ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія створення цільового профілю безпеки авторизованої системи безпеки об'єкту критичної інфраструктури»

зі спеціальності *125 Кібербезпека* та захист інформації
(код, найменування мпеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ілля ЗАБЕНКО
(підпис)

Виконав: здобувач вищої освіти, групи БСДМ-63
ЗАБЕНКО Ілля
(прізвище, ім'я)

Керівник доктор технічних наук, професор
ЗИБІН Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ВСТУП

У сучасній цифровій екосистемі забезпечення інформаційної безпеки є критично важливим завданням для організацій усіх форм власності та сфер діяльності. Зростаюча складність кіберзагроз, постійне збільшення обсягів оброблюваних даних та регуляторні вимоги вимагають впровадження надійних, стандартизованих і адаптивних механізмів контролю. Особливою уваги у процесі забезпечення належного та достатнього рівня захищеності вимагають системи що оброблюють інформацію доступ до якої обмежено у зв'язку з її важливістю або приватністю її власника.

В межах чинного законодавства України для протидії подібним загрозам у інформаційно-комунікаційних системах та забезпечення додаткової конфіденційності, цілісності та доступності законодавством передбачений процес авторизації систем з безпеки.

Ця наукова робота має на меті дослідити процеси та механізми авторизації з безпеки, як вони визначені в межах НД ТЗІ в сфері захисту інформації, з особливим акцентом на розробку та застосування цільового профілю безпеки. Авторизація є фінальним етапом у циклі управління ризиками, де керівництво приймає формальне рішення про функціонування системи, ґрунтуючись на оцінці ризиків. Дослідження сфокусується на тому, як саме цільовий профіль безпеки – адаптований набір контролів, який модифіковано для врахування конкретних загроз, технологій та місії системи – може оптимізувати процес авторизації, підвищити прозорість прийняття рішень та гарантувати належний рівень захисту.

В даній роботі буде розглянуто авторизацію з безпеки, різновиди профілів безпеки, особливості та відмінності кожного з них та приведено рекомендації щодо формування цільового профілю безпеки, що включатиме у себе і рекомендації на етапі підготовки до формування цільового профілю безпеки, і окремі рішення, що рекомендовані до впровадження.

Головним завданням цієї роботи є ознайомлення з процесом формування цільового профілю безпеки та надати рекомендації щодо його впровадження. Після прочитання даної роботи ви дізнаєтесь про авторизовані системи з безпеки та основні заходи захисту та посилення заходів захисту що рекомендовано додати до цільового профілю безпеки під час його формування та як їх краще реалізувати.

1 АВТОРИЗОВАНІ СИСТЕМИ З БЕЗПЕКИ

1.1. Вимоги законодавства України у галузі технічного та криптографічного захисту інформації

Умови та особливості обробки інформації в системі, об’єкті критичної інформаційної інфраструктури визначаються власником або розпорядником відповідної системи, але з урахуванням вимог щодо захисту інформації, що були визначені законодавством.

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації [1].

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, у системах, об’єктах критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, мають оброблятися в авторизованих системах з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності [1].

1.1.1. Інформація з обмеженим доступом

До інформації з обмеженим доступом відносять:

- конфіденційна інформація;
- службова інформація;
- таємна інформація.

Під час обробки конфіденційної, службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення [13].

До інформації з обмеженим доступом не можуть бути віднесені такі відомості [2]:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими особами, які брали участь або сприяли реалізації російської імперської політики, представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5.1) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов’язковому оприлюдненню відповідно до закону;

5.2) про використання публічних коштів розпорядниками та одержувачами коштів державного і місцевих бюджетів, суб’єктами господарювання державної і комунальної власності, органами Пенсійного фонду та Фонду загальнообов’язкового державного соціального страхування України на випадок безробіття, що підлягають обов’язковому оприлюдненню відповідно до закону;

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

1.1.2. Конфіденційна інформація

Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом [2].

1.1.3. Службова інформація

До службової може належати така інформація [4]:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування" [4].

1.1.4. Таємна інформація

Таємна інформація – інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить

державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [4].

Державна таємниця - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку державною таємницею і підлягають охороні державою [3].

Програмне забезпечення, що забезпечує функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляється інформація, що становить державну таємницю, використовується за умови проведення державної експертизи у сфері захисту інформації в порядку, встановленому Кабінетом Міністрів України [1].

Таємна інформація в залежності від її важливості, ступеня обмеження доступу та рівня її охорони державою, може бути додатково поділена на три ступені секретності:

– таємна;

– цілком таємна;

– особливої важливості.

Якщо інформацію, що була віднесена до державної таємниці, було оприлюднено, повторне її засекречення та віднесення до державної таємниці не можливе.

1.1.5. Вимоги до інформаційно-комунікаційної системи

Ключовою вимогою законодавства для інформаційно-комунікаційної системи що зберігає, передає або оброблює інформацію з обмеженим доступом є проведення авторизації з безпеки або отримання сертифіката відповідності.

Крім цього подібна система повинна виконувати наступні вимоги:

1. Використання для захисту інформації в системах засобів технічного та/або криптографічного захисту інформації, які мають позитивний експертний висновок

за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації або документ про відповідність (крім систем, об’єктів критичної інформаційної інфраструктури, в яких обробляється службова інформація або інформація, що становить державну таємницю), виданий органом з оцінки відповідності, який акредитовано національним органом України з акредитації або національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності [1].

2. Елементи системи об’єкта критичної інформаційної інфраструктури не повинні знаходитись:

– в регіонах що визнані як тимчасово окуповані території України;
– на території країни що була визнана Верховною Радою України як держава агресор;
– на території країни, що входить до митного або військового союзу з державою що була визнана державою-агресором.

3. Власник або розпорядник жодного з елементів системи, об’єкта критичної інформаційної інфраструктури не є юридичною або фізичною особою, зареєстрованою на тимчасово окупованій території України, резидентом держави, визнаної Верховною Радою України державою-агресором, резидентом держави, яка входить до митного або воєнного союзу з такими державами або щодо якої застосовано санкції відповідно до Закону України "Про санкції" [1].

4. Власник або розпорядник системи, об’єкта критичної інформаційної інфраструктури або його представник, який надає послуги з використанням системи, об’єкта критичної інформаційної інфраструктури, елементи якої розміщуються поза межами України, є юридичною особою, зареєстрованою в Україні, або має свого офіційного представника в Україні [1].

5. Виконання додаткових специфічних вимог в сфері забезпечення захисту інформації, що були встановленні Кабінетом Міністрів України та будуть залежати

від категорії державних інформаційних ресурсів або різновиду інформації з обмеженим доступом.

Інформація, що становить державну таємницю, має оброблятися в системі, об’єкті критичної інформаційної інфраструктури із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю та за умови використання засобів криптографічного захисту суб’єктів господарювання, які провадять ліцензовану діяльність відповідно до законодавства. Порядок атестації такого комплексу технічного захисту інформації визначається спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації [1].

Національний банк України визначає умови обробки інформації, використання засобів захисту інформації в системах у сфері надання платіжних, банківських та інших фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, валютного регулювання та валютного нагляду, а також у системі депозитарного обліку Національного банку України [1].

Власники або розпорядники систем, об’єктів критичної інформаційної інфраструктури для забезпечення їх належного функціонування та захисту інформації, що обробляється в них [1]:

– створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів, систем, об’єктів критичної інформаційної інфраструктури вимог щодо їх захисту, цілісності та конфіденційності;

– забезпечують створення резервних копій державних інформаційних ресурсів, систем, об’єктів критичної інформаційної інфраструктури на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), під час дії

воєнного стану в Україні та протягом шести місяців з дня його припинення чи скасування;

– забезпечують в установленому законодавством порядку передачу (переміщення) державних інформаційних ресурсів та їх резервних копій для розміщення на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, під час дії воєнного стану в Україні та протягом шести місяців з дня його припинення чи скасування.

Розміщення систем, об’єктів критичної інформаційної інфраструктури або їх елементів та зберігання резервних копій державних інформаційних ресурсів на тимчасово окупованій території України, території держави, визнаної Верховною Радою України державою-агресором, або на території держави, яка входить до митного або воєнного союзу з такими державами, забороняється [1].

Обов’язковою умовою використання програмного забезпечення та комунікаційного (мережевого) обладнання в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також на об’єктах критичної інформаційної інфраструктури є відсутність таких продуктів та обладнання у відкритому переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання [14].

Порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання затверджується Кабінетом Міністрів України [14].

Повноваження щодо забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання покладаються на Державну службу спеціального зв’язку та захисту інформації України [14].

1.2. Процедура проведення авторизації інформаційно-комунікаційної системи з безпеки

Авторизація з безпеки систем проводиться з метою прийняття рішення щодо можливості функціонування (експлуатації) системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту [5].

Авторизація з безпеки системи здійснюється такими етапами [5]:

– розроблення та затвердження для системи цільового профілю;

– виконання вимог цільового профілю;

– оцінювання дотримання вимог цільового профілю;

– оформлення та подання Адміністрації Держспецзв’язку авторизаційного листа;

– внесення даних щодо авторизації до переліку авторизованих систем з безпеки.

У процесі створення авторизованої системи з безпеки власник/розпорядник системи повинен визначити відповідальних за забезпечення захисту інформації. Для великих багатомашинних систем доцільним є покладання цих обов’язків на відповідний відділ з кіберзахисту. Однак, для малих автоматизованих систем допускається призначення відповідальної особи за забезпечення захисту інформації.

1.2.1. Оцінювання автоматизованої системи

Після процесу реалізації цільового профіля безпеки, шляхом впровадження організаційних заходів, програмно-апаратних та технічних засобів та інженерних рішень, необхідно провести попереднє оцінювання автоматизованої системи на відповідність та повну реалізацію цільового профілю безпеки. Цей етап

проводиться власником системи або організацією, що призначена розробником системи на договірній основі.

Після проведення попереднього оцінювання автоматизованої системи на відповідність та повну реалізацію цільового профілю безпеки, обов'язковим та необхідним етапом є організація та проведення незалежної перевірки автоматизованої системи на відповідність цільовому профілю безпеки. На цьому етапі є необхідним залучення на договірній основі сторонньої організації що має ліцензію на проведення відповідної перевірки та яка не приймала участі у попередніх етапах створення авторизованої системи з безпеки.

Після завершення перевірки автоматизованої системи незалежною компанією, оцінщик (незалежна організація, що має відповідну ліцензію) повинна надати власнику відповідні матеріали :

– методика проведення оцінювання на дотримання вимог цільовому профілю безпеки;

– план проведення оцінювання на дотримання вимог цільовому профілю безпеки;

– звіт з оцінювання на дотримання вимог цільовому профілю безпеки.

Якщо при перевірці автоматизованої системи на відповідність цільовому профілю безпеки власником системи та незалежною компанією не було виявлено жодних ознак невиконання або недотримання вимог заходів захисту з цільового профілю безпеки, власник/розпорядник може почати етап подання заяви на внесення інформаційно-комунікаційної системи до переліку авторизованих систем з безпеки.

