

**НОРМАТИВНИЙ ДОКУМЕНТ**

**СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

**Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці**

**НД ТЗІ 3.6 -004-21**

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Київ 2021

**НОРМАТИВНИЙ ДОКУМЕНТ**

**СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

|  |  |
| --- | --- |
|  | Затверджено  Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України  від " " 20 р. № |

**Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці**

**НД ТЗІ 3.6 -004-21**

Адміністрація Держспецзв'язку

Київ 2021

**ПЕРЕДМОВА**

1 РОЗРОБЛЕНО: Приватним акціонерним товариством "Інститут інформаційних технологій".

2. ВНЕСЕНО: Державною службою спеціального зв’язку та захисту інформації України.

УВЕДЕНО ВПЕРШЕ.

Цей документ не може бути повністю чи частково відтворений, тиражований і розповсюджений без дозволу Адміністрації Державної служби спеціального зв'язку та захисту інформації України

**ЗМІСТ**

[1 Галузь використання 1](#_Toc89505399)

[2 Нормативні посилання 2](#_Toc89505400)

[3 Визначення 3](#_Toc89505401)

[4 Позначення та скорочення 7](#_Toc89505402)

[5. Модель порядку впровадження СБІ 7](#_Toc89505403)

[6. Загальні положення 11](#_Toc89505404)

[6.1 Взаємодія між рівнями системи безпеки інформації Організації 11](#_Toc89505405)

[6.2 Типи заходів захисту та особливості їхнього застосування 12](#_Toc89505406)

[6.3 Документування заходів захисту 14](#_Toc89505407)

[6.4 Етапи розгортання системи безпеки інформації 15](#_Toc89505408)

[7. Впровадження заходів захисту як життєвий цикл розробки IT-систем 20](#_Toc89505409)

[8. Визначення етапів розгортання системи безпеки інформації 22](#_Toc89505410)

[8.1 Етап аналізу ризиків на організаційному рівні 22](#_Toc89505411)

[8.2 Етап категоріювання безпеки 22](#_Toc89505412)

[8.3 Етап вибору заходів захисту 22](#_Toc89505413)

[8.4 Етап впровадження (реалізації) заходів захисту 22](#_Toc89505414)

[8.5 Етап оцінювання безпеки 22](#_Toc89505415)

[8.6 Етап авторизації безпеки інформаційної системи 23](#_Toc89505416)

[8.7 Етап постійного моніторингу безпеки 23](#_Toc89505417)

**НД ТЗІ 3.6 -004-21**

|  |
| --- |
| **Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці** |

Чинний від \_\_\_\_\_\_\_\_\_\_\_\_\_

# 1 Галузь використання

Цей нормативний документ (НД) визначає основи організації та порядок впровадження системи безпеки інформації (СБІ) в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

Цей НД визначає загальну систему дій щодо проектування, впровадження, підтримки та постійного вдосконалення СБІ як частини загальної системи управління організацією, яка ґрунтується на підході управління ризиками безпеки та яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення безпеки інформації у поєднанні зі стратегічними, оперативними та бюджетними процесами планування в організації відповідно до міжнародних стандартів системи менеджменту інформаційної безпеки.

Вимоги цього НД розповсюджуються на інформаційні, інформаційно-комунікаційні, електронні комунікаційні системи, що розгорнуті та експлуатуються державними органами та установами, органами місцевого самоврядування, а також на підприємствах та організаціях всіх форм власності (далі – Організації).

Організаціям приватного сектору рекомендується розглянути можливість використання цього нормативного документа залежно від обставин.

Цей нормативний документ може бути застосований для захисту відкритої інформації, яка міститься в інформаційних системах, для забезпечення її цілісності та доступності.

Нормативний документ може застосовується для вибору та реалізації заходів захисту в інформаційних системах, спрямованих на забезпечення:

* конфіденційності інформації (виключення неавторизованого доступу, копіювання, надання та розповсюдження);
* цілісності інформації (виключення неавторизованого знищення та модифікації);
* доступності інформації (виключення неавторизованого блокування інформації та інформаційної системи).

Досягнення належного рівня безпеки в організації вимагає:

* чітко визначених та чітко сформульованих вимог безпеки та приватності для інформаційних систем і організацій;
* суворого планування безпеки та приватності, а також управління життєвим циклом інформаційної системи й інформації;
* використання надійних компонентів інформаційної системи, сучасних апаратних засобів і програмного забезпечення для захисту інформації;
* застосування системного підходу до забезпечення безпеки та приватності;
* ефективного процесу інтеграції засобів захисту в інформаційні системи;
* застосування добре задокументованих та інтегрованих у процеси практик безпеки та приватності;
* постійного моніторингу інформаційних систем і організацій для визначення поточного стану ефективності заходів захисту, необхідних змін в інформаційних системах і робочих середовищах, а також стану безпеки та приватності в цілому.

Організації мають проводити аналіз і реально оцінювати ризики безпеки для своїх операцій (процесів) і активів, фізичних осіб, інших організацій і держави, які виникають в результаті виконання їхніх завдань і функцій (процесів). Реалістичне оцінювання ризиків безпеки потребує глибокого розуміння загроз безпеки, реалізація яких ґрунтується на вразливостях інформаційних систем і організації в цілому, імовірності та можливих негативних наслідків, що виникають у разі порушення конфіденційності, цілісності, доступності та інших властивостей безпеки. Оцінювання ризиків безпеки також потребує розуміння ризиків приватності. Вимоги безпеки та приватності повинні бути сформульовані з урахуванням стратегії управління ризиками організації з увагою на особливості, витрати, порядок і ефективність впровадження заходів, пов’язаних з проєктуванням, розробкою, придбанням, розгортанням, експлуатацією та підтримкою інформаційних систем організації.

Результати оцінювань ризиків мають бути джерелом інформації для процесу вибору заходів захисту. Процес вибору призводить до формування узгодженого набору заходів захисту — профілю безпеки, що відповідає конкретним потребам організації. Цей процес має бути гнучким для того, щоб організації могли ефективно пристосовуватися до складних і мінливих умов функціонування інформаційних систем та робочого середовища.

