії, що виконується за посередництва ФБО від імені цього користувача. FIA_UAU.5.1: ФБО повинні надавати [призначення: список поєднуваних механізмів автентифікації] для підтримки автентифікації користувача. FIA_UAU.5.2: ФБО повинні автентифікувати будь-який наданий ідентифікатор користувача згідно з [призначення: *правила, що описують, як поєднання механізмів автентифікації забезпечує автентифікацію]*	Поєднувані механізми автентифікації функціонального елемента FIA_UAU.5.1 та правила поєднання механізмів та забезпечення автентифікації функціонального елемента FIA_UAU.5.2 забезпечують автентифікацію кожного користувача для всіх типів користувачів, на які поширюється політика ФПБ, з використанням захищених механізмів двох або більше типів
	КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування	FPT_ITT.1.1, FPT_ITT.2.1: ФБО повинні захищати свої дані від [вибір: розкриття, модифікація] при їх передачі між окремими частинами ФБО	Функціональні елементи FPT_ITT.1.1, FPT_ITT.2.1 забезпечують захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування

10.3 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Достовірний канал"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Достовірний канал" наведено у таблиці 10.3.

Таблиця 10.3

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
НК-1	Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	FTP_TRP.1.1: ФБО повинні надавати маршрут зв’язку між собою та *[вибір:* віддалений, локальний] користувачем, який логічно відрізняється від інших маршрутів зв’язку і забезпечує впевнену ідентифікацію його початку та кінця, а також захист переданих даних від модифікації або розкриття. FTP_TRP.1.2: ФБО повинні дозволяти *[вибір:* ФБО, локальні користувачі, віддалені користувачі] ініціювати зв’язок через довірений маршрут. FTP_TRP.1.3: ФБО повинні вимагати використання довіреного маршруту для *[вибір:* початкова автентифікація користувача, *[інші послуги, для яких потрібний довірений маршрут*]]	Функціональні елементи FTP_TRP.1.1 – FTP_TRP.1.3 забезпечують надання довіреного маршруту між користувачем та ФБО і вимагають його використання при початковій автентифікації для всіх типів користувачів, на які поширюється політика ФПБ "Ідентифікація і автентифікація" рівня НИ-2 або НИ-3
НК-2	Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/ КЗЗ або КЗЗ/ користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ	FTP_TRP.1.1: ФБО повинні надавати маршрут зв’язку між собою та *[вибір:* віддалений, локальний] користувачем, який логічно відрізняється від інших маршрутів зв’язку і забезпечує впевнену ідентифікацію його початку та кінця, а також захист переданих даних від модифікації або розкриття. FTP_TRP.1.2: ФБО повинні дозволяти *[вибір:* ФБО, локальні користувачі, віддалені користувачі] ініціювати зв’язок через довірений маршрут. FTP_TRP.1.3: ФБО повинні вимагати використання довіреного маршруту для *[вибір:* початкова автентифікація користувача, *[інші послуги, для яких потрібний довірений маршрут*]]	Функціональні елементи FTP_TRP.1.1 – FTP_TRP.1.3 забезпечують надання довіреного маршруту між користувачем та ФБО та вимагають його використання при початковій автентифікації для всіх типів користувачів, на які поширюється політика ФПБ "Ідентифікація і автентифікація" рівня НИ-2 або НИ-3. Функціональні елементи FTP_TRP.1.1 – FTP_TRP.1.3 забезпечують надання довіреного маршруту між ФБО та користувачем та

	Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача		надають можливість його використання для всіх типів користувачів, на які поширюється політика ФПБ, тільки після позитивного підтвердження готовності до обміну з боку користувача

10.4 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Розподіл обов'язків"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Розподіл обов'язків" наведено у таблиці 10.4.

Таблиця 10.4

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
НО-1	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції	FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	У переліку уповноважених ідентифікованих ролей функціональних елементів FMT_SMR.1.1, FMT_SMR.2.1 наявні ролі адміністратора і звичайного користувача, визначені у політиці ФПБ. У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні всі функції, притаманні ролям адміністратора і звичайного користувача, визначені у політиці ФПБ
	Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття ним цієї ролі	FMT_SMR.3.1: ФБО повинні вимагати явного запиту для прийняття таких ролей [призначення: *список ролей]*	У списку ролей функціонального елемента FMT_SMR.3.1 наявні ролі адміністратора і звичайного користувача, визначені у політиці ФПБ
НО-2	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції	FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі	У переліку уповноважених ідентифікованих ролей функціональних елементів FMT_SMR.1.1, FMT_SMR.2.1 наявні мінімум дві адміністративні ролі, а також роль звичайного користувача, визначені у політиці ФПБ. У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1

	Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі	функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	наявні всі функції, притаманні адміністративним ролям і ролі звичайного користувача, визначені у політиці ФПБ
	Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття ним цієї ролі	FMT_SMR.3.1: ФБО повинні вимагати явного запиту для прийняття таких ролей [призначення: *список ролей]*	У списку ролей функціонального елемента FMT_SMR.3.1 наявні адміністративні ролі і роль звичайного користувача, визначені у політиці ФПБ
НО-3	Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції	FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями. FMT_SMF.1.1: ФБО повинні бути здатними виконувати такі функції керування безпекою: [призначення: список функцій керування безпекою, що надаються ФБО]	У переліку уповноважених ідентифікованих ролей функціональних елементів FMT_SMR.1.1, FMT_SMR.2.1 наявні мінімум дві адміністративні ролі, а також множина ролей користувачів, визначені у політиці ФПБ. У списку функцій керування безпекою функціонального елемента FMT_SMF.1.1 наявні всі функції, притаманні адміністративним ролям і ролям звичайних користувачів, визначені у політиці ФПБ
	Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі		

	Політика розподілу обов'язків повинна визначати множину ролей користувачів		
	Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття ним цієї ролі	FMT_SMR.3.1: ФБО повинні вимагати явного запиту для прийняття таких ролей [призначення: *список ролей]*	У списку ролей функціонального елемента FMT_SMR.3.1 наявні адміністративні ролі і ролі звичайних користувачів, визначені у політиці ФПБ

10.5 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Цілісність комплексу засобів захисту"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Цілісність комплексу засобів захисту" наведено у таблиці 10.5.