З порядком процесу оцінювання відповідності цільового профілю безпеки можна ознайомитися на рисунку 1.1

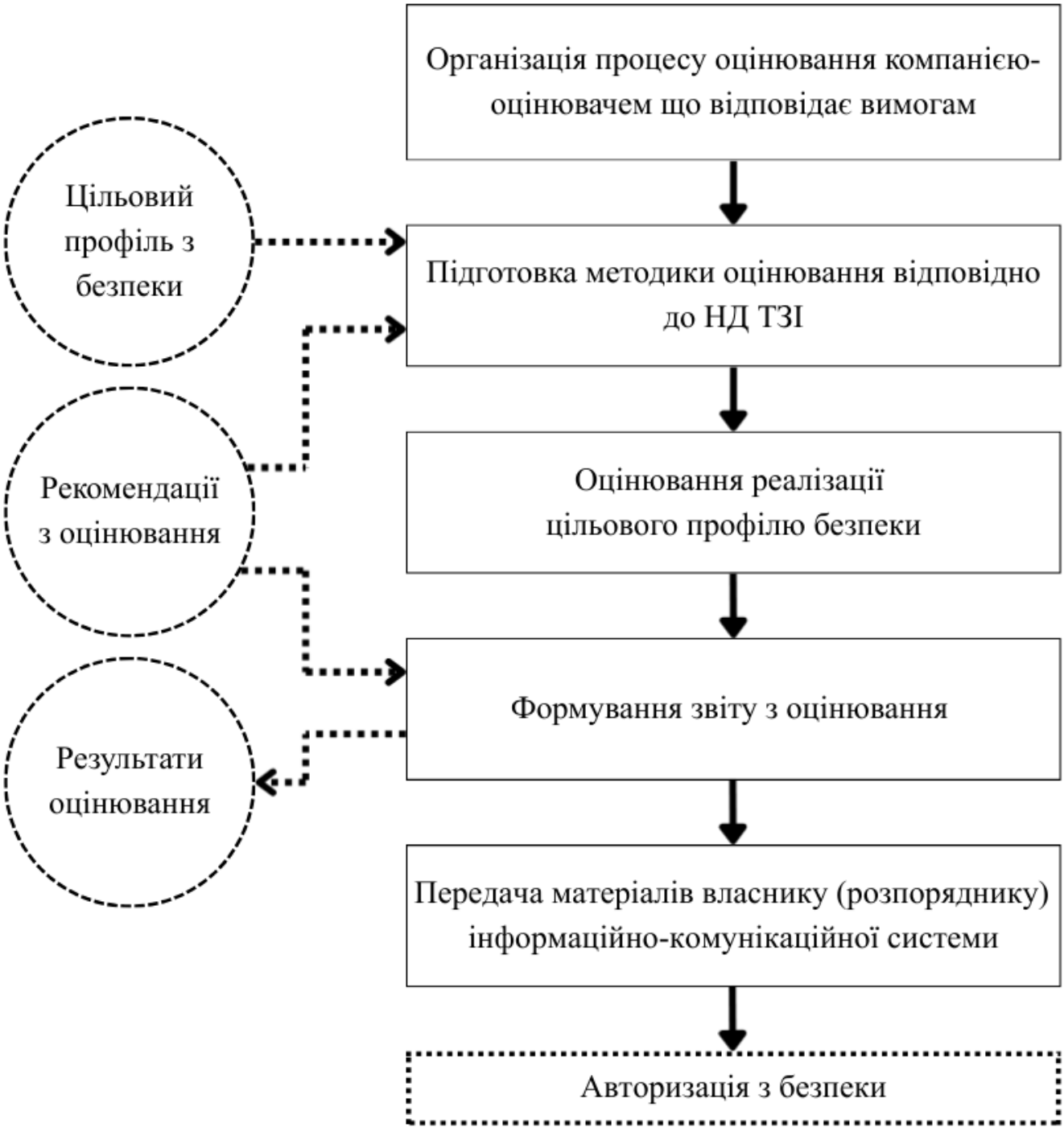

Рис. 1.1. Оцінювання цільового профілю безпеки

1.2.2. Види авторизації автоматизованої системи

Існує 3 види авторизації:

1. Первинна;

2. Планова;

3. Позапланова.

Первинна авторизація з безпеки системи є основним видом авторизації та здійснюється з метою початку функціонування (експлуатації) системи [5].

Планова авторизація з безпеки системи є найпоширенішим видом авторизації та слугує для щорічного підтвердження авторизації системи. При плановій авторизації необхідним є спирання на актуальність та відповідність затвердженому профілю безпеки, що визначається та перевіряється шляхом щорічного перегляду оцінки ризиків.

Планова авторизація з безпеки системи здійснюється протягом життєвого циклу системи, не пізніше одного календарного року після первинної, планової або позапланової авторизації з безпеки системи [5].

Позапланова авторизація з безпеки системи проводиться у разі [5]:

– внесення змін до базового профілю або галузевого профілю, з урахуванням якого був сформований цільовий профіль, якщо інше не передбачено актами, якими затверджуються базовий профіль або галузевий профіль;

– внесення змін до цільового профілю, зокрема в результаті зміни умов функціонування (експлуатації), модернізації системи, або у разі виконання вимог за результатами державного контролю за додержанням вимог законодавства у сферах технічного та криптографічного захисту інформації, кіберзахисту, за станом технічного або криптографічного захисту.

Позапланова авторизація з безпеки системи проводиться протягом шести місяців з дати внесення змін до базового профілю, галузевого профілю або цільового профілю, якщо інше не передбачено нормативно-правовими актами [5].

З узагальненим порядком дій при різних видах авторизацій можна ознайомитись на рисунку 1.2.

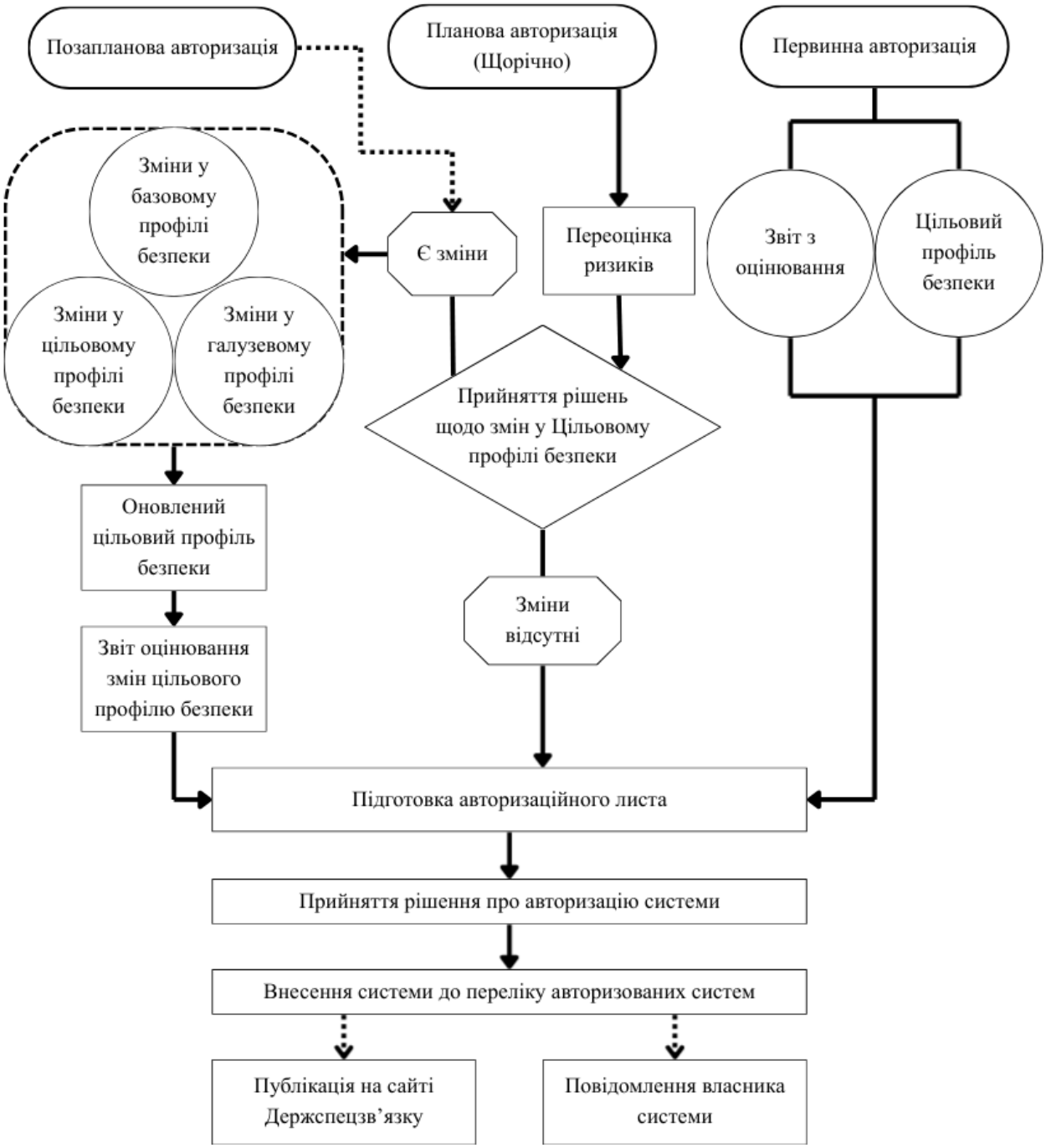

Рис. 1.2. Авторизація

Підставою для подання системи на первинну авторизацію з безпеки системи є позитивні результати оцінювання дотримання вимог цільового профілю, для планової та позапланової авторизації з безпеки системи - позитивні результати оцінювання дотримання вимог цільового профілю у частині, що стосується заходів, які зазнали змін [5].

1.3. Профілі безпеки та класи заходів захисту

В основі процесу створення авторизованої системи безпеки лежать профілі безпеки. Існує 3 види профілів безпеки:

– базовий;

– галузевий;

– цільовий.

Базовий профіль безпеки системи містить мінімальні вимоги з безпеки інформації, які необхідно реалізувати. Перелік вимог встановлюються залежно від класифікації оброблюваної в системі інформації та/або функціонального призначення самої системи.

Галузевий профіль безпеки системи це взаємопов’язана сукупність заходів щодо захисту інформації, визначених для системи органом державної влади, іншим державним органом у межах своїх повноважень у відповідній сфері або галузі з урахуванням мінімальних вимог щодо таких заходів із захисту (базового профілю), відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі, а також надання відповідних рекомендацій [5].

Цільовий профіль безпеки системи є результатом доповнення базового, або за наявності галузевого, профілю безпеки додатковими заходами захисту що визначаються шляхом дослідження особливостей середовища функціонування системи, визначення виду інформації що обробляється в інформаційно-комунікаційній системи та аналізу результатів проведення оцінки ризиків безпеки для конкретної системи. Цільовий профіль безпеки після його формування та перед початком його реалізації потребує затвердження шляхом формування та підписання відповідної настанови або розпорядження.

Усі профілі безпеки структурно є таблицями, що містять перелік вимог що повинні бути реалізовані у системі. Вимоги, у свою чергу, поділено на класи заходів захисту, що складаються з заходів захисту інформації та їхніх посилень.

1.3.1. Класи заходів захисту

Клас заходів захисту — це сукупність заходів захисту, які стосуються конкретного аспекту забезпечення безпеки інформації. Для позначення класу використовується ідентифікатор з двох літер, наприклад УПРАВЛІННЯ ДОСТУПОМ (AC) [6].

Усього визначено 20 класів заходів захисту, їхній перелік представлено у таблиці 1.1.

Таблиця 1.1.

Перелік класів заходів захисту

№	Індекс класу	Назва класу заходів захисту
1.	AC	Управління доступом
2.	AT	Обізнаність і навчання
3.	AU	Аудит і підзвітність
4.	CA	Оцінювання, акредитація та моніторинг безпеки
5.	CM	Управління конфігурацією
6.	CP	Планування безперервної роботи
7.	IA	Ідентифікація та автентифікація
8.	IR	Реагування на інциденти
9.	MA	Технічне обслуговування
10.	MP	Захист носіїв інформації
11.	PE	Фізичний захист і захист робочого середовища
12.	PL	Планування безпеки
13.	PM	Менеджмент інформаційної безпеки
14.	PS	Кадрова безпека
15.	PT	Повноваження на обробку персональних даних
16.	RA	Оцінка ризику
17.	SA	Придбання системи та послуг
18.	SC	Системний і комунікаційний захист
19.	SI	Цілісність системи та інформації
20.	SR	Управління ризиками ланцюга поставок

Управління доступом (AC) – цей клас заходів захисту спрямований на чітке визначення вимог щодо дозволених можливих шляхів отримання доступу до автоматизованої системи, захисту цієї системи від несанкціонованого доступу шляхом забезпечення автентифікації та авторизації легітимних користувачів та/або пристроїв, а також опис механізмів контролю за розповсюдженням інформації,

що класифікована як інформація з обмеженим доступом. Варто зазначити що у межах цього класу захисту до інформації з обмеженим доступом рекомендується віднести у тому числі технологічну інформацію що містить дані про компоненти системи, їхній взаємозв'язок, налаштування політик та системи запису подій. Основним принципом цього класу є мінімізація повноважень як для користувачів, так і для окремих програм та компонентів системи.