Цей НД призначений для посадових осіб, пов'язаних з розробкою, розвитком, впровадженням, оцінкою, експлуатацією, обслуговуванням та розпорядженням Системи, включаючи:

* суб’єктів інформаційних відносин (власників або розпорядників інформаційної системи, користувачів ІС), діяльність яких пов’язана з обробкою інформації, що підлягає захисту;
* осіб, діяльність яких пов’язана з використанням ІС в Організації, забезпеченням безпеки інформації, наглядом або управлінням (наприклад, керівники процесу управління ризиками, уповноважені посадові особи, співробітники підрозділів, що експлуатують інформаційну систему, адміністратори безпеки, співробітників служб захисту інформації та аналогічних підрозділів, відповідальні за безпеку інформації та приватність тощо);
* осіб, відповідальних за розробку та проектування систем безпеки інформації, які можуть залучатися власником (розпорядником ІС) на договірних умовах;
* постачальників послуг безпеки та засобів захисту;
* осіб, відповідальних за проведення оцінювання впроваджених заходів захисту;
* осіб, відповідальних за проведення державної авторизації інформаційних систем.

# 2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі закони, стандарти, політики, регламенти, директиви, інструкції та нормативні документи:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

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

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT);

Постанова Кабінету Міністрів України № 943 від 09.10.2020 р. "Деякі питання об'єктів критичної інформації інфраструктури";

Постанова Кабінету Міністрів України № 1109 від 09.10.2020 р. "Про затвердження Порядку віднесення об’єктів до об’єктів критичної інфраструктури";

ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)»;

НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації» ;

НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» ;

НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем»;

НД ТЗІ 2.3-025-21 «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» ;

НД ТЗІ 2.6-004-21 «Порядок авторизації безпеки інформаційних систем» ;

НД ТЗІ 3.6-008-21 «Порядок моніторингу безпеки інформаційних систем» ;

FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems. 2004;

FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems, 2006;

NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 1.1, April 2018;

NIST Special Publication 800-30. Rev.1. Guide for Conducting Risk Assessments, 2012;

NIST Special Publication 800-37. Rev.2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018;

NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View, 2011;

NIST Special Publication 800-53. Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020;

NIST Special Publication 800-64. Rev.2. Security Considerations in the System Development Life Cycle, 2008;

NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems, 2011;

NIST Special Publication 800-160 Vol. 1. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2018;

NIST Special Publication 800-160 Vol. 2. Developing Cyber Resilient Systems: A Systems Security Engineering Approach, 2019.

# 3 Визначення

У цьому НД ТЗI подано терміни та визначення згідно із ДСТУ 3396.2, ДСТУ 2226, НД ТЗІ 1.1-003.

Інші терміни вживаються у такому значенні:

**інформаційна (автоматизована) система** — організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

**електронна комунікаційна система** — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

**інформаційно-комунікаційна система** — сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Далі по тексту документа для всіх систем буде використовуватися термін **інформаційні системи (ІС).**

**Категоріювання безпеки** — процес визначення категорії безпеки ІС на основі рівня критичності інформації, яка циркулює всередині такої ІС у контексті рівня негативних наслідків (шкоди) в разі порушення конфіденційності, цілісності та доступності інформаційних активів.

**Категорія критичності системи (КК)** — характеристика ІС, що ґрунтується на оцінюванні потенційного впливу (шкоди) від втрати конфіденційності, цілісності або доступності інформації, яка циркулює в ІС на діяльність організації, активи організації, фізичних осіб, інші організації або державу. Встановлено три категорії критичності ІС — низька, середня та висока.

**Рівень критичності інформації (РК)** — характеристика інформації, яка відображає ступінь важливості інформації. Під ступенем важливості слід розуміти можливі негативні наслідки для особи, організацій, держави або суспільства в разі порушення конфіденційності, цілісності або доступності інформації.

**Система з високою категорією критичності** — ІС, у разі порушення однієї з властивостей (конфіденційності, цілісності, доступності) інформації, яка циркулює в ІС, можливі суттєві негативні наслідки для діяльності організації, а сама ІС та/або організація не може виконувати свої функції (завдання, процеси) за призначенням.

**Система з середньою категорією критичності** — ІС, у разі порушення однієї з властивостей (конфіденційності, цілісності, доступності) інформації, яка циркулює в ІС, можливі помірні негативні наслідки для діяльності організації, а сама ІС та/або організація не може виконувати хоча б одну зі своїх функцій (завдань, процесів) за призначенням або виконує функції із суттєвим зниженням ефективності.

**Система з низькою категорією критичності** — ІС, у разі порушення однієї з властивостей (конфіденційності, цілісності, доступності) інформації, яка циркулює в ІС, можливі незначні негативні наслідки для діяльності організації а сама ІС та/або організація може виконувати свої функції (завдання, процеси) за призначенням з недостатньою ефективністю або виконання функцій можливо лише із залученням додаткових ресурсів і засобів.

**Інцидент** — подія, яка теоретично або фактично загрожує конфіденційності та/або цілісності та/або доступності інформації або інформаційної системи; або являє собою порушення чи неминучу загрозу порушення закону, політики безпеки, процедур безпеки або прийнятних правил використання.

**Вимога безпеки** — твердження, яке виражає конкретну потребу в безпеці інформації (активу), включно із супутніми обмеженнями та умовами. Вимога безпеки, що висувається до інформації, інформаційної системи чи організації, може походити з різних джерел, серед яких, наприклад, закони, розпорядчі документи уряду, нормативні документи, міжнародні, національні та галузеві стандарти, накази, директиви, правила (політики), положення, а також потреби конкретної організації.

**Вимоги приватності** — вимоги,спрямовані на захист особистого життя приватних осіб, що пов’язано зі створенням, збиранням, використанням, обробкою, зберіганням, поширенням, розкриттям чи видаленням персональних даних.

**Концепція безпеки інформації та приватності** — офіційний документ, прийнятий на вищому організаційному рівні, який закріплює основні положення та відношення вищого керівництва щодо питань інформаційної безпеки організації, закріплює вимоги безпеки та приватності, а також прийняті організацією ризики.

**Програма безпеки інформації та приватності** – офіційний документи системного рівня, який наслідує принципи Концепції безпеки інформації та надає їхню специфікацію для конкретної інформаційної системи.

**Політика безпеки інформації** — документ або сукупність документів системного рівня, які містить набір вимог, правил, обмежень, рекомендацій, що регламентують порядок інформаційної діяльності в ІС і спрямовані на досягнення і підтримку стану інформаційної безпеки системи та організації в цілому.