Таблиця 10.5

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
НЦ-1	Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ	FPT_PHP.2.1: ФБО повинні забезпечувати однозначне виявлення фізичного впливу, який може загрожувати виконанню ФБО. FPT_PHP.2.2: ФБО повинні надавати можливість визначати, чи стався фізичний вплив на пристрої або елементи, що реалізують ФБО. FPT_PHP.2.3: Для [призначення: список пристроїв/ елементів, що реалізують ФБО, для яких потрібне активне виявлення] ФБО повинні постійно контролювати пристрої, елементи і сповіщати	У списку пристроїв/ елементів, що реалізують ФБО, функціонального елемента FPT_PHP.2.3 наявні всі компоненти, що входять до складу КЗЗ, визначені у політиці ФПБ. Функціональний елемент FPT_PHP.2.3 надає можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, одержати інформацію про порушення цілісності всіх компонентів, що
	В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести ОЕ до стану, з якого повернути його до нормального функціонування може		

	тільки адміністратор або користувачі, яким надані відповідні повноваження	[призначення: призначений користувач або роль], що відбувся фізичний вплив на пристрої або елементи, що реалізують ФБО. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями	входять до складу КЗЗ, визначених у політиці ФПБ
	Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ		Відповідні вимоги задоволені елементами довіри AVA_ADM.1.2C, AVA_ADM.1.3C, AVA_ADM.1.5C, AVA_ADM.1.8C, AVA_MSU.1.4C, AVA_MSU.1.4C, AVA_MSU.2.4C, AVA_MSU.3.4C, визначеними стандартом ISO/IEC 15408-3
НЦ-2	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів	FPT_SEP.1.1: ФБО повинні підтримувати домен безпеки для власного виконання, який захищає їх від втручання або пошкодження недовіреними суб’єктами. FPT_SEP.1.2: ФБО повинні реалізовувати розмежування між доменами безпеки суб’єктів в ОДФ. FPT_SEP.2.1: Неізольована частина ФБО повинна підтримувати домен безпеки для власного виконання, який захищає їх від втручання або пошкодження недовіреними суб’єктами. FPT_SEP.2.2: ФБО повинні реалізовувати розмежування між доменами безпеки суб’єктів в ОДФ. FPT_SEP.2.3: ФБО повинні підтримувати частину ФБО, зв’язаних із *[призначення: список* ПФБ керування доступом та/або ПФБ керування інформаційними потоками], у домені безпеки для їх власного виконання,	ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FPT_SEP.2.3 підтримують домен безпеки для всіх компонентів, що входять до складу КЗЗ, визначених у політиці ФПБ
	КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування		

		який захищає їх від втручання або пошкодження іншою частиною ФБО та суб'єктами, недовіреними відносно цих ПФБ	
	Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ		Відповідні вимоги задоволені елементами довіри AVA_ADM.1.2C, AVA_ADM.1.3C, AVA_ADM.1.5C, AVA_ADM.1.8C, AVA_MSU.1.4C, AVA_MSU.1.4C, AVA_MSU.2.4C, AVA_MSU.3.4C, визначеними стандартом ISO/IEC 15408-3
НЦ-3	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів	FPT_SEP.3.1: Неізольована частина ФБО повинна підтримувати домен безпеки для власного виконання, який захищає їх від втручання або пошкодження недовіреними суб'єктами. FPT_SEP.3.2: ФБО повинні реалізовувати розмежування між доменами безпеки суб'єктів в ОДФ. FPT_SEP.3.3: ФБО повинні підтримувати частину ФБО, яка реалізує ПФБ керування доступом та/або керування інформаційними потоками, у домені безпеки для їх власного виконання, який захищає їх від втручання або пошкодження іншою частиною ФБО та суб'єктами, недовіреними відносно цих ПБО. FPT_RVM.1.1: ФБО повинні забезпечувати, щоб функції, які реалізують ПБО, викликались та успішно виконувались перш, ніж дозволяється виконання будь якої іншої функції в межах ОДФ	ПФБ керування доступом та/або ПФБ керування інформаційними потоками функціонального елемента FPT_SEP.3.3 підтримують домен безпеки для всіх компонентів, що входять до складу КЗЗ, визначених у політиці ФПБ
	КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування		
	КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ		

10.6 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Самотестування"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Самотестування" наведено у таблиці 10.6.

Таблиця 10.6

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
НТ-1	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості ОЕ і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження	FPT_TST.1.1: ФБО повинні виконувати пакет програм самотестування [вибір: при старті, періодично в процесі нормального функціонування, за запитом уповноваженого користувача, за умов [призначення: умови, за яких слід передбачити самотестування]] для демонстрації правильного виконання [вибір: [призначення: частини ФБО], ФБО] FPT_TST.1.2: ФБО повинні надавати уповноваженим користувачам можливість верифікації цілісності [вибір: [призначення: даних частин ФБО], даних ФБО]. FPT_TST.1.3: ФБО повинні надавати уповноваженим користувачам можливість верифікації цілісності збереженого виконуваного коду ФБО. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями	Функціональні елементи FPT_TST.1.1 - FPT_TST.1.3 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, виконувати визначений у політиці ФПБ набір тестів з метою оцінки правильності функціонування критичних функцій КЗЗ