Обізнаність і навчання (AT) – цей клас заходів захисту спрямований на забезпечення навчання та підвищення обізнаності для усіх працівників, що взаємодіють з автоматизованою системою. Цим класом заходів захисту регламентується:

– загальна вимога ознайомлення окремого працівника з його правами та обов'язками;

– загальне ознайомлення персоналу з переліком дозволених та недозволених дій в межах автоматизованої системи;

– регулярне підвищення обізнаності про актуальні небезпеки та навчання персоналу правильно визначати;

– ідентифікація та реагування на подібні небезпеки.

Варто зазначити що ці процеси в межах профілю безпеки не мають чіткого переліку тем з якими варто ознайомити персонал, це зроблено задля забезпечення більш гнучкого підходу до навчання та полегшення зміни вектору навчання при виникненні надзвичайних ситуації або глобальних змінах.

Аудит і підзвітність (AT) – цей клас заходів захисту спрямований на забезпечення аудиту системи та регламентування налаштувань аудиту:

– що повинно реєструється;

– як довго потрібно зберігати дані аудиту;

– місце де повинні зберігатися ці дані;

– хто уповноважений ознайомлюватись з цими даними.

Також даний клас заходів захисту регламентує процеси підзвітності та загального плану дій при виявлені небезпечного інциденту у записах аудиту.

Оцінювання, акредитація та моніторинг безпеки (CA) – цей клас заходів захисту спрямований управління ризиками, перевірку автоматизованої системи на наявність вразливостей, реагування на виявлені ризики шляхом формування плану усунення недоліків. Відповідальна реалізація цього класу заходів захисту має вирішальну роль при формуванні механізмів захисту інформацію, розташуванні та налаштуванні системи і її компонентів. Недбале ставлення до цього класу заходів захисту може призвести до виявлення ризиків до яких власник/розпорядник не були готові, а система не мала жодного захисту.

Управління конфігурацією (CM) – цей клас заходів захисту спрямований на налаштування системи та її окремих компонентів шляхом створення документу що буде визначати усі налаштування які стосуються захисту автоматизованої системи, інформації в ній та будуть забезпечувати достатній для виконання покладених на систему завдань рівень працездатності, але не перевищувати його.

Планування безперервної роботи (CP) – цей клас заходів захисту спрямований на забезпечення безперервності роботи автоматизованої системи шляхом створення резервних копій або дублювання компонентів системи задля підвищення відмовостійкості системи.

Ідентифікація та автентифікація (IA) – цей клас заходів захисту спрямований на регламентування вимог та уточнення механізмів автоматизованої системи що спрямовані на забезпечення ідентифікації легітимних користувачів у системі та їхніх повноважень шляхом авторизації та автентифікації. До цього класу засобів захисту також належить і посилення механізмів входу до системи, наприклад застосування двохфакторної автентифікації або впровадження механізмів нестандартної автентифікації в автоматизованій системі.

Реагування на інциденти (IR) – цей клас заходів захисту спрямований на забезпечення чіткого плану дій у нештатних ситуаціях, інцидентах або при підозрах на них. Цим класом засобів захисту забезпечується чітке розмежування обов’язків та прав при виявлені інцидентів та створення відповідної документації, що у майбутньому допоможе персоналу чітко і правильно зреагувати на інциденти.

Технічне обслуговування (MA) – цей клас заходів захисту спрямований на документування необхідних процесів технічного обслуговування, регламентування частоти їхнього проведення, а також визначення та документування можливих способів проведення технічного обслуговування компонентів автоматизованої системи з визначенням відповідних осіб або організацій що можуть його проводити.

Захист носіїв інформації (MP) – цей клас заходів захисту спрямований на правила поводження з носіями інформації:

– флешки;

– диски;

– карти пам’яті;

– дискети;

– інші портативні носії інформації.

В межах цього класу засобів захисту на відповідну особу покладається відповідальність за облік носіїв інформації, слідкування за дотриманням вимог при використанні носіїв інформації, а також їхнє знищення та маркування при винесені їх за межі контрольованої зони.

Фізичний захист і захист робочого середовища (PE) – цей клас заходів захисту спрямований на забезпечення захисту автоматизованої системи та її компонентів від несанкціонованого фізичного втручання, забезпечення їхнього надійного зберігання що дозволить вберегти компоненти від умисного або ненавмисного пошкодження або знищення. В межах цього класу засобів захисту необхідно чітко визначити складові системи, щоб убезпечити їх від підміни, захищеність компонентів від стихійних лих, в особливості пожеж, а також забезпечення збереження цілісності, доступності та конфіденційності інформації в системі навіть під час нестандартних ситуацій.

Планування безпеки (PL) – цей клас заходів захисту спрямований на створення плану захисту інформації та персональних даних який чітко регламентує основні ризики для системи та зазначає шляхи їхнього нівелювання, перелічує усі

заходи захисту та описує організаційні або технічні рішення якими ці заходи захисту були виконані. Також даним документом описується архітектура автоматизованої системи та шляхи взаємодії між її окремими компонентами.

Менеджмент інформаційної безпеки (PM) – цей клас заходів захисту спрямований на документування осіб на яких покладаються визначенні обов'язки що стосуються захисту інформації в автоматизованій системі та описує загальні завдання і процеси що мають виконуватись у межах системи.

Кадрова безпека (PS) – цей клас заходів захисту спрямований на роботу з новими працівниками, починаючи від співбесіди і закінчуючи звільненням або переведенням у інший відділ. Цей клас заходів захисту спрямований на підвищення надійності майбутніх працівників шляхом їхньої перевірки під час працевлаштування, а також забезпечення конфіденційності інформації що оброблялася у системі шляхом зобов'язання її нерозголошення навіть після звільнення або переведення працівника.

Повноваження на обробку персональних даних (PT) – цей клас заходів захисту спрямований на регламентування переліку персональних даних які можуть або будуть оброблятися у автоматизованій системі, перелічення осіб або груп осіб що уповноважені обробляти персональні дані, а також створення документів що будуть регламентувати поводження персоналу автоматизованої системи з персональними даними. Цей клас заходів захисту може бути повністю виключений якщо персональні дані не обробляються у автоматизованій системі або якщо інші класи засобів захисту можуть забезпечити достатній та необхідний рівень компетенції для обробки персональних даних.

Оцінювання ризику (RA) – цей клас заходів захисту спрямований на нормування проведення оцінювання ризиків метою якого є виявлення вразливостей системи та оцінювання вірогідності появи інциденту через певну вразливість. Процес оцінювання ризиків проводиться перед кожною подачею автоматизованої системи на авторизацію.

Придбання системи та послуг (SA) – цей клас заходів захисту спрямований на перевірку ланцюга постачання задля забезпечення якісного надання послуг

сторонніми організаціями, а також уникнення недобросовісних постачальників послуг або продуктів. До цього класу заходів захисту також входить регламентування необхідності перевіряти продукти або рішення на наявність підробок або очевидних вразливостей.

Захист інформаційної системи та комунікацій (SC) – цей клас заходів захисту спрямований на опис схеми автоматизованої системи, взаємозв'язків у середині системи та планових взаємодій з іншими системами в межах виконання покладених на неї функцій. Велика увага цього класу заходів захисту приділена саме забезпеченню надійного та безпечного взаємозв'язку з іншими системами через незахищену мережу.

Цілісність системи та інформації (SI) – цей клас заходів захисту спрямований на забезпечення захист від спотворення інформації у системі шляхом її зараження шкідливим програмним забезпеченням або іншими збоями. Також до цього класу заходів захисту включені вимоги що стосуються регулярних оновлень компонентів системи та протидія подіям що можуть завдати системі функціонувати у штатному режимі.

Управління ризиками ланцюга постачання (SR) – цей клас заходів захисту спрямований на регламентування вимог до постачальника та розрахунок ризику під час постачання продуктів або послуг. Впровадження цього класу засобів захисту зобов'язує організацію створити відділ або призначити людину що буде аналізувати постачальників на доброчесність та перевіряти якість та прозорість угод.

1.3.2. Заходи захисту та посилення заходів захисту

Кожен клас засобів захисту містить певний перелік засобів захисту, деякі з них є обов'язковими до виконання та включені до базового профілю безпеки, інші можуть бути додані ґрунтуючись на особливостях системи, виявлених ризиках або особливостях розміщення чи функціонування системи.

В свою чергу переважна більшість заходів захисту має посилення що містять у собі додаткові вимоги до системи. Посилення може бути застосоване лише за умови впровадження заходу захисту посиленням якого воно є.

Деякі заходи захисту містять більше 20 можливих посилень заходів захисту, переважна більшість з яких може бути реалізована паралельно, доповнюючи одне одного. Однак варто зазначити до у переліку так можуть міститися і взаємовиключні посилення заходів захисту. Саме тому процес формування цільового профілю безпеки вимагає від розробників ретельного дослідження заходів захисту та посилень, що записані у базовому профілі безпеки, а також інших посилень заходів захисту, що були додані в межах формування цільового профілю безпеки.

Кожний клас містить декілька груп заходів захисту (всього 294 групи). Своєю чергою захід захисту може мати декілька посилень (всього 1039 посилених заходів захисту) [6].

Загальна структура заходів захисту приведена на рисунку 1.3 [6].

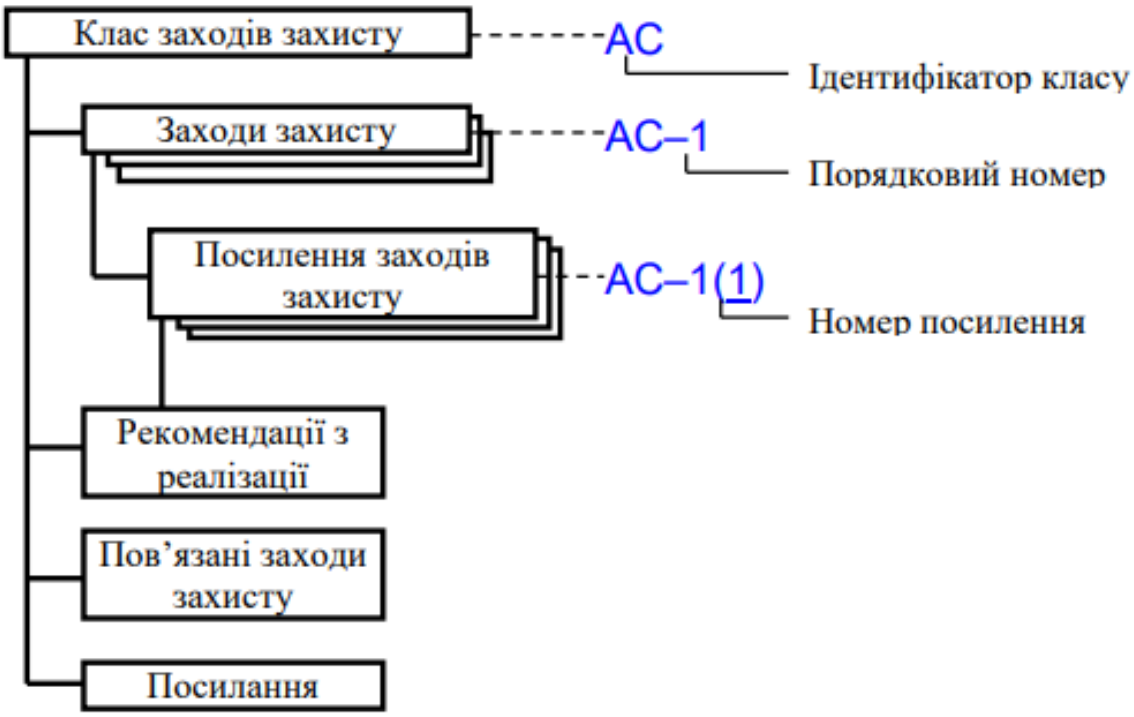

Рис. 1.3. Упорядкування заходів захисту (структура каталогу)

Висновки до розділу 1

Інформацію ділять на типи: відкрита інформація та інформація з обмеженим доступом. Якщо інформаційно-комунікаційна система зберігає, обробляє або передає інформацію що класифікована як інформація з обмеженим доступом, необхідним є створення авторизованої системи з безпеки.

До інформації з обмеженим доступом відносять:

– конфіденційна інформація;

– службова інформація;

– таємна інформація.

В свою чергу таємна інформація поділяється на ще три підрівні в залежності від рівня її секретності на цінності:

– таємна;

– цілком таємна;

– особливої важливості.