**План заходів захисту** — документ або сукупність документів системного рівня, які детально описують заходи захисту, вибрані для інформаційної системи для задоволення відповідних вимог безпеки та приватності й управління ризиками приватності; детально описують залучені способи/ролі управління, методології та показники, які використовуватимуться для оцінювання заходів захисту інформації та персональних даних.

**Профіль безпеки (ПБ)** — набір заходів захисту, які застосовуються до інформації або ІС для задоволення вимог чинної нормативної бази, а також спрямовані на захист потреб з метою управління ризиками безпеки.

**Базовий профіль безпеки (БПБ)** — це мінімальний набір заходів захисту, встановлених для відповідної категорії критичності ІС, який є відправною точкою для наступних налаштувань, що можуть бути застосовані до базового профілю безпеки для створення галузевого, цільового та адаптованого профілів безпеки інформаційної системи.

**Галузевий профіль безпеки (ГПБ)** — це визначений набір заходів захисту, посилених заходів захисту та додаткових рекомендацій, отриманих на основі налаштування й уточнення базового профілю безпеки з урахуванням особливостей галузі.

**Цільовий профіль безпеки (ЦПБ)** — це визначений набір заходів захисту, посилених заходів захисту та додаткових рекомендацій, отриманих на основі налаштування й уточнення базового (галузевого) профілю безпеки з урахуванням вимог чинного законодавства, нормативних документів, стандартів, політик безпеки, призначення інформаційної системи, структурно-функціональних характеристик інформаційної системи, результатів аналізу ризиків безпеки та особливостей функціонування інформаційної системи.

**Адаптований профіль безпеки (АПБ)** — це визначений набір заходів захисту, удосконалень заходів захисту та додаткових рекомендацій, отриманих на плановій основі за встановленими термінами перегляду цільового профілю безпеки.

**Заходи захисту інформації** — заходи або контрзаходи, передбачені для впровадження в ІС або організації для захисту конфіденційності, цілісності та доступності інформації, що циркулює в ІС.

**Заходи захисту персональних даних** — організаційні, технічні та фізичні заходи захисту, що використовуються в організації для дотримання вимог щодо приватності та управління ризиками приватності.

**Оцінювання заходів захисту** — тестування заходів захисту в ІС з метою визначення міри коректності впровадження, а також визначення того, чи працюють вони за призначенням і чи досягають бажаного результату стосовно дотримання вимог безпеки або приватності, що висуваються.

**Загальний захід захисту** — захід захисту, який успадковується декількома інформаційними системами.

**Успадкований захід захисту** — захід захисту, реалізований, коли інформаційна система отримує результати захисту від впровадженого заходу захисту, що контролюється, впроваджується (реалізується), оцінюється, санкціонується суб’єктами, які не несуть відповідальності за цю інформаційну систему.

**Компенсаційні заходи захисту** — заходи захисту, які застосовуються замість (на додаток до) заходів, що занесені в базовий профіль безпеки.

**Специфічні заходи захисту** — заходи захисту, що реалізуються на системному рівні та не успадковуються жодною іншою інформаційною системою.

**Гібридний захід захисту** — захід захисту, що реалізується для інформаційної системи, частково як загальний захід, а частково як специфічний.

**Посилення** **заходу** — розширення заходу захисту для створення додаткової, але пов’язаної з первинною, функціональності або для збільшення рівня гарантій.

**Рекомендації з реалізації** — положення, що використовуються для надання додаткової пояснювальної інформації для заходу безпеки або посилення заходу безпеки.

**Цифрова ідентичність** — інформація про сутність, яка використовується комп’ютерними системами для представлення зовнішнього агенту. Цей агент може бути фізичною особою, організацією, застосунком або пристроєм.

**Відкрита інформація** — інформація, яка може міститися на загальнодоступних ресурсах і до якої висуваються вимоги збереження цілісності та доступності.

**Інформація з обмеженим доступом** — інформація, доступ до якої може здійснюватися лише авторизованими цифровими ідентичностями. До інформації з обмеженим доступом належать: персональні дані, критична інформація, секретна інформація.

**Персональні дані (ПД)** — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

**Критична інформація** — інформація з обмеженим доступом, яка не містить ознак державної таємниці, порушення конфіденційності та/або цілісності та/або доступності якої може мати негативні наслідки (негативний вплив) для власника інформації та/або ІС, у якій циркулює така інформація.

**Секретна інформація** — інформація, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України.

**Роль** — визначена сукупність правил, які встановлюють рамки взаємодії між користувачем та інформаційною системою.

**Управління доступом на основі ролей** — набір дозволів доступу, який цифрова ідентичність отримує на основі явного або неявного припущення про певну роль.

**Життєвий цикл інформації** — етапи, через які проходить інформація, наприклад: створення або збір, обробка, поширення, використання, зберігання і розпорядження, включно зі знищенням і видаленням.

**Ланцюг довіри, ланцюг постачання** — певний рівень довіри під час взаємодії в ланцюгу постачання такий, що кожен учасник відносин «споживач-постачальник» забезпечує належний захист своїх компонентів продуктів, систем і послуг.

**Робоче середовище** — фізичне оточення, в якому ІС обробляє, зберігає та передає інформацію.

**Зовнішня система** — система (або компонент системи), що перебувають поза авторизаційними межами, встановленими організацією і над яким організація, як правило, не має прямого контролю.

**Підсистема** — підрозділ або компонент ІС, що складається з інформації, інформаційних технологій і персоналу, який виконує одну чи кілька конкретних функцій.

**Компонент системи** — дискретний ідентифікований актив інформаційних технологій, який являє собою функціональний блок системи й може містити апаратне та/або програмне забезпечення.

**Зовнішні системні служби** — системна послуга, яка реалізується поза авторизаційними межами організаційної системи (тобто послуга, яка використовується системою, але не є її частиною) і над якою організація, як правило, не має прямого контролю.

**Провайдер зовнішньої системної служби** — постачальник зовнішніх системних служб через різноманітні відносини «споживач-виробник» (включно з, але не обмежуючись: спільними підприємствами; діловим партнерством; аутсорсингом; ліцензійними угодами; та/або обміном ланцюгами постачань).