НТ-2	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості ОЕ і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження і при ініціалізації КЗЗ	FPT_TST.1.1: ФБО повинні виконувати пакет програм самотестування [вибір: при старті, періодично в процесі нормального функціонування, за запитом уповноваженого користувача, за умов [призначення: умови, за яких слід передбачити самотестування]] для демонстрації правильного виконання [вибір: [призначення: частини ФБО], ФБО] FPT_TST.1.2: ФБО повинні надавати уповноваженим користувачам можливість верифікації цілісності [вибір: [призначення: даних частин ФБО], даних ФБО]. FPT_TST.1.3: ФБО повинні надавати уповноваженим користувачам можливість верифікації цілісності збереженого виконуваного коду ФБО. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями	Функціональні елементи FPT_TST.1.1 - FPT_TST.1.3 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, виконувати визначений у політиці ФПБ набір тестів з метою оцінки правильності функціонування критичних функцій КЗЗ. Функціональні елементи FPT_TST.1.1, FPT_TST.1.2 надають можливість виконувати визначений у політиці ФПБ набір тестів з метою оцінки правильності функціонування критичних функцій КЗЗ при ініціалізації (старті) КЗЗ
НТ-3	Політика самотестування, що реалізується КЗЗ, повинна описувати властивості ОЕ і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ КЗЗ має бути здатним виконувати набір тестів з метою оцінки	FPT_TST.1.1: ФБО повинні виконувати пакет програм самотестування [вибір: при старті, періодично в процесі нормального функціонування, за запитом уповноваженого користувача, за умов [призначення: умови, за яких слід передбачити самотестування]] для демонстрації правильного виконання [вибір: [призначення: частини ФБО], ФБО] FPT_TST.1.2: ФБО повинні надавати уповноваженим користувачам можливість верифікації цілісності [вибір: [призначення: даних частин ФБО], даних ФБО].	Функціональні елементи FPT_TST.1.1 - FPT_TST.1.3 надають можливість користувачу, асоційованому з певною роллю функціональних елементів FMT_SMR.1.1 чи FMT_SMR.2.1, виконувати визначений у політиці ФПБ набір тестів з метою оцінки правильності функціонування критичних функцій КЗЗ. Функціональні елементи FPT_TST.1.1, FPT_TST.1.2 надають можливість виконувати визначений у політиці ФПБ набір тестів з метою оцінки правильності функціонування критичних функцій КЗЗ при ініціалізації (старті) КЗЗ, а також у процесі його штатного

	правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ і в процесі штатного функціонування	FPT_TST.1.3: ФБО повинні надавати уповноваженим користувачам можливість верифікації цілісності збереженого виконуваного коду ФБО. FMT_SMR.1.1, FMT_SMR.2.1: ФБО повинні підтримувати такі ролі [призначення: уповноважені ідентифіковані ролі]. FMT_SMR.1.2, FMT_SMR.2.2: ФБО повинні бути здатними асоціювати користувачів із ролями	функціонування

10.7 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Ідентифікація і автентифікація при обміні"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Ідентифікація і автентифікація при обміні" наведено у таблиці 10.7.

Таблиця 10.7

Рівень ФПБ	**Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ**	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
НВ-1	Політика ідентифікації і автентифікації при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен	FTP_ITC.1.1: ФБО повинні надавати канал зв’язку між ними і віддаленим довіреним продуктом ІТ, який логічно відрізняється від інших каналів зв’язку та забезпечує впевнену автентифікацію його кінцевих сторін, а також захист даних каналу від модифікації або розкриття. FTP_ITC.1.2: ФБО повинні дозволяти [вибір: ФБО, віддалений довірений продукт ІТ] ініціювати зв’язок через довірений канал. FTP_ITC.1.3: ФБО повинні ініціювати зв’язок через довірений канал для виконання [призначення: список функцій, для	У списку функцій, для яких потрібний довірений канал, функціонального елемента FDP_ITC.1.3 наявні всі типи операцій обміну даними між КЗЗ (компонентами КЗЗ), на які поширюється політика ФПБ. Для всіх типів операцій обміну даними між КЗЗ (компонентами КЗЗ), на які поширюється політика ФПБ, функціональний елемент FDP_ITC.1.1 надає можливість КЗЗ (компоненту КЗЗ) за допомогою криптографічних операцій

	автентифікувати цей КЗЗ з використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.	яких потрібний довірений канал]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації, перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), ідентифікувати і автентифікувати цей КЗЗ (компонент КЗЗ)
НВ-2	Політика ідентифікації і автентифікації при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим	FTP_ITC.1.1: ФБО повинні надавати канал зв'язку між ними і віддаленим довіреним продуктом ІТ, який логічно відрізняється від інших каналів зв'язку та забезпечує впевнену автентифікацію його кінцевих сторін, а також захист даних каналу від модифікації або розкриття. FTP_ITC.1.2: ФБО повинні дозволяти [вибір: ФБО, віддалений довірений продукт ІТ]	У списку функцій, для яких потрібний довірений канал, функціонального елемента FDP_ITC.1.3 наявні всі типи операцій обміну даними між КЗЗ (компонентами КЗЗ), на які поширюється політика ФПБ. Для всіх типів операцій обміну даними між КЗЗ (компонентами КЗЗ), на які поширюється політика

	КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.	ініціювати зв'язок через довірений канал. FTP_ITC.1.3: ФБО повинні ініціювати зв'язок через довірений канал для виконання [призначення: список функцій, для яких потрібний довірений канал]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	ФПБ, функціональний елемент FDP_ITC.1.1 надає можливість КЗЗ (компоненту КЗЗ), за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації, перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), ідентифікувати і автентифікувати цей КЗЗ (компонент КЗЗ)
156	КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що	FDP_DAU.1.1: ФБО повинні надавати можливість генерувати свідоцтво, яке може бути використано як гарантія правильності [призначення: *список об'єктів або типів інформації].*	У списку об'єктів або типів інформації функціонального елемента FDP_DAU.1.1 наявні всі типи об'єктів, на які поширюється політика ФПБ.