Одним з ключових етапів створення захищеної системи з подальшою її авторизацією є виконання вимог цільового профілю безпеки.

В свою чергу цільовий профіль безпеки формується шляхом додавання додаткових заходів захисту та посилень заходів захисту до базового профілю безпеки, вимоги якого є обов’язковими до реалізації.

У деяким випадках для деяких автоматизованих систем може існувати галузевий профіль безпеки, що містить у собі базовий профіль безпеки та деякі додаткові, але також обов’язкові до виконання, вимоги. У такому випадку цільовий профіль безпеки формується базуючись на галузевому профілі безпеки замість базового.

Усі профілі безпеки складаються з заходів захисту та посилень заходів захисту, що об’єднані у класи заходів захисту та представлені у табличному варіанті.

2 РОЗРОБКА ЦІЛЬОВОГО ПРОФІЛЮ БЕЗПЕКИ

Цільовим профілем безпеки інформації є взаємопов’язана сукупність заходів із захисту інформації та їх налаштування, визначених для системи її власником (розпорядником) відповідно до базового профілю (далі – БПБ) з урахуванням вимог законодавства та стандартів у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки в системах, а також призначення системи, її характеристик та особливостей функціонування, результатів проведеної оцінки ризиків [11]. Порядок розробки цільового профілю безпеки приведено на рисунку 2.1 [7].

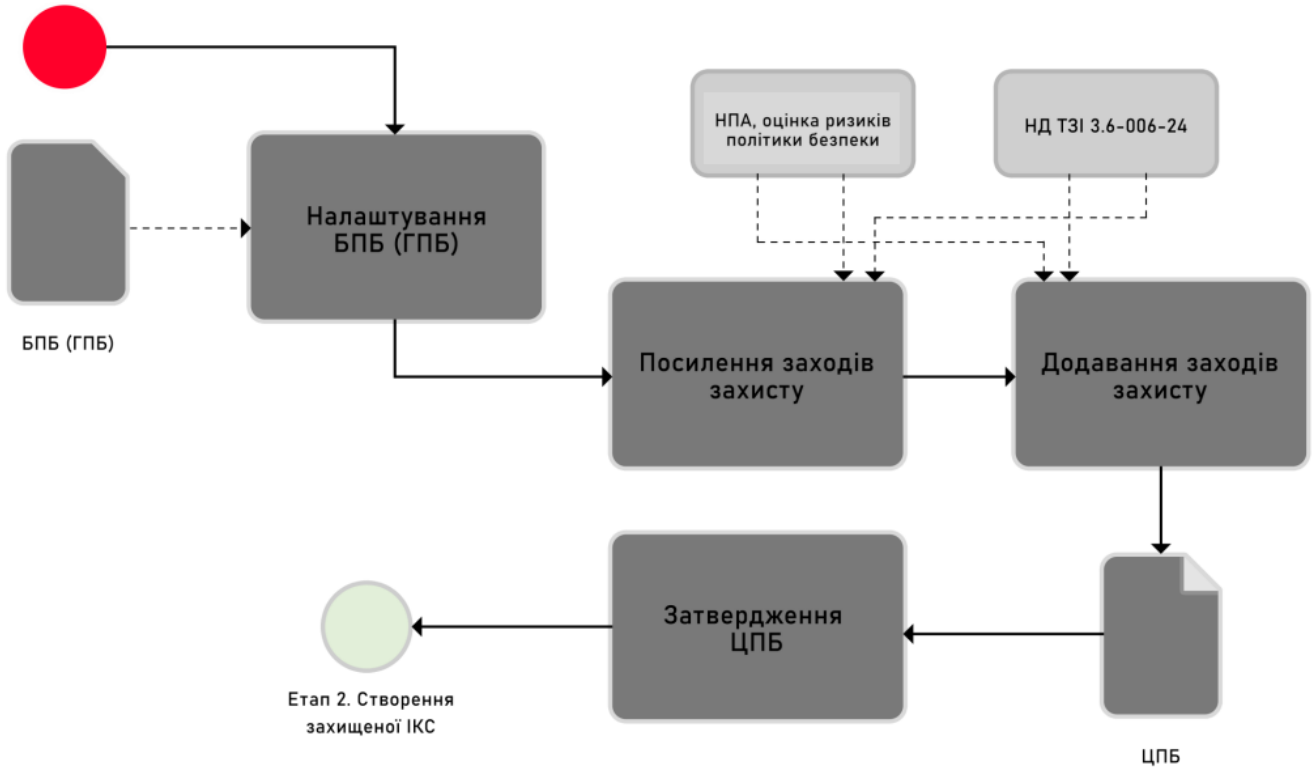

Рис. 2.1. Розробка ЦПБ

Для забезпечення захисту інформації в системі запроваджуються заходи захисту, які призначаються для захисту інформації від [13]:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, зокрема з використанням шкідливого програмного забезпечення;

– кіберзагроз;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Охорона інформації від спеціального впливу на засоби її обробки забезпечується в межах системи, якщо власник інформації ухвалив рішення про необхідність такого захисту.

Захист інформації від витоку технічними каналами здійснюється шляхом використання комплексу технічного захисту з підтвердженою відповідністю у випадках, коли система обробляє дані, що становлять державну таємницю, або коли власник інформації приймає рішення щодо необхідності такого захисту.

Механізми захисту від кіберзагроз впроваджуються за умови поширення на систему вимог Закону України «Про основні засади забезпечення кібербезпеки України».

Об’єктами кіберзахисту є [14]:

– інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

– об’єкти критичної інформаційної інфраструктури;

– інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Порядок формування переліку об’єктів критичної інформаційної інфраструктури та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України [14].

Повноваження щодо формування та забезпечення функціонування реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, регулювання та нагляд за діяльністю на яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг покладаються на Національний банк України [14].

Захист інформації від несанкціонованого доступу, включаючи загрози шкідливого програмного забезпечення, забезпечується у всіх системах.

2.1. Підхід розробки цільового профілю безпеки

Цільовий профіль безпеки (ЦПБ) створюється з метою розробки авторизованої системи з безпеки в інформаційно-комунікаційній системі.

Рекомендована структура цільового профілю безпеки містить [11]:

1) титульний аркуш;

2) загальні відомості про інформаційно-комунікаційну систему:

- назва ІКС;
- відомості про власника ІКС;
- відомості про виконавця робіт з розробки ЦПБ;
- підстава розробки;

- призначення ІКС та функції ІКС;
- загальна архітектура ІКС;
- відомості про обраний базовий профіль безпеки;
- перелік нормативно-правових актів які використовувались при формуванні цільового профілю безпеки, політики безпеки, звіт з оцінки ризиків;

3) ЦПБ.

2.1.1. Титульний аркуш

На титульному аркуші документа представляється назва інформаційно-комунікаційної системи, для якої формується цільовий профіль безпеки. Також зазначається рік укладання, прізвище та ім’я власника системи, його підпис і печатка, що підтверджує затвердження даного профілю безпеки.

Крім того, на титульному аркуші зазначається гриф обмеження доступу до інформації. Затвердження цільового профілю безпеки здійснюється власником (або розпорядником) інформаційно-комунікаційної системи, у межах якої передбачається реалізація авторизованої системи безпеки

2.1.2. Загальні відомості про ІКС

У розділі «Назва ІКС» представлено повну назву інформаційно-комунікаційної системи (ІКС) та її скорочені варіанти що будуть використовуватись у документі.

У розділі «Відомості про власника ІКС» зазначено інформацію щодо власника або розпорядника інформаційно-комунікаційної системи, включаючи назву організації (підприємства, установи) та її юридичну адресу.

У розділі «Відомості про виконавця робіт з розробки ЦПБ» подано дані про розробника авторизованої системи з безпеки. Це включає назву відповідної установи (організації, підприємства) та її місцезнаходження.

Розділ «Підстава розробки» містить перелік нормативно-правових актів, а також внутрішніх документів, таких як накази чи розпорядження, що є підґрунтям для розробки авторизованої системи з безпеки із застосуванням профілів безпеки інформації.

У розділі «Призначення ІКС та функції ІКС» наведені основні відомості про цілі системи, її функціональне призначення, ключові функції та їх технологічні етапи. Також міститься детальний опис організаційних і технологічних заходів захисту інформації, характеристика функціональних особливостей авторизованої системи з безпеки в контексті її призначення, специфіка використання авторизованої системи з безпеки в рамках інформаційної системи з безпеки. Даний розділ є ключовим для розуміння цілей для яких автоматизована система буде створена.

Розділ «Загальна архітектура ІКС» включає детальний опис апаратної складової системи, програмного та комунікаційного забезпечення. На додачу до тексту подається загальна структурна схема системи та її деталізований графічний опис.

У розділі «Відомості про обраний БПБ» висвітлюються нормативно-правові акти, на основі яких було визначено базовий профіль безпеки (БПБ) для оброблюваної в системі інформації.

Розділ «Перелік нормативно-правових актів, які використовувались при розробці ЦПБ» містить перелік нормативно-правових актів і нормативних документів, що регулюють порядок забезпечення захисту даних у рамках функціонування інформаційно-комунікаційної системи.

У розділі «перелік нормативно-правових актів які використовувались при розробці ЦПБ» наводяться нормативно правові акти та нормативні документи, якими регламентується порядок захисту інформації в інформаційно-комунікаційній системі.

2.1.3. ЦПБ

У розділі «ЦПБ» в табличному вигляді наводиться розроблений цільовий профіль безпеки за формою що приведена у таблиці 2.1.

Таблиця 2.1.

Структура цільового профілю безпеки

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1	2	3	4	5

де наводиться наступна інформація [12]:

1 – номер вимоги з безпеки інформації у відповідності до обраного БПБ;

2 – назва вимоги з безпеки інформації у відповідності до обраного БПБ;

3 – зміст вимоги БПБ у відповідності до обраного БПБ;

4 – позначення заходу захисту відповідно до НД ТЗІ 3.6-006-24;

5 – зміст заходу захисту відповідно до НД ТЗІ 3.6-006-24 з визначеними параметрами.

Під час формування цільового профілю безпеки власник або розпорядник системи самостійно обирає стандарти у сфері інформаційного захисту, які застосовуються в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Він визначає шляхи і методи реалізації заходів із захисту інформації відповідно до вимог ЦПБ, а також аналізує наявність в системі інформації з обмеженим доступом. Крім того, власник забезпечує дотримання норм і правил роботи з документами, що містять інформацію з обмеженим доступом.

2.2. Налаштування параметрів заходів захисту цільового профілю безпеки

Заходи захисту характеризуються варіативними параметрами, які необхідно визначати або обирати з переліку під час налаштування профілю безпеки інформаційно-комунікаційної системи, зважаючи на специфічні умови функціонування, особливості її використання, а також структурно-функціональні характеристики самої системи. Крім того, враховуються результати аналізу ризиків, пов’язаних із безпекою.

Зазначений підхід забезпечує можливість адаптації заходів захисту до вимог політики конфіденційності та безпеки, що визначаються конкретними запитами зацікавлених сторін. Оцінка ризиків безпеки відіграє значну роль у процесі встановлення точних параметрів заходів захисту. При цьому відповідальність за вибір, обґрунтування та призначення параметрів кожного із заходів несе виключно власник інформаційної системи.

ODP (Organization-Defined Parameter) являє собою змінну або значення, яке організація повинна самостійно встановлювати для впровадження конкретних заходів безпеки. У багатьох заходах, викладених у НД ТЗІ 3.6-006-24, містяться параметри, які не задаються за замовчуванням, а залишаються на розсуд організації. Це дозволяє організації враховувати власні потреби, ризики, масштаби робіт і доступні ресурси. У тексті заходів захисту НД ТЗІ 3.6-006-24 такий параметр вказується в квадратних дужках. Розберемо детальніше у першому прикладі з яким можна ознайомитись у табличці 2.2.

Висновки першого прикладу, що показаний у таблиці 2.2:

– налаштований зміст заходу захисту є точною цитатою заходу захисту або, як у даному прикладі посилення заходу захисту АС-9(2), з відповідного пункту НД ТЗІ 3.6-006-24;

– змінам підлягають виключно ті частини що виокремлені квадратними дужками;

– якщо текст у квадратних дужках починається зі слова «*Вибір:*», необхідно обрати пункт або декілька пунктів що будуть запропоновані у межах цих квадратних дужок;

– якщо текст у квадратних дужках починається зі слова «*Призначення:*», власнику системи або організації яка виконує формування цільового профілю безпеки необхідно власноруч визначити необхідні вимоги та внести до квадратних дужок;

– після внесення змін до квадратних дужок, дужки залишаються та відокремлюють змінений текст від тексту що не підлягає будь яким редагуванням.