**Авторизація ІС** – офіційне управлінське рішення, що надається уповноваженим на авторизацію органом для надання дозволу на використання СБІ на основі інформації, наданої в пакеті авторизації, який був підготовлений Організацією та переданий уповноваженому органу з авторизації;

**Уповноважений орган з авторизації –** центральний орган виконавчої влади, інший державний орган, який здійснює функції авторизації;

**Пакет авторизації** – перелік документації, який надається Власником (Розпорядником) ІС до уповноваженого органу для проходження процедури державної авторизації;

**Реєстр авторизованих систем** – перелік ІС, які успішно пройшли процедуру державної авторизації.

**Постійний моніторинг безпеки** – набір процедур, направлених на підтримку обізнаності (поінформованості) про поточний стан безпеки та приватності в ІС та Організації для прийняття рішень щодо управління ризиками безпеки.

# 4 Позначення та скорочення

У цьому НД використано такі позначення та скорочення:

НД – Нормативний документ

СБІ – Система безпеки інформації

БІ – Безпека інформації

ІС – Інформаційна система

ПД – Персональні дані

ІТ – Інформаційна технологія

ОТ – Операційна технологія

SDLC – Життєвий цикл розробки системи (System Development Life Cycle).

КК – Категорія критичності

РК – Рівень критичності

ПБ – Профіль безпеки

БПБ – Базовий профіль безпеки

ГПБ – Галузевий профіль безпеки

ЦПБ – Цільовий профіль безпеки

АПБ – Адаптований профіль безпеки

ЗЗ – Заходи захисту

ПЗЗ – План заходів захисту

# 5. Модель порядку впровадження СБІ

Впроваджені системи безпеки інформації (СБІ) мають забезпечувати задоволення вимог щодо захисту інформації. Такі вимоги можуть бути сформульовані національними та міжнародними інстанціями. Необхідною умовою забезпечення інтероперабельності національних систем з міжнародними партнерами є можливість легкого впровадження міжнародних стандартів у галузі безпеки інформації FIPS PUB 199, FIPS PUB 200, NIST Special Publication 800-30, NIST Special Publication 800-37, NIST Special Publication 800-39, NIST Special Publication 800-53, NIST Special Publication 800-64, NIST Special Publication 800-128, NIST Special Publication 800-160. Для більш швидкого та ефективного розроблення СБІ необхідним вбачається впровадження механізму, який здатен забезпечити легкий процес інтеграції галузевих національних та міжнародних стандартів безпеки.

При побудові СБІ має бути забезпечена можливість «персоналізації» даного процесу для кожної ІС. Під персоналізацією розуміється можливість гнучкого процесу проектування системи безпеки інформації, яка максимально забезпечує задоволення потреб конкретної ІС та є економічно ефективною.

Рішення щодо типу СБІ для розгортання в конкретній ІС має прийматися в залежності від типу ІС та інформації, яка в ній циркулює. В рамках даного НД для визначення типу інформації використовується наступна класифікація інформації за типом властивостей, що забезпечуються (рисунок 5.1).

Інформація

Відкрита інформація

Інформація з обмеженим доступом

Персональні дані

Критична інформація

Секретна інформація

Рисунок 5.1 – Класифікація інформації за типом властивостей, що забезпечуються

Для рішення щодо типу СБІ, яка розгортається в ІС використовується наступна модель (таблиця 5.1).

Власники інформаційних систем, які обробляють відкриту інформацію не залежно від форми власності ІС, мають розгортати системи безпеки інформації (СБІ) керуючись положеннями цього нормативного документу для впровадження відповідних заходів захисту, направлених на забезпечення цілісності та доступності відкритої інформації, яка циркулює у даних ІС.

Власники ІС, які обробляють будь-які ПД, не залежно від форми власності ІС, мають розгортати СБІ керуючись положеннями цього нормативного документу, а також вимог національного стандарту ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)» для впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності ПД. Власники ІС, які обробляють ПД та знаходяться у приватній власності додатково можуть прийняти рішення щодо впровадження відповідності ІС вимогам міжнародних Регламентів (GDPR).

Критична інформація розрізняється за рівнем критичності: низький, середній, високий. До критичної інформації також належать: комерційна таємниця, банківська таємниця, таємниця слідства, службова інформація тощо.

Державні ІС, у яких циркулює критична інформація, мають розгортати СБІ керуючись положеннями цього нормативного документу для впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності критичної інформації, яка циркулює у таких ІС.

ІС, які відповідно до Постанови Кабінету Міністрів України № 943 від 09.10.2020 р. та Постанови Кабінету Міністрів України № 1109 від 09.10.2020 р., розгортаються на ОКІІ I-ІI категорії критичності мають розгортати СБІ керуючись положеннями цього нормативного документу для впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності критичної інформації, яка циркулює у таких ІС. ІС, які відповідно до Постанови Кабінету Міністрів України № 943 від 09.10.2020 р. та Постанови Кабінету Міністрів України № 1109 від 09.10.2020 р., розгортаються на ОКІІ III - IV категорії критичності можуть розгортати СБІ керуючись положеннями цього нормативного документу або міжнародних стандартів, враховуючи особливості ІС та умов її функціонування. Незалежно від категорії критичності об’єкти критичної інфраструктури, у інформаційних системах, у яких циркулює критична інформація, мають проходити процедуру державної авторизації розгорнутої СБІ.

ІС, у яких циркулює секретна інформація мають розгортати комплексну систему захисту інформації (КСЗІ), керуючись вимогами чинного національного законодавства.