	експортується та імпортується	FDP_DAU.1.2: ФБО повинні надавати [призначення: *список суб'єктів]* можливість верифікації свідоцтва правильності зазначеної інформації. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	Для всіх типів операцій обміну даними між КЗЗ (компонентами КЗЗ) та всіх типів об'єктів, на які поширюється політика ФПБ, функціональні елементи FDP_DAU.1.1, FDP_DAU.1.2 надають можливість КЗЗ (компоненту КЗЗ) за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації встановити джерело кожного об'єкта, що експортується та імпортується
НВ-3	Політика ідентифікації і автентифікації при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для	FTP_ITC.1.1: ФБО повинні надавати канал зв'язку між ними і віддаленим довіреним продуктом ІТ, який логічно відрізняється від інших каналів зв'язку та забезпечує впевнену автентифікацію його кінцевих сторін, а також захист даних каналу від модифікації або	У списку функцій, для яких потрібний довірений канал, функціонального елемента FDP_ITC.1.3 наявні всі типи операцій обміну даними між КЗЗ (компонентами КЗЗ), на які поширюється політика ФПБ.

	взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.	розкриття. FTP_ITC.1.2: ФБО повинні дозволяти [вибір: ФБО, віддалений довірений продукт ІТ] ініціювати зв'язок через довірений канал. FTP_ITC.1.3: ФБО повинні ініціювати зв'язок через довірений канал для виконання [призначення: список функцій, для яких потрібний довірений канал]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	Для всіх типів операцій обміну даними між КЗЗ (компонентами КЗЗ), на які поширюється політика ФПБ, функціональний елемент FDP_ITC.1.1 надає можливість КЗЗ (компоненту КЗЗ) за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації, перш ніж почати обмін даними з іншим КЗЗ (компонентом КЗЗ), ідентифікувати і автентифікувати цей КЗЗ (компонент КЗЗ)
158	КЗЗ повинен використовувати захищені	FDP_DAU.2.1: ФБО повинні надавати можливість генерувати свідоцтво, яке може бути	У списку об'єктів або типів інформації функціонального

	механізми для встановлення джерела кожного об'єкта, що експортується та імпортується Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною	використано як гарантія правильності [призначення: список об’єктів або типів інформації]. FDP_DAU.2.2: ФБО повинні надавати [призначення: список суб’єктів] можливість верифікації свідоцтва правильності зазначеної інформації та ідентифікатор користувача, який створив свідоцтво. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	елемента FDP_DAU.2.1 наявні всі типи об’єктів, на які поширюється політика ФПБ. Для всіх типів операцій обміну даними між КЗЗ (компонентами КЗЗ) та всіх типів об’єктів, на які поширюється політика ФПБ, функціональні елементи FDP_DAU.2.1, FDP_DAU.2.2 надають можливість КЗЗ (компоненту КЗЗ) за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації встановити джерело кожного об'єкта, що експортується та імпортується, із можливістю однозначного підтвердження джерела об'єкта незалежною третьою стороною

10.8 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Автентифікація відправника"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Автентифікація відправника" наведено у таблиці 10.8.

Таблиця 10.8

Рівень ФПБ	Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ	Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99	Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99
НА-1	Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	FCO_NRO.1.1: ФБО повинні бути здатними генерувати свідоцтво відправлення переданої [призначення: список типів інформації] за запитом [вибір: відправник, одержувач, [призначення: список третіх осіб]]. FCO_NRO.1.2: ФБО повинні бути здатними зв’язувати [призначення: список атрибутів] відправника інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRO.1.3: ФБО повинні надавати можливість верифікації свідоцтва відправлення інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво відправлення]. FCO_NRO.2.1: ФБО повинні завжди здійснювати генерацію свідоцтва відправлення переданої [призначення: список типів інформації]. FCO_NRO.2.2: ФБО повинні бути здатними зв’язувати [призначення: список атрибутів] відправника інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRO.2.3: ФБО повинні	У списку типів інформації функціонального елемента FCO_NRO.1.1 або FCO_NRO.2.1 наявні всі типи об’єктів, що передаються, на які поширюється політика ФПБ. У списку атрибутів та списку інформаційних полів об’єктів функціонального елемента FCO_NRO.1.2 або FCO_NRO.2.2 наявні всі властивості та всі атрибути об’єктів та інтерфейсних процесів відповідних типів, визначені у політиці ФПБ. Для всіх типів об’єктів, на які поширюється політика ФПБ, функціональні елементи FCO_NRO.1.1 - FCO_NRO.1.3 або FCO_NRO.2.1 - FCO_NRO.2.3 надають можливість за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації однозначно встановити, що певний об'єкт був відправлений (створений) певним користувачем
	Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації		

		надавати можливість верифікації свідоцтва відправлення інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво відправлення]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
НА-2	Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати	FCO_NRO.1.1: ФБО повинні бути здатними генерувати свідоцтво відправлення переданої [призначення: список типів інформації] за запитом [вибір:	У списку типів інформації функціонального елемента FCO_NRO.1.1 або FCO_NRO.2.1 наявні всі типи об’єктів, що

	множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	відправник, одержувач, [призначення: список третіх осіб]]. FCO_NRO.1.2: ФБО повинні бути здатними зв’язувати [призначення: список атрибутів] відправника інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRO.1.3: ФБО повинні надавати можливість верифікації свідоцтва відправлення інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво відправлення]. FCO_NRO.2.1: ФБО повинні завжди здійснювати генерацію свідоцтва відправлення переданої [призначення: список типів інформації]. FCO_NRO.2.2: ФБО повинні бути здатними зв’язувати [призначення: список атрибутів] відправника інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRO.2.3: ФБО повинні надавати можливість верифікації свідоцтва відправлення інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво відправлення]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення:	передаються, на які поширюється політика ФПБ. У списку атрибутів та списку інформаційних полів об’єктів функціонального елемента FCO_NRO.1.2 або FCO_NRO.2.2 наявні всі властивості та всі атрибути об’єктів та інтерфейсних процесів відповідних типів, визначені у політиці ФПБ. Для всіх типів об’єктів, на які поширюється політика ФПБ, функціональні елементи FCO_NRO.1.1 - FCO_NRO.1.3 або FCO_NRO.2.1 - FCO_NRO.2.3 надають можливість за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації однозначно встановити, що певний об'єкт був відправлений (створений) певним користувачем, із можливістю однозначного підтвердження належності об'єкта незалежною третьою стороною
	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною		
	Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації		
	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною		

		довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	

10.9 Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Автентифікація одержувача"

Відомості щодо відповідності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам НД ТЗІ 2.5-004-99 до ФПБ "Автентифікація одержувача" наведено у таблиці 10.9.

Таблиця 10.9

Рівень ФПБ	Вимоги НД ТЗІ 2.5-004-99 щодо політики ФПБ	Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99	Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99
НП-1	Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів	FCO_NRR.1.1: ФБО повинні бути здатними генерувати свідоцтво одержання переданої [призначення: список типів інформації] за запитом [вибір: відправник, одержувач, [призначення: список третіх осіб]]. FCO_NRR.1.2: ФБО повинні бути здатними зв’язувати [призначення: список атрибутів] одержувача інформації і [призначення: список	У списку типів інформації функціонального елемента FCO_NRR.1.1 або FCO_NRR.2.1 наявні всі типи об’єктів, що передаються, на які поширюється політика ФПБ.

	об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRR.1.3: ФБО повинні надавати можливість верифікації свідоцтва одержання інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво одержання]. FCO_NRR.2.1: ФБО повинні завжди здійснювати генерацію свідоцтва одержання переданої [призначення: список типів інформації]. FCO_NRR.2.2: ФБО повинні бути здатними зв’язувати [призначення: список атрибутів] одержувача інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRR.2.3: ФБО повинні надавати можливість верифікації свідоцтва одержання інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво одержання]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів].	У списку атрибутів та списку інформаційних полів об’єктів функціонального елемента FCO_NRR.1.2 або FCO_NRR.2.2 наявні всі властивості та всі атрибути об’єктів та інтерфейсних процесів відповідних типів, визначені у політиці ФПБ. Для всіх типів об’єктів, на які поширюється політика ФПБ, функціональні елементи FCO_NRR.1.1 - FCO_NRR.1.3 або FCO_NRR.2.1 - FCO_NRR.2.3 надають можливість за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації однозначно встановити, що певний об'єкт був одержаний певним користувачем.
	Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації		

		FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	
НП-2	Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	FCO_NRR.1.1: ФБО повинні бути здатними генерувати свідоцтво одержання переданої [призначення: список типів інформації] за запитом [вибір: відправник, одержувач, [призначення: список третіх осіб]]. FCO_NRR.1.2: ФБО повинні бути здатними зв'язувати [призначення: список атрибутів] одержувача інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRR.1.3: ФБО повинні надавати можливість верифікації свідоцтва одержання інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво одержання]. FCO_NRR.2.1: ФБО повинні завжди здійснювати генерацію свідоцтва одержання переданої [призначення: список типів інформації]. FCO_NRR.2.2: ФБО повинні бути здатними зв'язувати [призначення: список атрибутів] одержувача інформації і [призначення: список інформаційних полів] інформації, до якої додається свідоцтво. FCO_NRR.2.3: ФБО повинні надавати можливість верифікації свідоцтва одержання інформації [вибір: відправник, одержувач, [призначення: список третіх осіб]] при встановлених [призначення: обмеження на свідоцтво одержання]. FCS_COP.1.1: ФБО повинні виконувати [призначення: список криптографічних операцій] згідно з визначеними алгоритмами [призначення: криптографічні алгоритми] та довжиною [призначення: довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.1.1: ФБО повинні генерувати криптографічні ключі згідно з визначеним алгоритмом [призначення: алгоритм генерації криптографічних ключів] та довжиною [призначення:	У списку типів інформації функціонального елемента FCO_NRR.1.1 або FCO_NRR.2.1 наявні всі типи об'єктів, що передаються, на які поширюється політика ФПБ. У списку атрибутів та списку інформаційних полів об'єктів функціонального елемента FCO_NRR.1.2 або FCO_NRR.2.2 наявні всі властивості та всі атрибути об'єктів та інтерфейсних процесів відповідних типів, визначені у політиці ФПБ. Для всіх типів об'єктів, на які поширюється політика ФПБ, функціональні елементи FCO_NRR.1.1 - FCO_NRR.1.3 або FCO_NRR.2.1 - FCO_NRR.2.3 надають можливість за допомогою криптографічних операцій функціонального елемента FCS_COP.1.1 та з використанням відповідного протоколу автентифікації однозначно встановити, що певний об'єкт був одержаний певним користувачем, із можливістю однозначного підтвердження факту одержання об'єкта незалежною третьою стороною
	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для однозначного підтвердження факту одержання об'єкта		
	Встановлення одержувача має виконуватися на підставі затвердженого протоколу		

	автентифікації Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта	довжина криптографічних ключів], що відповідають вимогам: [призначення: список стандартів]. FCS_CKM.2.1: ФБО повинні розподіляти криптографічні ключі згідно з визначеним методом [призначення: метод розподілу криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.3.1: ФБО повинні виконувати [призначення: тип доступу до криптографічних ключів] згідно з визначеним методом доступу [призначення: метод доступу до криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]. FCS_CKM.4.1: ФБО повинні знищувати криптографічні ключі згідно з визначеним методом [призначення: метод знищення криптографічних ключів], що відповідає вимогам: [призначення: список стандартів]	

11 Порядок документування результатів зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99

11.1 Якщо зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 виконувалося у ході робіт із оцінювання ФПБ під час проведення державної експертизи в сфері ТЗІ, результати зіставлення мають бути документовані у порядку, визначеному НД ТЗІ 2.6-001-11, наприклад, у вигляді технічних вимог до оцінюваного ОЕ у частині реалізації ФПБ.