Таблиця 2.2.

Перший приклад оформлення цільового профілю безпеки

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1	…	…	АС-9(2)	Сповіщати користувача, після успішного входу/доступу до системи про кількість *[Вибір: успішних спроб доступу/входу; невдалих спроб входу/доступу; обидва варіанти]* за *[Призначення: визначений організацією період часу]*.

В межах однієї вимоги з безпеки у базовому профілі безпеки може перелічуватись одразу декілька різних заходів захисту або посилень заходів захисту. Розберемо другий приклад що показаний у табличці 2.3.

Таблиця 2.3.

Другий приклад оформлення цільового профілю безпеки

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1	Мінімізація повноважень	Надавати користувачам (або процесам, що діють від імені користувачів) лише авторизований доступ до системи, необхідний для виконання поставлених завдань організації; авторизувати доступ до (призначення: функції безпеки, визначені організацією, таважлива для безпеки інформація); переглянути повноваження, надані користувачам (призначення: періодичність, визначена організацією), щоб підтвердити необхідність таких повноважень; перепризначити або видалити повноваження, за необхідності.	AC-6	…
			AC-6(1)	…
			AC-6(7)	…
			AU-9(4)	…

Висновки другого прикладу, що показаний у таблиці 2.3:

– для реалізації однієї вимоги безпеки базового профілю безпеки можливе залучення одразу кількох заходів захисту та їх посилень, наприклад: AC-6, AC-6(1), AC-6(7) та AU-9(4);

– в межах однієї вимоги з безпеки інформації можливе поєднання заході захисту з різних класів заходів захисту, наприклад AC та AU;

– для впровадження посилень AC-6(1) та AC-6(7) обов'язковим є впровадження AC-6;

– в межах однієї вимоги з безпеки можливе знаходження лише посилення заходу захисту, однак у тому ж профілі безпеки, але у межах іншої вимоги з безпеки інформації обов'язково повинен бути впроваджений відповідний захід захисту, наприклад у прикладі показано посилення AU-9(4) значить у цьому ж профілі безпеки обов'язковим є присутність заходу захисту AU-9.

При доповнені додатковими заходами захисту або посиленнями заходів захисту в межах формування цільового профілю безпеки на основі базового профілю безпеки, що був затверджений адміністрацією Держспецзв'язку, рекомендується їхнє виділення для подальшого спрощення у процесі щорічного перегляду цільового профілю безпеки. Найпростішим способом буде виділення підкресленням або додатковим спеціальним символом після заходу захисту. Такі заходи захисту виносяться у окремі пункти цільового профілю безпеки. Розберемо третій приклад що показаний у табличці 2.4.

Таблиця 2.4.

Третій приклад оформлення цільового профілю безпеки

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1	…	…	AC-6(9)*	Реєструвати виконання привілейованих функцій.

Висновки третього прикладу, що показаний у таблиці 2.4:

– пункти, що були додані у процесі формування цільового профілю безпеки, додають окремими пунктами під окремим номером;

– пункти, що були додані у процесі формування цільового профілю безпеки, рекомендовано виділяти додатковим символом, наприклад AC-6(9)*.

Додаткові заходи захисту та/або їхні посилення, що були додані в результаті формування цільового профілю безпеки, мають особливості внесення інформації: у зв'язку з відсутністю даних пунктів у базовому профілі безпеки, до них не виставлено вимог базового профілю безпеки. Тому замість опису вимог базового профілю безпеки, додаткові заходи захисту дублюють вимогу конкретного заходу захисту або його посилення, але при налаштуванні змісту заходу захисту вимоги базового профілю безпеки редагуванню не підлягають. Розберемо четвертий приклад що показаний у табличці 2.5.

Таблиця 2.5.

Четвертий приклад оформлення цільового профілю безпеки

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1	Навчальні записи	a. Документувати та відстежувати індивідуальні навчальні заходи із забезпечення безпеки та приватності, включно з базовою підготовкою з питань безпеки та приватності, а також спеціальною підготовкою з питань безпеки та приватності	AT-4*	a. Документувати та відстежувати індивідуальні навчальні заходи із забезпечення безпеки та приватності, включно з базовою підготовкою з питань безпеки та приватності, а також спеціальною підготовкою з питань безпеки та приватності

Продовження табл. 2.5.

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		визначених посадових осіб. b. Зберігати індивідуальні записи про навчання впродовж *[Призначення: визначеного організацією періоду часу*].		визначених посадових осіб. b. Зберігати індивідуальні записи про навчання впродовж ***[року]***.

Висновки четвертого прикладу, що показаний у таблиці 2.5:

– при додаванні необов’язкових заходів захисту або їхніх поселень в межах цільового профілю безпеки, колонка «Вимоги БПБ» буде дублювати вміст колонки «Налаштований зміст заходу захисту» без налаштувань;

– після внесення змін до квадратних дужок, дужки залишаються та відокремлюють змінений текст від тексту що не підлягає будь яким редагуванням.

2.3. Адаптація цільового профілю безпеки інформації

Згідно вимог базового профілю безпеки, незалежно від класифікації інформації яка обробляється у інформаційно-комунікаційній системі або особливостей функціонування автоматизованої системи, разом з щорічною плановою авторизацією з безпеки необхідно проводити повторне оцінювання з ризиків на основі даних, що були зібрані у процесі безперервного моніторингу системи.

Постійний моніторинг безпеки інформаційних систем є одним з етапів життєвого циклу системи в організації, що ґрунтується на моделі ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2015 [11]. З цією моделлю, що була модернізована під українське законодавств, можна ознайомитись на рисунку 2.2 [15].

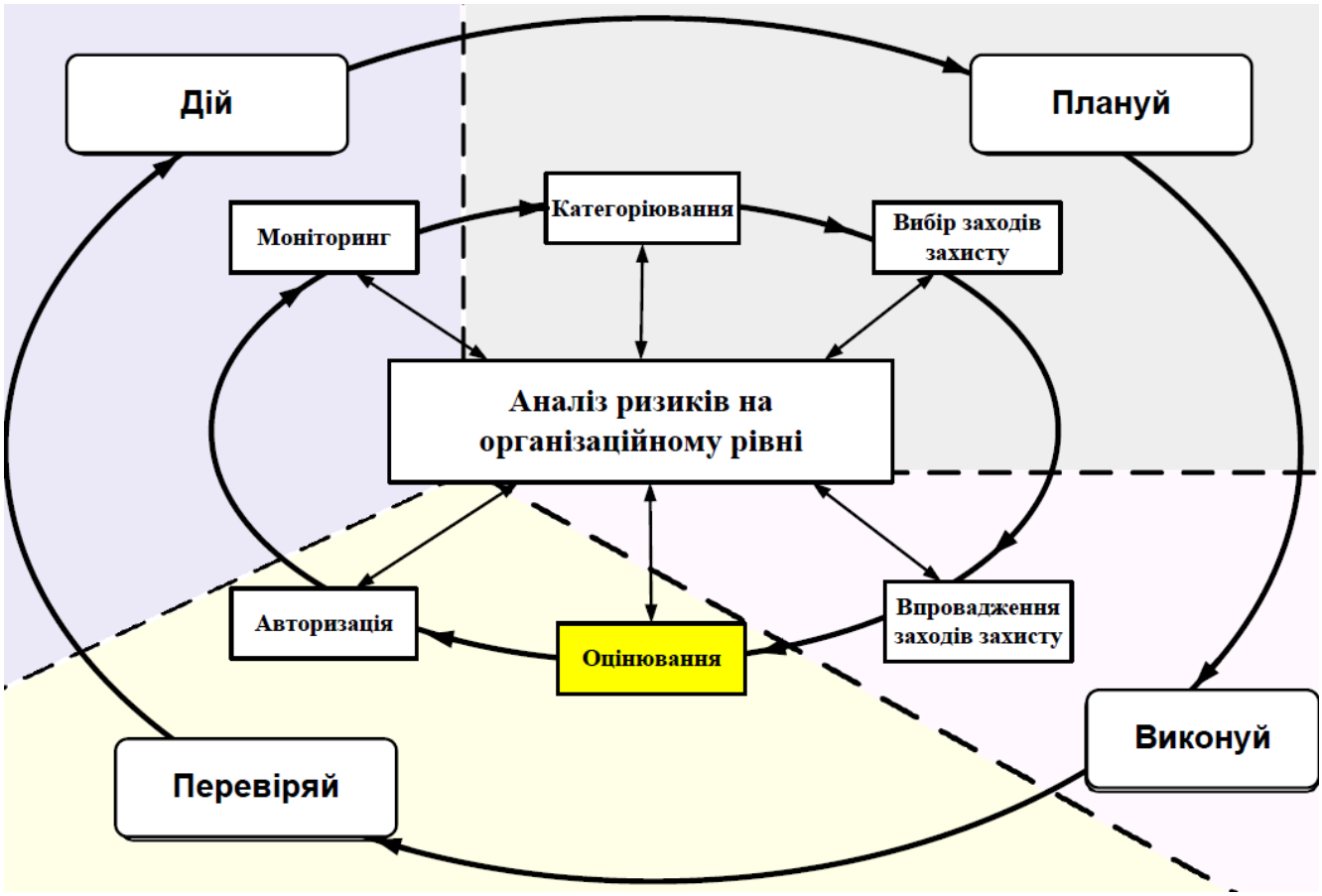

Рис. 2.2. Модель ПВПД

Метою етапу моніторингу безпеки є підтримка обізнаності (поінформованості) про поточний стан безпеки в інформаційно-комунікаційній системі та аргументування прийняття організацією рішень щодо внесення змін до налаштувань системи та цільового профілю безпеки.

Відповідальність за проведення постійного моніторингу безпеки покладається на власника (розпорядника) інформаційно-комунікаційної системи.

Завдання з безперервного моніторингу, аналізу результатів моніторингу, реагування на інциденти, а також внесення необхідних змін до документації

виконується працівниками, на яких покладено функції забезпечення безпеки інформації.

Безперервний моніторинг за окремим компонентами інформаційно-комунікаційної системи можна покласти на інші організації уклавши відповідні договори. В такому випадку важливим є внесення до договору пунктів що будуть вимагати від організації-виконавця надання власнику/розпоряднику системи регулярних звітів що будуть відображати результати моніторингу за останній час та рекомендації щодо усунення інцидентів, якщо такі будуть виявлені.

В залежності від результатів проведеної перевірки результатів моніторингу системи, можливо, необхідним буде внесення змін до базових налаштувань системи або навіть редагування цільового профілю безпеки з метою мінімізувати серйозність наслідків від інциденту або забезпечити захист від повторного інциденту.

Якщо під час проведення постійного моніторингу автоматизованої системи, з метою оперативного реагування на появу нових загроз для системи, було виявлено загрозу яка потребує негайного реагування та внесення змін до цільового профілю безпеки – працівники, що відповідальні за забезпечення захисту у інформаційно-комунікаційній системі, повинні внести необхідні зміни до системи та документації. Після внесення подібних змін до цільового профілю безпеки його класифікація змінюється на адаптивний профіль безпеки.

Адаптивний профіль безпеки стає цільовим профілем безпеки після подання автоматизованої системи на авторизацію з безпеки. Варто зазначити що після внесення змін до профілю безпеки необхідним є проведення повторного оцінювання інформаційно-комунікаційної системи незалежним оцінювачем на відповідність та виконання вимог цільового профілю безпеки.

У таблиці 2.6. наведено короткий опис завдань та очікуваних результатів постійного моніторингу безпеки.

Таблиця 2.6.