Таблиця 5.1 – Модель впровадження системи безпеки інформації

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Типи інформації  Типи ІС | | Інформація з обмеженим доступом | | | | | | | | Відкрита інформація |
| Секретна | | | Критична інформація | | | | Персональні дані |
| Гриф секретності | | | Рівень критичності | | | |
| Т | ЦТ | ОВ | Високий | Середній | | Низький |
| Державні ІС | | Комплексні системи захисту інформації (КСЗІ) | | | СБІ відповідно до національних вимог  + державна авторизація | | | | СБІ відповідно до національних вимог  Додаткові вимоги ДСТУ 7731:2015 | СБІ |
| ОКІІ | I/II категорія критичності | КСЗІ | | | СБІ відповідно до національних вимог  + державна авторизація | | | | СБІ відповідно до національних вимог  Додаткові вимоги ДСТУ 7731:2015 | СБІ |
| III/IV категорія критичності | СБІ відповідно до національних /міжнародних вимог  + державна авторизація | | | |
| ІС у приватній власності | | КСЗІ | | | СБІ відповідно до національних/міжнародних вимог | | | | СБІ відповідно до національних вимог  Додаткові вимоги ДСТУ 7731:2015 / GDPR | СБІ |
| Класифікація ІС | | Відповідно до НД ТЗІ 2.5-005 -99  АС клас 1  АС клас 2  АС клас 3 | | | Відповідно до НД ТЗІ 3.6-004-21 | | | | - | - |
| ІС з високою  категорією  критичності | | ІС з середньою  категорією  критичності | ІС з низькою  категорією  критичності |

# 6. Загальні положення

## 6.1 Взаємодія між рівнями системи безпеки інформації Організації

Система безпеки інформації - частина загальної системи управління, яка ґрунтується на підході, що враховує [ризики інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%A0%D0%B8%D0%B7%D0%B8%D0%BA_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)), призначена для розроблення, впровадження, функціонування, [моніторингу](https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3), перегляду, підтримування та вдосконалення [інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) в Організації.

СБІ повинна забезпечити безпечність та надійність виконання функцій/-процесів за призначенням Організації. Впровадження та функціонування СБІ стосується всіх підрозділів Організації. Тому відповідальні особи повинні брати участь у вирішенні питань, що належать до сфери їх відповідальності, під час впровадження та функціонування СБІ.

Цілі СБІ, заходи захисту (існуючі або ті, що будуть впроваджені), документація, що описує функціонування СБІ, повинні бути зрозумілими для всіх зацікавлених сторін (стейкхолдерів).

Впровадження в Організації СБІ дозволить:

- оптимізувати вартість побудови та підтримання системи інформаційної безпеки;

- постійно відслідковувати та оцінювати ризики безпеки з урахуванням призначення (місії) Організації (цілей бізнесу);

- ефективно виявляти ризики безпеки та знижати ймовірність їх виникнення;

- розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;

- ефективно розробляти, впроваджувати та тестувати заходи захисту інформації;

- забезпечити розуміння питань інформаційної безпеки та приватності керівництвом та всіма працівниками Організації.

Управління ризиками безпеки та приватності вимагає участі посадових осіб на всіх ланках управління Організації – від керівництва, що визначає стратегічне бачення (місію), цілі та задачі для Організації, до керівників середньої ланки, які здійснюють планування, виконання та управління функціями/процесами, та осіб, які розробляють, впроваджують, використовують і підтримують системи та процеси управління ризиками. Такий підхід підтримує виконання функціональних завдань Організації та реалізації процесів. Управління ризиками є цілісною діяльністю, яка впливає на всі аспекти діяльності Організації, включаючи планування, архітектуру підприємства, процеси життєвого циклу розробки системи (system development life cycle – SDLC).

На рисунку 6.1 наведено багаторівневий підхід до управління ризиками безпеки та приватності. Управління ризиками здійснюється на організаційному, процесуальному (функціональному) та на системному рівнях.

Взаємодія між рівнями забезпечується двонаправленими інформаційними потоками. Це дозволяє обробляти ризики безпеки на всіх рівнях.



Рисунок 6.1 – Загальний підхід щодо управління ризиками безпеки

## 6.2 Типи заходів захисту та особливості їхнього застосування

Заходи, що проводяться на організаційному, процесуальному (функціональному) та системному рівнях (рисунок 6.2) є важливими для підготовки Організації до реалізації концепції управління ризиками та впровадження СБІ. Така підготовка передбачає широкий спектр заходів.

РІВЕНЬ ПЕРШИЙ

**ОРГАНІЗАЦІЯ**

(організаційний рівень)

РІВЕНЬ ДРУГИЙ

**ФУНКЦІЇ / ПРОЦЕСИ**

(процесуальний (функціональний) рівень)

РІВЕНЬ ТРЕТІЙ

**ІНФОРМАЦІЙНА СИСТЕМА**

(системний рівень)

Концепція безпеки інформації та приватності

Програма безпеки інформації

та приватності

Політика безпеки

інформації

План

заходів

захисту

Загальні заходи захисту

Гібридні заходи захисту

Специфічні заходи захисту

Рисунок 6.2 — Розподіл заходів захисту за рівнями управління ризиками в організації

Прийняття рішення щодо управління ризиками безпеки на системному рівні тісно пов’язане з такими аспектами:

- призначення (місія, цілі), завдання, функції та процеси Організації;

- ініціативи з модернізації ІС, компонентів та послуг ІС;

- архітектура підприємства, зменшення складності ІС шляхом інтеграції, оптимізації та стандартизації;

- розподіл ресурсів для забезпечення ефективного, результативного та економічно-вигідного виконання функцій/ процесів та досягнення цілей Організації.

Цей нормативний документ визначає три типи заходів захисту інформації та персональних даних: *загальні заходи захисту*, *специфічні для інформаційної системи заходи захисту* (далі — *специфічні заходи захисту*) та *гібридні заходи захисту*. Тип заходу захисту визначає:

- сферу застосування заходу захисту;

- спільний характер або спадковість заходів захисту;

- відповідальність за розробку (налаштування), впровадження, оцінювання та надання дозволу на впровадження заходу захисту.

Кожен тип заходу захисту має конкретну спрямованість і завдання, що допомагає організаціям ефективно впроваджувати його та отримувати очікувані результати в контексті виконання вимог безпеки. Застосування певних типів заходів захисту забезпечує оптимізацію витрат (часових, матеріальних, людських) у різних інформаційних системах і робочих середовищах на впровадження (реалізацію) заходів захисту та побудову системи захисту інформації в цілому.