Крім цього, факт виконання зіставлення в ході проведення експертних робіт має бути зазначений у розділі "Результати експертних робіт" експертного висновку, складеного за результатами експертизи відповідно до рекомендацій, наведених у Додатку Е до НД ТЗІ 2.6-001-11. При цьому у розділі "Перелік документів, склад програмних та технічних засобів, які надано на експертизу" експертного висновку мають бути наведені посилання на всі документи (матеріали), що містять результати оцінювання (сертифікації) відповідного ЗТЗІ від НСД (захищеного від НСД компонента обчислювальної системи) на відповідність стандарту ISO/IEC 15408, які були використані під час проведення державної експертизи.

11.2 У всіх інших випадках результати зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 документуються у довільній формі.

Додаток А
(рекомендований)

Відомості щодо застосовності функціональних елементів функціональних компонентів безпеки згідно з ISO/IEC 15408 для реалізації вимог НД ТЗІ 2.5-004-99 до функціональних послуг безпеки

У таблиці А.1 Додатка А викладено відомості щодо застосовності функціональних елементів функціональних компонентів безпеки сімейств функціональних класів згідно з ISO/IEC 15408-2 для реалізації вимог НД ТЗІ 2.5-004-99 до ФПБ. Відповідні відомості сформульовано на підставі таблиць 7.1 - 10.9 та призначено для спрощення визначення в ході виконання прямого зіставлення груп функціональних елементів, які у сукупності здатні задовольнити вимоги НД ТЗІ 2.5-004-99 щодо певних ФПБ певних рівнів.

Таблиця А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FAU_ARP – автоматична реакція аудита безпеки	FAU_ARP.1.1	НР-3, НР-4, НР-5
FAU_GEN – генерація даних аудита безпеки	FAU_GEN.1.1	НР-1, НР-2, НР-3, НР-4, НР-5
	FAU_GEN.1.2	НР-1, НР-2, НР-3, НР-4, НР-5
	FAU_GEN.2.1	НР-1, НР-2, НР-3, НР-4, НР-5
FAU_SAA – аналіз аудита безпеки	FAU_SAA.1.1	ДС-1, ДС-2, ДС-3, НР-3, НР-4, НР-5
	FAU_SAA.1.2	НР-3, НР-4, НР-5
	FAU_SAA.2.1	НР-3, НР-4, НР-5
	FAU_SAA.2.2	НР-3, НР-4, НР-5
	FAU_SAA.2.3	НР-3, НР-4, НР-5
	FAU_SAA.3.1	НР-5
	FAU_SAA.3.2	НР-5
	FAU_SAA.3.3	НР-5
	FAU_SAA.4.1	НР-5
	FAU_SAA.4.2	НР-5
	FAU_SAA.4.3	НР-5

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FAU_SAR – перегляд аудита безпеки	FAU_SAR.1.1	НР-2, НР-3, НР-4, НР-5
	FAU_SAR.1.2	НР-2, НР-3, НР-4, НР-5
FAU_SEL – вибір подій аудита безпеки	FAU_SEL.1.1	НР-4, НР-5
FAU_STG – зберігання даних аудита безпеки	FAU_STG.1.1	НР-2, НР-3, НР-4, НР-5
	FAU_STG.1.2	НР-2, НР-3, НР-4, НР-5
	FAU_STG.2.1	НР-2, НР-3, НР-4, НР-5
	FAU_STG.2.2	НР-2, НР-3, НР-4, НР-5
FCO_NRO – неспростовність відправлення	FCO_NRO.1.1	НА-1, НА-2
	FCO_NRO.1.2	НА-1, НА-2
	FCO_NRO.1.3	НА-1, НА-2
	FCO_NRO.2.1	НА-1, НА-2
	FCO_NRO.2.2	НА-1, НА-2
	FCO_NRO.2.3	НА-1, НА-2
FCO_NRR – неспростовність одержання	FCO_NRR.1.1	НП-1, НП-2
	FCO_NRR.1.2	НП-1, НП-2
	FCO_NRR.1.3	НП-1, НП-2
	FCO_NRR.2.1	НП-1, НП-2
	FCO_NRR.2.2	НП-1, НП-2
	FCO_NRR.2.3	НП-1, НП-2