Завдання та їх реалізація у межах процесу безперервного моніторингу безпеки

Завдання	Реалізація
Відстеження змін	Внесення до документів пов'язаного інциденту, результатів аналізу інциденту та внесення записів про зміни у налаштуваннях інформаційно-комунікаційної системи
Формування адаптованого профілю безпеки	Редагування цільового профілю безпеки, що перетворює його у адаптований профіль безпеки. Внесення відповідних змін до політики безпеки та плану захисту інформації
Впровадження та подальше оцінювання адаптованого профілю безпеки	Реалізація вимог, що були додані до цільового профілю безпеки у процесі формування адаптованого профілю безпеки, та внесення відповідних записів до документації. Організація проведення незалежного оцінювання інформаційно-комунікаційної системи сертифікованим оцінювачем.
Подання автоматизованої системи на авторизацію з безпеки	Формування авторизаційного листа та направлення його до Держспецзв'язку для їхнього розгляду та внесення до списку авторизованих систем з безпеки

Моніторинг безпеки інформаційно-комунікаційної системи має проводитися протягом усього етапу експлуатації та підтримки системи. Результати, які отримані в рамках постійного моніторингу безпеки інформаційних систем напряму можуть впливати на:

– рівень критичності інформації, яка циркулює в інформаційно-комунікаційної системи;

– вимоги з безпеки до інформаційно-комунікаційної системи;

– адаптований профіль безпеки.

Порядок проведення постійного моніторингу безпеки інформаційних систем наведений на рисунку 2.3.

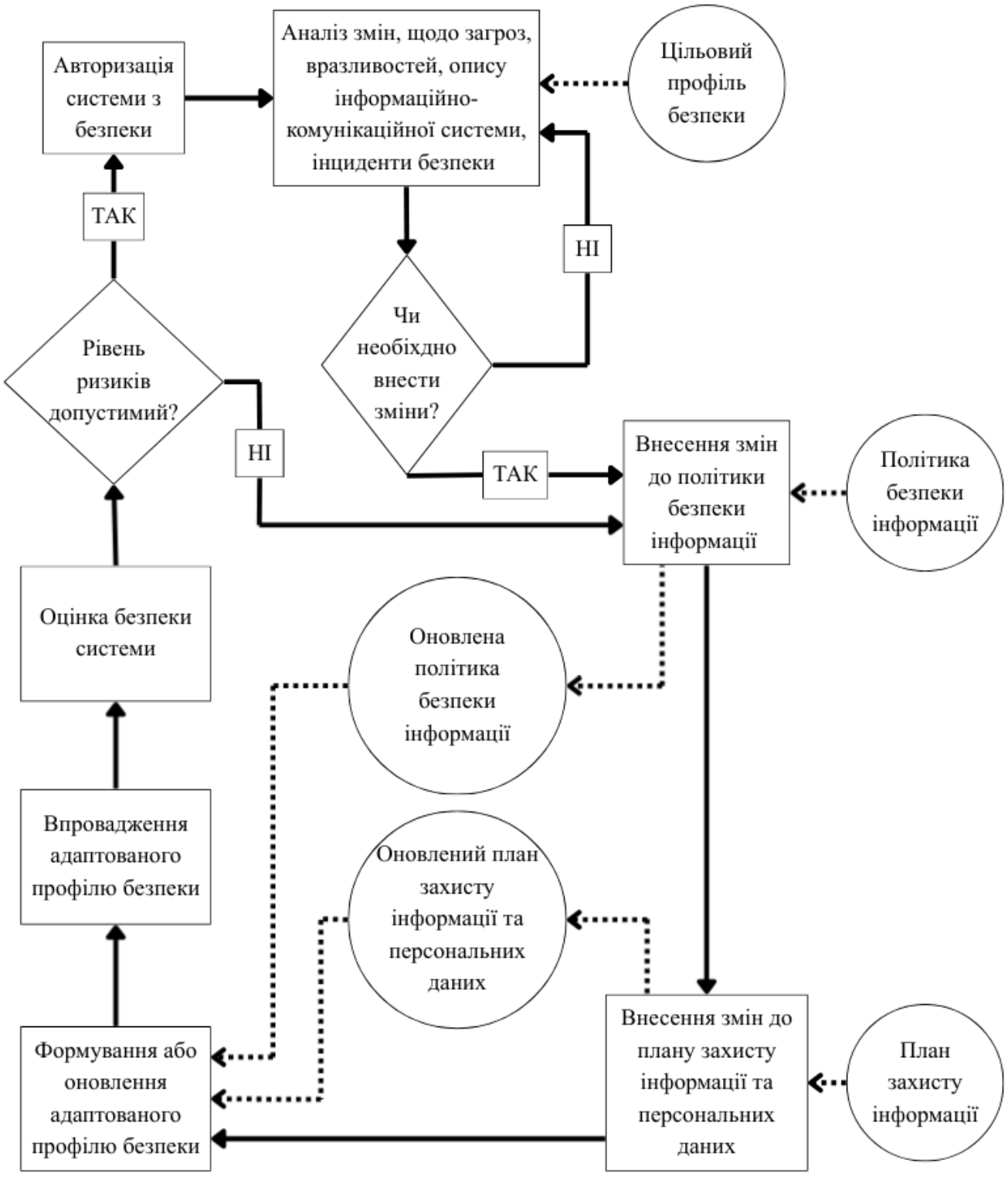

Рис. 2.3. Процес моніторингу безпеки інформаційної системи

Вхідними даними для проведення постійного моніторингу безпеки інформаційних систем виступають [11]:

– концепція безпеки інформації (в частині поточної стратегії управління ризиками) затверджена на організаційному рівні;

– поточні задокументовані результати аналізу ризиків на організаційному та системному рівнях, отримані на етапі аналізу ризиків на організаційному рівні та етапі впровадження заходів захисту (керуючись положеннями НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем») відповідно;

– проектна та експлуатаційна документація на інформаційно-комунікаційну систему, яка входить до складу власника (розпорядника) інформаційно-комунікаційної системи;

– затверджений цільовий профіль безпеки;

– поточні політики безпеки інформації, які були сформовані та затверджені на етапі впровадження заходів захисту;

– поточні плани заходів захисту, які були сформовані та затверджені на етапі впровадження заходів захисту;

– діючі національні законодавчі акти в сфері безпеки інформації.

Висновки до розділу 2

Цільовий профіль безпеки має жорстко регламентовану структуру, яка складається з трьох основних блоків:

– юридичне затвердження: титульний аркуш із грифом обмеження доступу, підписом та печаткою власника;

– контекст системи (загальні відомості): детальний опис того, що ми захищаємо (архітектура, функції, власник) та чому (нормативна база);

– технічна частина (власне ЦПБ): конкретний перелік вимог та заходів.

ЦПБ не є статичним шаблоном. Це гнучкий інструмент, який базується на Базовому профілі безпеки (БПБ), але налаштовується під конкретну організацію.

Використання параметрів, що визначаються організацією (ODP) – це змінні у квадратних дужках, які дозволяють власнику самостійно обирати глибину та складність заходів захисту залежно від наявних ресурсів та потреб.

Також особливістю цільового профілю безпеки є можливість додавати специфічні вимоги, яких немає в базовому профілі, для посилення безпеки.

Створення ЦПБ – це не одноразова дія. Безпека розглядається як безперервний процес згідно з моделлю PDCA (Plan-Do-Check-Act) та включає наступні особливості:

– необхідна щорічна планова авторизація;

– повторне та регулярне оцінювання ризиків;

– постійний моніторинг системи.

3 ОСОБЛИВОСТІ ТА РЕКОМЕНДАЦІЇ ЗІ СТВОРЕННЯ ЦІЛЬОВОГО ПРОФІЛЮ БЕЗПЕКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ З БЕЗПЕКИ ОБ'ЄКТУ КРИТИЧНОЇ ІНФОРАСТРУКТУРИ

3.1. Особливості інформаційно-комунікаційної системи об'єкту критичної інфраструктури

Процес авторизації системи з безпеки для конфіденційної або службової інформації відрізняється від процесу авторизації для інформації що визначена як таємна.

3.1.1 Авторизація з безпеки системи що обробляє конфіденційну або службову інформацію

Авторизація системи безпеки, за винятком систем, де обробляється інформація, що має статус державної таємниці, здійснюється на основі авторизаційного листа, який подає власник або розпорядник зазначеної системи до Адміністрації Держспецзв'язку.

Авторизаційний лист чітко визначений по оформленню та змісту і відповідно не може бути змінений у формулюванні, порядку викладення інформації або зміни формату листа.

Додавання такої системи до переліку авторизованих проводиться Адміністрацією Держспецзв'язку протягом десяти робочих днів після отримання авторизаційного листа, оформленого належним чином, за умови повноти вказаної в ньому інформації згідно з встановленими вимогами.

Особи, які представляють власника або розпорядника системи і подали до Адміністрації Держспецзв'язку відповідний авторизаційний лист, несуть відповідальність згідно із законом за достовірність зазначених у ньому відомостей. Вони також відповідають за правильність і повноту вибору засобів та методів

реалізації заходів безпеки відповідно до обраних профілів, враховуючи вимоги чинного законодавства включно з особливими вимогами певної сфери діяльності та відповідною класифікацією інформації що буде оброблятися у автоматизованій системі. Наприклад при створені системи з захисту інформації з подальшою авторизацією для автоматизованої системи що буде обробляти банківську таємницю необхідно зважати на особливості обробки та захисту цієї інформації.

У випадках, коли авторизаційний лист містить недоліки чи неточності, Адміністрація Держспецзв'язку у межах десяти робочих днів із моменту його отримання повертає документ для доопрацювання власнику або розпоряднику системи із наданням рекомендацій щодо виправлення помилок. Повернення авторизаційного листа відбувається, якщо:

– зазначена в документі інформація є неповною;

– виявлено невідповідності між даними в авторизаційному листі та фактичними даними про систему, її власника чи суб'єкта оцінювання;

– обрано неправильний базовий або галузевий профіль для визначення остаточного профілю безпеки системи, враховуючи тип інформації (відкритої чи з обмеженим доступом) або її функціональне призначення.

3.1.2. Авторизація з безпеки системи що обробляє таємну інформацію

Авторизація системи, у якій обробляється інформація, що належить до державної таємниці, здійснюється на основі авторизаційного листа, форма якого чітко визначена по оформленню та змісту і відповідно не може бути змінена у формулюванні, порядку викладення інформації або зміни формату листа. Цей лист, що подається власником або розпорядником системи до Адміністрації Держспецзв'язку, має супроводжуватися наступними документами:

1. Копія затвердженого цільового профілю, який є основою для здійснення авторизації або внесення змін до системи.

2. Копія звіту щодо оцінки відповідності вимогам цільового профілю. Якщо в профіль внесено зміни, звіт має відображати їх впровадження. У разі відсутності

змін під час проведення планової авторизації надається звіт про відповідність вимогам з підтвердженням відсутності таких змін на основі щорічної оцінки ризиків.

3. Копія документа, який підтверджує оцінку відповідності комплексу технічного захисту інформації.

Адміністрацією Держспецзв'язку рішення щодо авторизації системи безпеки та внесення інформації до реєстру авторизованих систем ухвалюється протягом 30 календарних днів з моменту отримання авторизаційного листа разом з усіма необхідними додатками (авторизаційною документацією). У процесі ухвалення рішення здійснюється аналіз цільового профілю та звіту про дотримання його вимог з метою перевірки відповідності базовому чи галузевому профілю (за наявності), чинному законодавству, національним стандартам і нормативним документам у сферах технічного та криптографічного захисту інформації, а також кіберзахисту.

Також для електронно-обчислювальних систем, які обробляють дані, що становлять державну таємницю, обов'язковим є створення та атестація комплексу технічного захисту інформації (КТЗІ). Цей комплекс має забезпечувати захист інформації з обмеженим доступом від витоків через технічні канали, зокрема через побічні електромагнітні випромінювання та наведень.

3.1.3. Комплекс технічного захисту інформації

Атестація КТЗІ є однією з важливих частин створення КТЗІ і проводиться з метою визначення відповідності вимогам НД з питань ТЗІ виконаних робіт зі створення комплексу ТЗІ на об'єкті інформаційної діяльності (ОІД) та повноти проведених випробувань. Вимоги щодо проведення атестації мають бути передбачені у технічному завданні на створення КТЗІ [10].

Атестація комплексу ТЗІ може бути первинною (при створенні нового КТЗІ), черговою (відповідно до НД ТЗІ через кожні два роки) та позачерговою (у разі змін

умов функціонування ОІД) [10]. Відповідно на стадії розроблення та впровадження нової системи захисту інформації в інформаційно-телекомунікаційних системах, де циркулює інформація, що становить державну таємницю, передбачається створення і проведення первинної атестації комплексу технічного захисту інформації.