*Загальні заходи захисту*. Загальні заходи захисту можуть бути використані для декількох інформаційних систем одночасно. Захід захисту вважається *успадкованим*, коли інформаційна система використовує результати захисту від впровадженого заходу захисту, що контролюється, впроваджується (реалізується), оцінюється, санкціонується суб’єктами, які не несуть відповідальності за цю інформаційну систему. Загальні заходи захисту можуть впроваджуватися різними технологіями: застосування засобів захисту периметру, засобів управління доступом, засобів ідентифікації та автентифікації, а також заходів захисту, які є елементом міждоменних рішень. Витрати на розробку, впровадження (реалізацію), оцінювання, акредитацію та моніторинг загальних заходів захисту можуть бути амортизовані в різних інформаційних системах і організаційних елементах. Вибір загальних заходів захисту рекомендуються здійснювати на загальноорганізаційній основі із залученням керівництва організації, яке розуміє цілі та завдання організації, організаційні ризики безпеки, важливість інформаційних систем, що підтримують функції, процеси та активи організації. Залучення керівництва організації забезпечить оптимальність розподілу ресурсів і відповідальності щодо розроблення, впровадження, оцінювання, надання дозволу та моніторингу загальних заходів захисту.

Відповідальність за провадження загальних заходів захисту покладається на конкретних посадових осіб. Ці посадові особи розробляють, впроваджують, оцінюють, акредитують і контролюють вибрані організацією для впровадження (реалізації) загальні заходи захисту. Визначення та вибір загальних заходів захисту найефективніше проводити в співпраці з уповноваженими посадовими особами, представниками керівництва, власниками бізнесу, аналітиками безпеки, власниками (розпорядниками) інформації та з іншими зацікавленими сторонами. Загальні заходи захисту мають бути задокументовані в програмі (концепції) безпеки інформації та приватності організації. Вони також можуть бути задокументовані в політиках безпеки інформаційних систем, які успадковують ці заходи захисту, або в ситуаціях, коли загальні заходи захисту впроваджуються в межах конкретних інформаційних систем. Загальні заходи захисту можуть бути описані в одному документі або в кількох документах з посиланнями на інші документи. Якщо програма (концепція) безпеки інформації та приватності складається з декількох документів, у кожному документі мають бути визначені посадові особи, відповідальні за розробку, реалізацію, оцінювання, акредитацію та моніторинг відповідних загальних заходів захисту. Якщо загальні заходи захисту включаються в окрему політику безпеки інформаційної системи, концепція безпеки інформації та приватності організації має вказувати, які окремі політики безпеки містять опис загальних заходів захисту.

Заходи захисту, які не визначені як загальні заходи, вважаються *специфічними або гібридними*. За впровадження специфічного заходу захисту, що стосується конкретної інформаційної системи, відповідальність несуть власники (розпорядники) та посадові особи цієї інформаційної системи.

Захід захисту може бути визначений як гібридний, якщо одна частина заходу захисту є загальною, а інша частина заходу захисту є специфічною для інформаційної системи. Наприклад, організація може реалізовувати заходи планування безперервної роботи, використовуючи для всіх інформаційних систем заздалегідь погоджений з окремими власниками (розпорядниками) шаблон плану, пристосовуючи план для конкретного використання. Розподіл гібридних заходів захисту на загальні та специфічні може залежати від організації, типів використовуваних інформаційних технологій, розподілу обов’язків і методів (механізмів), що використовуються організацією для реалізації заходів захисту.

Визначення того, чи є захід захисту загальним, гібридним або специфічним, залежить від контексту його впровадження (реалізації). Захід захисту не можна визначити загальним, гібридним або специфічним, лише ґрунтуючись на його формулюванні. Наприклад, захід захисту може бути специфічним для однієї інформаційної системи, і водночас може бути загальним заходом для іншої інформаційної системи (тобто успадкованим від першої системи). Одним з методів визначення того, чи може специфічний захід бути загальним заходом для інших інформаційних систем, є розгляд того, хто чи що залежить від функціональності цього заходу захисту. Якщо певна частина інформаційної системи, що є зовнішньою для цієї системи, залежить від заходу захисту, то цей захід може бути загальним.

Розмежування заходів захисту на загальні, гібридні та специфічні може допомогти оптимізувати витрати на впровадження та оцінювання заходів захисту, а також забезпечити гнучкість і послідовність застосування засобів захисту в рамках всієї організації. Хоча розподіл заходів захисту на загальні, гібридні й специфічні є простим та інтуїтивно зрозумілим, фактично застосування зазначених заходів вимагає планування та координації діяльності із захисту інформації.

## 6.3 Документування заходів захисту

Даний розділ надає рекомендації щодо порядку документування основних вимог безпеки та приватності, а також впроваджених ЗЗІ та ПД на Організаційному та системному рівні.

До основних документів, які мають бути сформовані та затверджені в Організації на ІС належать наступні:

* концепція безпеки інформації та приватності;
* опис ІС;
* категорія критичності;
* програма безпеки інформації та приватності;
* політики безпеки інформації;
* плани заходів захисту інформації та персональних даних.

Даний перелік не є вичерпним і може доповнюватися на розсуд Власника (Розпорядника) Організації та/або ІС виходячи із особливостей Організації/ІС та/або нормативних вимог, сформованих центральними або галузевими органами влади.

У таблиці 6.1 наведені рекомендовані розділи відповідних документів. Кожен із цих документів може бути представлений як окремий документ або сукупність документів.

Таблиця 6.1 – Рекомендовані документи та їхній стислий зміст

|  |  |
| --- | --- |
| Назва документу | Рекомендовані розділи |
| 1 | 2 |
| Концепція БІ  (Організаційний рівень) | 1. Висновки щодо явного прийняття ризиків на рівні вищого керівництва. 2. Наміри керівництва. 3. Припущення , що будуть успадковуватися програмою БІ та приватності. 4. Виділення ІС в складі Організації. 5. Виділення структурних компонентів Організації. |
| Опис ІС  (Системний рівень) | Опис ІС:   * опис організаційної належності ІС, * опис процедур, функцій, активів, прикладних процесів ІС, * опис дійових осіб ІС, * варіанти використання ІС, * результати інвентаризації IT-активів, * результати інвентаризації типів інформації ІС |
| Категорія критичності ІС  (Системний рівень) | 1. Визначення РК типів інформації в ІС 2. Визначення КК ІС |
| Програма БІ та приватності  (Системний рівень) | 1. Формулювання вимоги безпеки ІС 2. Формулювання вимоги приватності ІС 3. Обґрунтування вибору БПБ або ГПБ 4. Обґрунтування вибору рівня БПБ (ГПБ) 5. Місце впровадження ІС в структурі Організації |
| Політики БІ  (Системний рівень) | 1. Ціль/цілі політики БІ 2. Сфера застосування Політики БІ 3. Ролі в ІС та сфера їхньої відповідальності 4. Перегляд Політики БІ |
| Плани ЗЗ  (Системний рівень) | 1. Застосовані в ІС технічні та програмні, організаційні засоби для реалізації ЗЗ 2. Обґрунтування параметрів |

## 6.4 Етапи розгортання системи безпеки інформації

Розгортання та подальше функціонування СБІ здійснюється як безперервна цілеспрямована діяльність Організації, яка складається з етапів та завдань (рисунок 6.3).