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FCS_CKM – керування криптографічними ключами	FCS_CKM.1.1	КВ-1, КВ-2, КВ-3, КВ-4, ЦВ-1, ЦВ-2, ЦВ-3, НВ-1, НВ-2, НВ-3, НА-1, НА-2, НП-1, НП-2
	FCS_CKM.2.1	КВ-1, КВ-2, КВ-3, КВ-4, ЦВ-1, ЦВ-2, ЦВ-3, НВ-1, НВ-2, НВ-3, НА-1, НА-2, НП-1, НП-2
	FCS_CKM.3.1	КВ-1, КВ-2, КВ-3, КВ-4, ЦВ-1, ЦВ-2, ЦВ-3, НВ-1, НВ-2, НВ-3, НА-1, НА-2, НП-1, НП-2
	FCS_CKM.4.1	КВ-1, КВ-2, КВ-3, КВ-4, ЦВ-1, ЦВ-2, ЦВ-3, НВ-1, НВ-2, НВ-3, НА-1, НА-2, НП-1, НП-2
FCS_COP – криптографічні операції	FCS_COP.1.1	КВ-1, КВ-2, КВ-3, КВ-4, ЦВ-1, ЦВ-2, ЦВ-3, НВ-1, НВ-2, НВ-3, НА-1, НА-2, НП-1, НП-2
FDP_ACC – політика керування доступом	FDP_ACC.1.1	КД-1, КД-2, КА-1, КА-2, ЦД-1, ЦД-2, ЦА-1, ЦА-2
	FDP_ACC.2.1	КД-3, КД-4, КА-3, КА-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_ACC.2.2	КД-3, КД-4, КА-3, КА-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
FDP_ACF – функції керування доступом	FDP_ACF.1.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4
	FDP_ACF.1.2	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4
	FDP_ACF.1.3	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4
	FDP_ACF.1.4	КД-3, КД-4, КА-3, КА-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FDP_DAU – автентифікація даних	FDP_DAU.1.1	НВ-2, НВ-3
	FDP_DAU.1.2	НВ-2, НВ-3
	FDP_DAU.2.1	НВ-2, НВ-3
	FDP_DAU.2.2	НВ-2, НВ-3
FDP_ETC – експорт даних за межі дії ФБО	FDP_ETC.1.1	КД-1, КД-2, КА-1, КА-2, КВ-1, ЦД-1, ЦД-2, ЦА-1, ЦА-2, ЦВ-1,
	FDP_ETC.1.2	КД-1, КД-2, КА-1, КА-2, ЦД-1, ЦД-2, ЦА-1, ЦА-2,
	FDP_ETC.2.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
	FDP_ETC.2.2	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
	FDP_ETC.2.3	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
	FDP_ETC.2.4	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3
FDP_IFC – політика керування інформаційними потоками	FDP_IFC.1.1	КД-1, КД-2, КА-1, КА-2, КВ-1, КВ-2, ЦД-1, ЦД-2, ЦА-1, ЦА-2, ЦВ-1, ЦВ-2, ЦВ-3
	FDP_IFC.2.1	КД-3, КД-4, КА-3, КА-4, КВ-3, КВ-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_IFC.2.2	КД-3, КД-4, КА-3, КА-4, КВ-3, КВ-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FDP_IFF – функції керування інформаційними потоками	FDP_IFF.1.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-1, КВ-2, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-1, ЦВ-2, ЦВ-3
	FDP_IFF. 1.2	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-1, КВ-2, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-1, ЦВ-2, ЦВ-3
	FDP_IFF. 1.5	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4
	FDP_IFF. 1.6	КД-3, КД-4, КА-3, КА-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_IFF.2.1	КД-3, КД-4, КА-3, КА-4, КВ-3, КВ-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_IFF.2.2	КД-3, КД-4, КА-3, КА-4, КВ-3, КВ-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_IFF.2.5	КД-3, КД-4, КА-3, КА-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_IFF.2.6	КД-3, КД-4, КА-3, КА-4, ЦД-3, ЦД-4, ЦА-3, ЦА-4
	FDP_IFF.4.1	КВ-4
	FDP_IFF.4.2	КВ-4
	FDP_IFF.5.1	КК-3, КВ-4
	FDP_IFF.6.1	КК-2, КВ-4
FDP_ITC – імпорт даних із-за меж дії ФБО	FDP_ITC.1.1	КД-1, КД-2, КА-1, КА-2, КВ-1, ЦД-1, ЦД-2, ЦА-1, ЦА-2, ЦВ-1,
	FDP_ITC.1.2	КД-1, КД-2, КА-1, КА-2, ЦД-1, ЦД-2, ЦА-1, ЦА-2,
	FDP_ITC.1.3	КД-1, КД-2, КА-1, КА-2, ЦД-1, ЦД-2, ЦА-1, ЦА-2,
	FDP_ITC.2.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FDP_ITC – імпорт даних із-за меж дії ФБО (продовження)	FDP_ITC.2.2	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
	FDP_ITC.2.3	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
	FDP_ITC.2.4	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
	FDP_ITC.2.5	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3,
FDP_ITT – передача в межах ОО	FDP_ITT.1.1	КВ-3, КВ-4,
	FDP_ITT.2.1	КВ-3, КВ-4,
FDP_RIP – захист залишкової інформації	FDP_RIP.1.1	КО-1
	FDP_RIP.2.1	КО-1
FDP_ROL – відкат	FDP_ROL.1.1	ЦО-1
	FDP_ROL.1.2	ЦО-1
	FDP_ROL.2.1	ЦО-2
	FDP_ROL.2.2	ЦО-2
FDP_UCT – захист конфіденційності даних користувача при передачі між ФБО	FDP_UCT.1.1	КВ-1, КВ-2, КВ-3, КВ-4,
FDP_UIT – захист цілісності даних користувача при передачі між ФБО	FDP_UIT.1.1	ЦВ-1, ЦВ-2, ЦВ-3,
	FDP_UIT.1.2	ЦВ-1, ЦВ-2, ЦВ-3,
FIA_ATD – визначення атрибутів користувача	FIA_ATD.1.1	НИ-1, НИ-2, НИ-3
FIA_UAU – автентифікація користувача	FIA_UAU.2.1	НИ-1, НИ-2, НИ-3
	FIA_UAU.5.1	НИ-1, НИ-2, НИ-3
	FIA_UAU.5.2	НИ-1, НИ-2, НИ-3