Періодичний контроль за станом захищеності інформації від витоків через канали побічних електромагнітних випромінювань та наведень регламентується відповідними нормативно-законодавчими актами з питань технічного захисту інформації.

На етапі розробки та впровадження системи захисту інформації яка становить державну таємницю, в ІТС необхідно створити та провести первинну атестацію КТЗІ, яка включає такі види робіт [8]:

– проведення спеціальних досліджень персональної електронно-обчислювальної машини (ПЕОМ) по каналах ПЕМВН, при якому визначаються можливі канали витоку інформації;

– визначення необхідності встановлення активних та/або пасивних засобів захисту;

– встановлення обладнання з Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність захисту якої визначено законодавством України;

– розробка програми та методики випробовувань;

– проведення оцінки захищеності інформації з обмеженим доступом від витоку технічними каналами на об’єкті ЕОТ (атестація комплексу ТЗІ);

– акустичним та віброакустичним;

– акустоелектричними;

– шляхом застосування закладних пристроїв.

Кожна атестація КТЗІ розпочинається розробленням, погодженням в Держспецзв’язку та затвердженням відповідної програми та методики атестації КТЗІ і закінчується оформленням, затвердженням та реєстрацією в

ДССЗЗІ підсумкового документу – акта атестації КТЗІ, в якому повинні бути відображені [10]:

– підстави для проведення атестації

– дані про виконавця атестації

– результати атестації, висновки за результатами атестації

– термін проведення чергової атестації (строк дії акта атестації)

– можливі зауваження і рекомендації, яких потрібно дотримуватися під час подальшої експлуатації КТЗІ, інші відомості.

Виконавцем атестації комплексу ТЗІ може бути установа, яка має відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку. Відносини між замовником створення та виконавцем атестації комплексу ТЗІ регламентуються укладеним між ними договором [9].

3.2. Особливості доповнення та посилення заходів захисту в межах інформаційно-комунікаційної системи об’єкту критичної інфраструктури

Як вже було зазначено цільовий профіль безпеки – це базовий або, за наявності, галузевий профіль безпеки що було доповнено додатковими заходами захисту та/або їхніми посиленнями. Відповідно крім вимог, що визначені базовим профілем безпеки або, за наявності, галузевим профілем безпеки, усі інші заходи захисту та їхні посилення цілковито залежать від компетентності та уважності розробника системи з безпеки.

Якщо організація (власник) не забезпечить професійного підходу під час оцінювання середовища функціонування та оцінки ризиків, що притаманні та особливі для кожної системи, подальше створення цільового профілю безпеки на основі зібраних даних не зможе забезпечити створення дійсно надійного та відповідного дійсності профілю безпеки.

Цільовий профіль безпеки, незалежно від інформації яку оброблятиме системи, рекомендується доповнити наступними заходами захисту та посиленнями заходів захисту:

- AC-2(1);
- AC-3(7);
- CM-6(1);
- SC-7(21);
- SA-11;
- CP-10;
- PE-3(7);
- MP-6(1);
- MP-6(3);
- PS-4(1);
- SR-11;
- PE-11;
- PE-13;
- MA-2;
- MA-6(2).

3.2.1. AC-2(1) Управління обліковими записами – автоматизоване управління системними обліковими записами

Для великих авторизованих систем з безпеки або автоматизованих системи що обробляють інформацію з високим рівнем секретності, важливим рішенням буде впровадження SIEM систем або аналогічних за функціональністю систем для забезпечення постійного та неперервного процесу моніторингу дій користувачів з подальшим їх аналізом та прийняттям рішень стосовно їхньої небезпечності, незвичайності або підозрілості. Подібні події відповідними системами у автоматичному режимі повинні формуватися у повідомлення для подальшого їх

розгляду відповідальними за захист інформації в інформаційно-комунікаційній системі особами.

Застосування автоматизованих механізмів також може включати такі заходи, як надсилання електронних листів або текстових повідомлень для автоматичного інформування менеджерів облікових записів про завершення роботи користувачів. Сюди також належать використання систем моніторингу активності облікових записів та застосування телефонних сповіщень для повідомлення про нестандартне використання облікового запису.

3.2.2. AC-3(7) Забезпечення доступу – управління доступом на основі ролей

Контроль доступу на основі ролей є стратегією управління доступом, яка забезпечує обмежений доступ до системи лише для авторизованих користувачів. У рамках цієї моделі створюються специфічні ролі, які базуються на завданнях користувачів і пов’язаних із ними дозволах (привілеях), що необхідні для виконання визначених дій у системі. Після призначення організаційної ролі користувач автоматично отримує всі права, передбачені для цієї ролі. Це значно спрощує процес управління привілеями, оскільки права не призначаються окремо кожному користувачеві, що є особливо важливим для великих організацій із численними співробітниками. Замість цього права успадковуються відповідно до розподілу ролей.

3.2.3. CM-6(1) Налаштування конфігурації – автоматизоване управління, застосування та верифікація

Автоматизовані інструменти, зокрема засоби для підвищення безпеки та базової конфігурації, здатні значно покращити точність, узгодженість і доступність відомостей щодо налаштувань конфігурації. Крім того, автоматизація забезпечує ефективну агрегацію й кореляцію даних, впроваджує механізми попередження та

пропонує інформаційні панелі, які сприяють прийняттю обґрунтованих рішень, базованих на аналізі ризиків в організації.

Подібні програмні рішення також сприяють кращому контролю за оновленнями компонентів автоматизованої системи та перевірку правильності їх встановлення на окремих пристроях.

3.2.4. SC-7(21) Захист периметра – ізоляція компонентів системи

Організації здатні відокремлювати складові системи, що виконують різні завдання або бізнес-функції, за рахунок створення ізоляції. Такий підхід дозволяє обмежити несанкціоновані потоки інформації між компонентами системи, одночасно забезпечуючи більш високий рівень захисту для окремих елементів. Ізоляція системних компонентів із використанням периметральних механізмів захисту сприяє підвищенню безпеки певних частин системи та забезпечує кращий контроль і управління потоками інформації між ними. Це також допомагає мінімізувати потенційну шкоду, яка може виникнути внаслідок кібератак чи помилок.

Рівень ізоляції залежить від обраних захисних механізмів. До таких механізмів належать: маршрутизатори, шлюзи та брандмауери, що розділяють компоненти системи на фізично ізольовані мережі чи підмережі; міждоменні пристрої для відокремлення підмереж; засоби віртуалізації; а також технології шифрування даних, що забезпечують захист інформаційних потоків між компонентами системи за допомогою використання різних ключів шифрування.

3.2.5. SA-11 Тестування та оцінювання розробника

Процес тестування і оцінювання розробки підтверджує коректність впровадження необхідних заходів захисту, що функціонують згідно з поставленими завданнями. Ці заходи забезпечують відповідність політиці безпеки та приватності, а також виконання встановлених вимог у цій сфері. Проте, безпека

систем і конфіденційність окремих осіб можуть залежати від взаємодії між складовими системи або змін у цих компонентах. Оновлення чи заміна програмного забезпечення, операційних систем або мікропрограм можуть мати негативний вплив на раніше реалізовані заходи захисту.

Регулярне оцінювання в ході розробки дозволяє проводити додаткові види тестувань і перевірок, які допомагають виявляти та усувати потенційні недоліки. Аналіз програмних компонентів часто потребує таких методів, як ручний перегляд коду, аналіз архітектури безпеки, тестування на проникнення, а також статичний, динамічний, бінарний чи гібридний аналіз.

Плани оцінки безпеки та приватності включають конкретні дії, які повинні виконувати розробники. Це стосується вибору типів аналізу, тестування, перевірок і оглядів програмних компонентів та мікропрограм, визначення рівня суворості процедур, частоти тестувань і перевірок, створення артефактів у процесі виконання цих завдань. Глибина тестувань пов'язана з рівнем деталізації та суворістю перевірок, тоді як їхнє охоплення характеризується кількістю й типом артефактів, що включені до процесу аналізу.

Контракти встановлюють критерії прийнятності для планів оцінки безпеки та приватності, водночас забезпечуючи усунення можливих недоліків і підтвердження ретельного виконання запланованих процедур. Методи верифікації та захисту оцінювальної документації відповідають рівню безпеки або класифікації системи. Крім того, контракти можуть передбачати вимоги щодо належного збереження документації в рамках забезпечення безпеки.

3.2.6. CP-10 Відновлення та відтворення системи

Відновлення передбачає реалізацію комплексу заходів для забезпечення безперервності роботи та відновлення працездатності систем. Цей процес націлений на повернення до нормального функціонування після виникнення непередбачуваних подій. Наступним етапом є відтворення, що включає дії з повного відновлення систем до їхньої початкової продуктивності.

Відновлення та відтворення враховують ключові пріоритети, часові рамки та цільові показники, що визначені в плані забезпечення безперервності діяльності. Під час відтворення ліквідуються всі тимчасові механізми, які могли використовуватися для стабілізації системи. Крім того, цей етап охоплює перевірку відновлених функцій системи, поновлення постійного моніторингу її роботи та підготовку до можливих майбутніх проблем чи загроз.

Всі ці дії можуть бути реалізовані як вручну, так і за допомогою автоматизованих рішень. Організації визначають ключові параметри, такі як допустимий час простою та цільовий рівень відновлення, у рамках загального плану готовності до надзвичайних ситуацій.

3.2.7. PE-3(7) Керування фізичним доступом – фізичні перешкоди

Дане посилення заходу захисту не включено до базового профілю безпеки для конфіденційної та службової інформації, однак використання фізичних перешкод є очевидним та необхідним рішенням для забезпечення компонентів системи від пошкодження, крадіжки або шпигування. До найпоширеніших фізичних перешкод можна віднести: стіни будівлі, двері з замками, вікна з гратами, ролети або жалюзі, інші інженерно-технічні рішення що перешкоджатимуть або ускладнюватимуть доступ зловмисника до компонентів системи.

3.2.8. MP-6(1) Знищення інформації на носіях інформації – перегляд, затвердження, відстеження, документування та перевірка

Організації здійснюють перегляд і затвердження списку носіїв інформації, які підлягають очищенню, щоб забезпечити дотримання політики збереження даних. В рамках цього процесу проводиться відстеження та документування таких дій: формування списку працівників, що відповідають за перегляд і затвердження процедур очищення, визначення типів носіїв інформації, деталізація конкретних файлів розміщених на носіях, вибір методів очищення, фіксація дати й часу

очищення, а також інформації про співробітників, які виконували ці дії. Крім того, організації перевіряють якість проведеного очищення носіїв перед їх остаточним знищенням.

3.2.9. MP-6(3) Знищення інформації на носіях інформації – неруйнівні методи

До портативних пристроїв зберігання даних належать зовнішні або знімні жорсткі диски (зокрема, твердотільні та магнітні), оптичні диски, магнітні чи оптичні стрічки, флеш-накопичувачі, карти пам'яті та інші подібні носії. Ці пристрої можуть стати носіями зловмисного програмного забезпечення. Більш того, багато таких пристроїв походять із ненадійних джерел і мають ризик містити шкідливий код, який легко поширюється через порти USB або інші інтерфейси підключення. Хоча сканування таких пристроїв є рекомендованим заходом безпеки, процедури очищення забезпечують додатковий рівень захисту, гарантуючи відсутність шкідливого програмного забезпечення. Організації часто вдаються до попереднього очищення портативних носіїв, особливо коли вони були придбані у виробників або постачальників, до їхньої експлуатації.

3.2.10. PS-4(1) Звільнення персоналу – вимоги після закінчення трудової діяльності

Після закінчення роботи з інформацією з обмеженим доступом, працівник що звільняється або переводиться має підписати документ про нерозголошення інформації, яку він дізнався в процесі взаємодії з авторизованою системою безпеки.

Даний підхід забезпечить юридичне підґрунтя у разі виникнення інцидентів з розповсюдженням інформації з обмеженим доступом колишніми працівниками. У деяких організаціях цей процес вже реалізовано на моменті підписання договору про працевлаштування, однак для надійності та нагадування працівнику про забезпечення конфіденційності інформації рекомендується або дублювання

(для компаній у яких даний процес впроваджено на етапі працевлаштування) або впровадження в межах автоматизованої системи (якщо подібні дії не заборонялися на етапі працевлаштування).