Організації під час впровадження СБІ слід дотримуватися послідовного підходу, який застосовується до всіх етапів управління ризиками в масштабах всієї організації: від організаційного до системного рівня. Відповідальні особи Організації визначають та захищають необхідні ресурси для виконання завдань щодо управління ризиками та забезпечують доступність цих ресурсів для відповідного персоналу.

Діяльність з впровадження СБІ складається з семі етапів:

* аналіз ризиків на організаційному та системному рівнях;
* категоріювання безпеки;
* вибір заходів захисту;
* впровадження заходів захисту;
* оцінювання безпеки;
* авторизація безпеки ІС;
* постійний моніторинг безпеки.

Усі виконані дії щодо виконання вище зазначених етапів повинні документуватися відповідальними особами в частині, яка регулюється їхніми повноваженнями. За своїми ролями та впливом при виконанні на процесів аналізу ризиків на організаційному рівні, категоріювання безпеки, вибір, впровадження та оцінювання безпеки, а також авторизації безпеки ІС та процесів постійного моніторингу безпеки, усі особи можливо розподілити на наступні:

1. Власник ІС (Розпорядник).
2. Розробник (Проектувальник) системи захисту інформації. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як проектувальник системи безпеки, проектувальник системи приватності. За необхідності для виконання цієї ролі можуть залучатися сторонні фахівці на договірній основі.
3. Постачальник послуг безпеки та засобів захисту. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як інженер з безпеки системи, інженер з приватності системи. За необхідності для виконання цієї ролі можуть залучатися сторонні фахівці на договірній основі.
4. Адміністратор безпеки. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як службова особа з безпеки, службова особа з приватності, системний адміністратор.
5. Оцінювач безпеки/група оцінювачів. Для виконання цієї ролі повинні залучатися сторонні фахівці на договірній основі.
6. Уповноважений орган з авторизації.

В свою чергу, кожній з етапів складається із завдань. Кожне завдання розглядається як функціональний блок, який містить мету, вхідні дані, вихідні дані та перелік ролей, що відповідають за виконання завдання.

Впровадження вимог цього та інших НД з питань управління безпекою інформації є безперервним процесом розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи безпеки інформації (СБІ).

Цей нормативний документ щодо впровадження системи безпеки інформації деталізує вимоги міжнародного стандарту ISO/IEC 27003:2010 "Information technology - Security techniques - Information security management system implementation guidance" (Настанова з впровадження системи управління інформаційною безпекою) з урахуванням особливостей діяльності організацій, установ, відомств та підприємств з питань безпеки інформації. Модель, що впроваджується цим НД, конкретизує модель ПВПД (плануй - виконуй - перевіряй - дій), яка визначена в ISO/IEC 27001:2015 (рисунок 6.4).

Відповідність СБІ, закріпленої в цьому нормативному документі, вимогам міжнародних стандартів ISO/IEC 27001 та ISO/IEC 27002 надасть можливість власниками ІС, які розгорнули СБІ керуючись положеннями цього НД за потреби також отримати відповідний міжнародний сертифікат.



Рисунок 6.3 – Етапи впровадження системи безпеки інформації в Організації



Рисунок 6.4 – Відповідність етапів розгортання СБІ моделі ПВПД, яка визначена у ISO/IEC 27001

Кожний із етапів має перелік вхідних та вихідних даних (рисунок 6.5). Вихідні дані кожного із етапів можуть бути вхідними для подальших.



Рисунок 6.5. – Взаємозв’язок етапів впровадження СБІ

# 7. Впровадження заходів захисту як життєвий цикл розробки IT-систем

З метою підвищення ефективності системи безпеки інформації, вона має бути інтегрована до життєвого циклу розробки IT-систем (SDLC) з самого початку створення систем.

Є багато методологій SDLC, які можуть використовуватися організацією, щоб ефективно розробити інформаційну систему. Традиційний SDLC - лінійна послідовна модель (також відома як метод водоспаду), передбачає, що система буде поставлена в її заключних етапах життєвого циклу розробки. Інший метод SDLC використовує модель прототипування, яка часто застосовується, щоб зробити можливим розуміння системних вимог, не розробляючи насправді закінчену інформаційну систему. Складніші системи можуть зажадати моделей більш ітераційної розробки. Так, складні моделі розроблялися та успішно використовувалися, щоб врахувати розвинуту складність передових та іноді великих проєктів інформаційних систем. Прикладами таких складних моделей є:

* модель швидкої розробки додатків (RAD),
* модель спільної розробки додатків (JAD),
* модель прототипування,
* спіральна модель.

Очікуваний розмір і складність системи, графік розробки та тривалість життя системи будуть впливати на вибір того, яку модель SDLC використовують. В багатьох випадках вибір моделі SDLC буде визначений Концепцією безпеки інформації Організації.

Типовий SDLC включає п'ять фаз: ініціювання, розробка/придбання, реалізація/оцінка, експлуатація/підтримка та ліквідація (рисунок 7.1). Кожна фаза включає мінімальний набір завдань з безпеки інформації, необхідних для ефективного включення безпеки в процес розробки системи. Фази можуть постійно повторюватися протягом життя системи до виведення її з експлуатації.



Рисунок 7.1 – Концептуальне подання SDLC

Ініціювання. Під час фази ініціювання виражається потреба в системі та документується призначення системи. Під час цієї першої фази життєвого циклу розробки розгляд безпеки є ключовими для ретельної та ранньої інтеграції, гарантуючи, таким чином, що будуть розглянуті загрози, вимоги та потенційні обмеження у функціональності та інтеграції. У цей момент на безпеку дивляться більше з точки зору ризиків для діяльності з позиції служби інформаційної безпеки.