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FIA_UID – ідентифікація користувача	FIA_UID.2.1	НИ-1, НИ-2, НИ-3
FIA_USB – зв'язування користувач – суб'єкт	FIA_USB.1.1	НИ-1, НИ-2, НИ-3
	FIA_USB.1.2	НИ-1, НИ-2, НИ-3
	FIA_USB.1.3	НИ-1, НИ-2, НИ-3
FMT_MOF – керування окремими функціями ФБО	FMT_MOF.1.1	ДЗ-1, ДЗ-2, ДЗ-3, ДВ-1, ДВ-2, ДВ-3,
FMT_MSA – керування атрибутами безпеки	FMT_MSA.1.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3, ДР-1, ДР-2, ДР-3,
	FMT_MSA.2.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КО-1, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4,
	FMT_MSA.3.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КО-1, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4,
FMT_SMF – специфікація функцій керування	FMT_SMF.1.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-1, КВ-2, КВ-3, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-1, ЦВ-2, ЦВ-3, ДР-1, ДР-2, ДР-3, ДЗ-1, ДЗ-2, ДЗ-3, ДВ-1, ДВ-2, ДВ-3, НР-2, НР-3, НР-4, НР-5, НО-1, НО-2, НО-3
FMT_SMR – ролі керування безпекою	FMT_SMR.1.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3, ДР-1, ДР-2, ДР-3, ДС-1, ДС-2, ДС-3, ДЗ-1, ДЗ-2, ДЗ-3, ДВ-1, ДВ-2, ДВ-3, НР-2, НР-3, НР-4, НР-5, НО-1, НО-2, НО-3, НЦ-1, НТ-1, НТ-2, НТ-3,

Продовження таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FMT_SMR – ролі керування безпекою (продовження)	FMT_SMR.2.1	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3, ДР-1, ДР-2, ДР-3, ДС-1, ДС-2, ДС-3, ДЗ-1, ДЗ-2, ДЗ-3, ДВ-1, ДВ-2, ДВ-3, НР-2, НР-3, НР-4, НР-5, НО-1, НО-2, НО-3, НЦ-1, НТ-1, НТ-2, НТ-3,
	FMT_SMR.1.2	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3, ДР-1, ДР-2, ДР-3, ДС-1, ДС-2, ДС-3, ДЗ-1, ДЗ-2, ДЗ-3, ДВ-1, ДВ-2, ДВ-3, НР-2, НР-3, НР-4, НР-5, НО-1, НО-2, НО-3, НЦ-1, НТ-1, НТ-2, НТ-3,
	FMT_SMR.2.2	КД-1, КД-2, КД-3, КД-4, КА-1, КА-2, КА-3, КА-4, КВ-2, КВ-3, КВ-4, ЦД-1, ЦД-2, ЦД-3, ЦД-4, ЦА-1, ЦА-2, ЦА-3, ЦА-4, ЦВ-2, ЦВ-3, ДР-1, ДР-2, ДР-3, ДС-1, ДС-2, ДС-3, ДЗ-1, ДЗ-2, ДЗ-3, ДВ-1, ДВ-2, ДВ-3, НР-2, НР-3, НР-4, НР-5, НО-1, НО-2, НО-3, НЦ-1, НТ-1, НТ-2, НТ-3,
	FMT_SMR.3.1	НО-1, НО-2, НО-3
FPT_FLS – безпека при збої	FPT_FLS.1.1	ДС-1, ДС-2, ДС-3
FPT_ITA – доступність експортованих даних ФБО	FPT_ITA.1.1	НР-1
FPT_ITI – цілісність експортованих даних ФБО	FPT_ITI.1.1	НР-1
	FPT_ITI.2.1	НР-1
FPT_ITT – передача даних ФБО у межах ОО	FPT_ITT.1.1	НИ-2, НИ-3
	FPT_ITT.2.1	НИ-2, НИ-3
FPT_PHP – фізичний захист ФБО	FPT_PHP.2.1	НЦ-1
	FPT_PHP.2.2	НЦ-1
	FPT_PHP.2.3	НЦ-1

Закінчення таблиці А.1

Сімейство функціонального класу згідно з ISO/IEC 15408-2	**Функціональні елементи функціональних компонентів безпеки відповідного сімейства**	**Позначення рівнів ФПБ згідно з НД ТЗІ 2.5-004-99, для задоволення вимог щодо яких можуть бути задіяні функціональні елементи функціональних компонентів безпеки відповідного сімейства**
FPT_RCV – надійне відновлення	FPT_RCV.1.1	ДВ-1
	FPT_RCV.2.1	ДВ-2
	FPT_RCV.2.2	ДВ-2
	FPT_RCV.3.1	ДВ-3
FPT_RVM – посередництво при звертаннях	FPT_RVM.1.1	НЦ-3
FPT_SEP – розподіл доменів	FPT_SEP.1.1	НЦ-2
	FPT_SEP.1.2	НЦ-2
	FPT_SEP.2.1	НЦ-2
	FPT_SEP.2.2	НЦ-2
	FPT_SEP.2.3	НЦ-2
	FPT_SEP.3.1	НЦ-3
	FPT_SEP.3.2	НЦ-3
	FPT_SEP.3.3	НЦ-3
FPT_TST – самотестування ФБО	FPT_TST.1.1	НТ-1, НТ-2, НТ-3
	FPT_TST.1.2	НТ-1, НТ-2, НТ-3
	FPT_TST.1.3	НТ-1, НТ-2, НТ-3
FRU_FLT – стійкість до відмов	FRU_FLT.1.1	ДС-1, ДС-2
	FRU_FLT.2.1	ДС-3
FRU_PRS – пріоритет обслуговування	FRU_PRS.2.1	ДР-3
	FRU_PRS.2.2	ДР-3
FRU_RSA – розподіл ресурсів	FRU_RSA.1.1	ДР-1
	FRU_RSA.2.1	ДР-2, ДР-3
	FRU_RSA.2.2	ДР-2, ДР-3
FTP_ITC – довірений канал передачі між ФБО	FTP_ITC.1.1	НВ-1, НВ-2, НВ-3
	FTP_ITC.1.2	НВ-1, НВ-2, НВ-3
	FTP_ITC.1.3	НВ-1, НВ-2, НВ-3
FTP_TRP – довірений маршрут	FTP_TRP.1.1	НК-1, НК-2
	FTP_TRP.1.2	НК-1, НК-2
	FTP_TRP.1.3	НК-1, НК-2