3.2.11. SR-11 Автентичність компоненту

Виробники, розробники, постачальники та підрядники є основними джерелами підроблених компонентів. Політики та процедури, спрямовані на боротьбу з підробками, покликані забезпечити захист від несанкціонованого доступу, а також гарантувати певний рівень безпеки від проникнення шкідливого програмного забезпечення.

Також варто зазначити що використання підробленого технічного або програмного компоненту може призвести до поломок, збоїв або невиконання певних функцій системи у зв’язку з не правильним програмним-кодом компоненту, використанням неякісних матеріалів або непрофесійної збірки, імітацією повного функціоналу компонента.

3.2.12. PE-11 Аварійне енергозабезпечення

Джерело безперебійного живлення (ДБЖ) є електричною системою, створеною для забезпечення аварійного живлення у випадках відмови основного джерела енергії. Такі пристрої найчастіше застосовуються для захисту комп’ютерів, серверів, центрів обробки даних, мережевого та іншого обладнання, де раптове зникнення електропостачання може викликати збої в роботі, втрату даних, інформації або навіть стати причиною травм чи летальних наслідків.

На відміну від резервних генераторів або аварійних систем електроживлення, ДБЖ забезпечує майже миттєву реакцію на перебої в енергопостачанні, гарантуючи безперервну роботу підключеної апаратури. Час автономної роботи ДБЖ зазвичай є обмеженим, проте його вистачає для безпечного завершення роботи системи або активації альтернативного джерела живлення.

3.2.13. PE-13 Протипожежний захист

Цей захід безпеки стосується зон з високою концентрацією системних компонентів, таких як серверні приміщення, області зберігання інформаційних носіїв або комунікаційні центри. До обладнання або систем пожежогасіння, які можуть вимагати автономного джерела живлення, належать спринклерні установки, стаціонарні пожежні шланги та димові детектори.

Однак забезпечення протипожежної системи або системи пожежного оповіщення для усіх приміщень у яких розміщено компоненти майбутньої авторизованої системи з безпеки не буде зайвим та забезпечить впевненість у безпеці роботи автоматизованої системи.

3.2.14. MA-2 Контрольоване обслуговування

Цей захід спрямований на забезпечення інформаційної безпеки в процесі технічного обслуговування програмного забезпечення та застосунків. У рамках обслуговування системи враховуються також компоненти, які не мають прямого відношення до обробки чи збереження даних або інформації, наприклад, сканери, копіювальні пристрої та принтери.

Для створення якісної документації щодо технічного обслуговування необхідно фіксувати таку інформацію:

– дату і час виконаних робіт;

– імена осіб чи назву групи, яка здійснювала обслуговування;

– за потреби - назву використаного супроводу;

– опис виконаних операцій;

– перелік компонентів системи або обладнання, які були замінені чи вилучені, зокрема їхні серійні або ідентифікаційні номери.

Рівень деталізації записів технічного обслуговування має відповідати вимогам безпеки, визначеним для категорій систем організації.

3.2.15. МА-6(2) Своєчасне обслуговування – планове технічне обслуговування

Для реалізації посилення заходу захисту МА-6(2) необхідним також є впровадження заходу захисту МА-6 Своєчасне обслуговування.

Планове або поточне обслуговування спрямоване на оцінювання технічного стану обладнання шляхом організації періодичного або безперервного (онлайнового) моніторингу. Основним завданням такого обслуговування є здійснення технічних заходів у заздалегідь визначений час, що забезпечує максимальну економічну ефективність і запобігає виходу обладнання з ладу. Цей підхід базується на використанні принципів контролю статистичних процесів, які дозволяють оптимально визначити інтервали для технічного обслуговування. У більшості випадків перевірки та процедури в рамках планового обслуговування виконуються без необхідності зупинки обладнання, що сприяє мінімізації переривань у функціонуванні системи. Такий підхід забезпечує суттєву економію ресурсів та підвищує загальну надійність роботи технічних систем.

3.3. Рекомендації щодо розробки цільового профілю безпеки інформаційно-комунікаційної системи об’єкту критичної інфраструктури

Для розробки цільового профілю безпеки, що буде повністю відповідати особливостям системи та забезпечуватиме її захист та надійність незалежно від джерела ризику, необхідно виявити особливу увагу дослідженню особливостей середовищ функціонування інформаційно-комунікаційної системи.

Незалежно від масштабів організації чи державної установи, для первинного обстеження та оцінювання рекомендується залучення окремої незалежної організації, що має відповідну ліцензію.

Залучення сторонньої незалежної організації дозволить убезпечити та гарантувати неупередженість щодо інформаційно-комунікаційної системи, її особливостей та вразливих місць.

Для повноцінного та всебічного дослідження інформаційно-комунікаційної системи для подальшого якісного створення цільового профілю безпеки, виконавцем робіт з обстеження та попереднього оцінювання автоматизованої системи, рекомендується створити 3 документи:

– акт категоріювання;

– акт обстеження функціонування інформаційно-комунікаційної системи;

– звіт з оцінювання ризиків.

Акт категоріювання був одним з обов’язкових документів при створенні комплексної системи захисту інформації (КСЗІ), що в свою чергу була попередницею авторизованої системи з безпеки в межах якої і створюється цільовий профіль безпеки. У акті категоріювання визначається основна інфорація про класифікацію системи:

– підстава для категоріювання;

– клас автоматизованої системи;

– ступінь обмеження доступу до інформації;

– опис дій які будуть здійснюватися над інформацією.

Акт обстеження функціонування інформаційно-комунікаційної системи також був одним з документів комплексної системи захисту інформації (КСЗІ). В цьому документі особлива увага приділена:

– фізичному середовищу функціонування, включно з описом вже реалізованих механізмів протидії умисному, випадковому або стихійному фізичному втручанню;

– фізичній, мережевій та логічній архітектурі інформаційно-комунікаційної системи з чітким переліком компонентів системи та описом усіх взаємозв’язків між ними;

– особливостям та різновидам інформації яка буде присутня у автоматизованій системі включно з описом формату збереження інформації та загального опису даних що містяться у різних видах інформації;

– переліку ролей у системі, якщо систему планується створювати на основі ролей. У випадку застосування мандатного механізму або застосування атрибутів доступу, усі атрибути або можливі мандати підлягають короткому опису.

Звіт з оцінювання ризиків – документ що містить у собі перелік усіх вразливостей, що були виявлені на етапі обстеження та аналізування середовищ функціонування інформаційно-комунікаційної системи. До основних розділів звіту належать:

– перелік усіх можливих ризиків з їхньої класифікацією за вірогідністю реалізації, наслідків та зальної їх складності;

– виділення серед переліку можливих загроз найнебезпечніших або найчастіших, їхній опис та шляхи реалізації;

– надання рекомендацій щодо їхнього нівелювання або зменшення вірогідності появи чи серйозності наслідків. Усі способи боротьби з ризиками рекомендується підкріпити переліком заходів захисту та/або посилень заходів захисту для подальшого їх впровадження на етапі формування цільового профілю безпеки, за умови що заходи захисту та їх посилення дійсно виконуванні та будуть реалізовані.

Саме тому перед початком формування цільового профілю безпеки дуже важливим є детальне та комплексне обговорення та аналізування з керівництвом власника інформаційно-комунікаційної системи висновків звіту з оцінювання ризиків.

У процесі формування цільового профілю безпеки рекомендовано почати реалізацію вимог цільового профілю безпеки. Це дозволить корегувати вимоги та значення що будуть внесені до цільового профілю безпеки, а також забезпечить більш точну і повну відповідність цільового профіля безпеки реаліям інформаційно-комунікаційної системи.

Для запобігання невідповідностей цільового профілю безпеки відносно реалізованих вимог, не бажано додавати до цільового профілю безпеки додаткові

заходи захисту та посилення заходів захисту що не будуть реалізовані або будуть реалізовано лише частково.

Висновки до розділу 3

Для якісного та професійного формування цільового профілю безпеки рекомендовано заключити договір з організацією що спеціалізується на подібних видах роботи. У процесі формування цільового профілю безпеки дуже важливу роль відіграє попереднє обстеження середовища функціонування інформаційно-комунікаційної системи та якісне дослідження основних ризиків для автоматизованої системи.

Якщо захід захисту або посилення заходу захисту не буде реалізовано у повному обсязі, рекомендується відмовитись від його внесення до цільового профілю безпеки. Виключеннями є заходи захисту та їх посилення що перелічені у базовому профілі безпеки, їхня реалізація є обов’язковою.

ВИСНОВКИ

В даній роботі було проведено аналіз нормативних документів та законів України в сфері захисту інформації для визначення основних вимог щодо захисту інформації з обмеженим доступом, визначено класифікацію інформації та наведено перелік інформації, що відноситься до кожного з класів. В основі процесу забезпечення захисту такої інформації лежить авторизація системи з безпеки, одним з ключових процесів створення захищеної інформаційно-комунікаційної системи з подальшою її авторизацією є обстеження середовищ функціонування, оцінка ризиків та формування, на основі зібраних даних, цільового профілю безпеки з подальшим його затвердженням та реалізацією його вимог. Дана тема є актуальною у зв'язку з необхідністю захисту інформації з обмеженим доступом та у зв'язку з відміною комплексної системи захисту інформації.

Було проаналізовано перелік усіх можливих заходів захисту та посилень заходів захисту, що можуть бути додатково включені до вимог базового профілю безпеки, або галузевого профілю безпеки, під час формування цільового профілю безпеки. Серед вищезгаданих профілів безпеки також варто виділити адаптований профіль безпеки що є тимчасовим цільовим профілем безпеки, що з'являється лише під час позапланових змін цільового профілю безпеки, що можуть виникнути у зв'язку зі змінами базового профілю безпеки або змінами у налаштуваннях, що були викликані певними інцидентами безпеки у межах авторизованої системи з безпеки.

Також в даній роботі наведено перелік рекомендованих до впровадження заходів захисту та/або посилень заходів захисту які допоможуть покращити ефективність роботи авторизованої системи з безпеки шляхом прямого регламентування певних видів робіт та/або налаштування інтервалів проведення цих робіт.

Отже, робота несе у собі ознайомчий характер та має на меті ознайомити читача з особливостями формування цільового профіля безпеки, а також надати розуміння методики написання цільового профіля безпеки. Також робота надає рекомендовані до впровадження, в межах цільового профілю безпеки, заходи захисту та посилення заходів захисту. Ознайомлення з цією роботу дозволить краще зрозуміти сутність цільового профілю безпеки та його важливість під час створення авторизованої системи з безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України. Про захист інформації в інформаційно-комунікаційних системах. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 24.10.2025).

2. Закон України. Про інформацію. Стаття 21. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 25.10.2025).

3. Закон України. Про державну таємницю. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення 26.10.2025).

4. Закон України. Про доступ до публічної інформації. Стаття 7-9. URL: https://zakon.rada.gov.ua/laws/show/2939-17#w1_1 (дата звернення 27.10.2025).

5. Постанова кабінету міністрів України. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем. URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text (дата звернення 28.10.2025).

6. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем, НД ТЗІ 3.6-006-24. Нормативний документ системи технічного захисту інформації. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66109 (дата звернення 29.10.2025).

7. Авторизація з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=70372 (дата звернення 01.11.2025).

8. Створення та атестація комплексів ТЗІ на ОІД. ТЗІ. URL: https://tzi.co.ua/stvorennya-ta-atestaczya-kompleksv-tz-na-od.html (дата звернення 02.11.2025).

9. НД ТЗІ 2.1-002-07, Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. URL: https://tzi.com.ua/downloads/2.1-002-07.pdf (дата звернення 03.11.2025).

10. Атестація КТЗІ. URL: https://usts.kiev.ua/atestatsiia-ktzi/ (дата звернення 04.11.2025).

11. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ з формування цільового профілю безпеки інформації. URL: https://www.cip.gov.ua/services/cm/api/attachment/download?id=68015 (дата звернення 05.11.2025).

12. Базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69624 (дата звернення 08.11.2025).

13. Постанова кабінету міністрів України. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення 15.11.2025).

14. Закон України. Про основні засади забезпечення кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 19.11.2025).

15. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем, НД ТЗІ 2.3-025-24. Нормативний документ системи технічного захисту інформації. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66105 (дата звернення 25.11.2025).