Розробка/придбання. Під час цієї фази система проєктується, закуповується, програмується, розробляється або інакше створюється. Ключові роботи з безпеки для цієї фази охоплюють:

* проведення оцінки ризику та використання результатів для доповнення базового набору заходів забезпечення безпеки;
* аналіз вимог безпеки;
* проведення функціонального тестування та тестування безпеки;
* підготовку вихідних документів до сертифікації та атестації системи;
* проєктування архітектури безпеки.

Реалізація/оцінка. Під час цієї фази система повинна бути встановлена та оцінена в експлуатаційному середовищі Організації. Ключові роботи з безпеки для цієї фази включають:

* інтеграцію інформаційної системи в її середовище;
* планування та проведення робіт по оціночним випробуванням системи в синхронізації з тестуванням заходів безпеки;
* роботи по комплексній оцінці системи.

Експлуатація/підтримка. Під час цієї фази система виконує свою роботу. Система майже завжди змінюється з додаванням апаратного та програмного забезпечення та різними іншими подіями. У цій фазі системи розгорнуті та експлуатуються поліпшення та/або модифікації для систем розроблені й протестовані, й апаратні засоби та/або програмне забезпечення додані або замінені. Система контролюється для тривалої роботи відповідно до вимог безпеки та впроваджують необхідні модифікації системи. Експлуатована система періодично оцінюється, щоб визначити, як система може бути зроблена більш ефективною, безпечною та результативною. Експлуатація триває до тих пір, поки система може бути ефективно змінена, щоб відповісти на потреби Організації, та підтримується на встановленому рівні ризику. Коли визначена необхідність модифікації або змін, система може повторно перейти в попередню фазу SDLC. Ключові роботи з безпеки для цієї фази включають:

* проведення аналізу експлуатаційної готовності;
* управління конфігурацією системи;
* встановлення процесів і процедур для надійної експлуатації та безперервного моніторингу заходів безпеки інформаційної системи;
* виконання повторного санкціонування за необхідності.

Виведення з експлуатації. Роботи, проведені під час цієї фази, гарантують організоване припинення функціонування системи, збереження суттєвої інформації системи, а переносяться дані, передаються системою до нової системи, або зберігаються відповідно до застосовних нормативних документів та політик управління записами. Проблеми безпеки інформації, пов'язані з ліквідацією інформації й системи, повинні бути повністю вирішені. Коли інформаційні системи передаються, стають застарілими або більше не застосовні, важливо гарантувати, що ресурси та активи захищені. Зазвичай, це не остаточний кінець системи. Системи зазвичай розвиваються або переходять до наступного покоління через зміни вимог або поліпшення технологій. Плани забезпечення безпеки системи повинні безперервно розвиватися з системою. Крім того, велика частина інформації щодо оточення, управління та експлуатації повинна бути відповідною і корисною в розробці плану забезпечення безпеки для системи.

Роботи по виведенню з експлуатації гарантують акуратне завершення використання системи та зберігають важливу інформацію про систему так, щоб деяка або вся інформація могла б бути, в разі необхідності, відновлена в майбутньому. Особливий акцент робиться на належному збереженні даних, які обробляються системою з тим, щоб дані були ефективно переміщені в іншу систему або заархівовані відповідно до застосовних нормативних актів та політик з управління записами для потенційного майбутнього доступу.

Роботи по розгортанню системи безпеки повинні бути фізично і логічно інтегровані в політику і керівництва Організації по SDLC.

# 8. Визначення етапів розгортання системи безпеки інформації

## 8.1 Етап аналізу ризиків на організаційному рівні

Даний етап передбачає підготовку на Організаційному рівні до реалізації процесів управління ризиками безпеки включає:

* визначення ролей в Організації в сфері управління ризиками безпеки;
* розробка Концепції ІБ та приватності;
* визначення цілей, завдань, функцій та процесів, які має підтримувати інформаційна системи (фокус ІС);
* визначення ключових стейкхолдерів (внутрішніх і зовнішніх для організації), які зацікавлені у функціонуванні ІС;
* розуміння загроз та потенційного негативного впливу загроз на фізичних осіб та інформаційні системи;
* проведення оцінювання ризиків на рівні Організації;
* визначення (вибір) та розстановка пріоритетів вимог безпеки та приватності;
* визначення та узгодження вимог безпеки та приватності;
* побудова ІС (сукупності ІС).

## 8.2 Етап категоріювання безпеки

З метою оцінки рівня критичності активів Організації та ІС проводиться категоріювання всіх активів ІС на основі її опису. Категоріювання проводиться з точку зору оцінки рівня негативного впливу (шкоди), який може настати у разі, якщо будуть порушені конфіденційність, цілісність та доступність активів ІС. Для цього визначаються критерії оцінки впливу за кожною властивістю безпеки та встановлюється рівень критичності – низький, середній та високий. Порядок оцінки критичності та проведення категоріювання встановлюється окремим нормативним документом «Порядок категоріювання безпеки інформаційної системи та інформації».

## 8.3 Етап вибору заходів захисту

Організація, за результатами оцінки ризиків безпеки та категоріювання безпеки, обирає набір заходів захисту – базовий (галузевий) профіль безпеки. Заходи захисту обираються на основі системи заходів захисту, що встановлюється окремим нормативним документом, спираючись на стандартні профілі безпеки та профілі кібербезпеки. Під час визначення заходів захисту також враховуються профілі безпеки засобів захисту, вимоги міжнародних та галузевих стандартів. Порядок вибору базового (галузевого) профілю безпеки встановлюється окремим нормативним документом «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

## 8.4 Етап впровадження (реалізації) заходів захисту

Впровадження (реалізація) заходів захисту здійснюється у відповідності до розробленої Концепції безпеки інформації та приватності із застосуванням методології проектування систем захисту інформації. Особливості впровадження заходів захисту визначаються окремим нормативним документом «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

## 8.5 Етап оцінювання безпеки

Перевірка відповідності заходів захисту встановленим вимогам безпеки та приватності здійснюється під час оцінювання безпеки. Під оцінюванням розуміється широкий спектр підходів до встановлення коректності реалізації заходів захисту інформації та ПД в ІС відповідно до обраного профілю захисту. Порядок та методика визначаються окремим нормативним документом «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

## 8.6 Етап авторизації безпеки інформаційної системи

Рішення щодо можливості використання СБІ інформаційної системи набирає чинності в результаті внесення запису до реєстру авторизованих систем. Рішення приймається уповноваженим органом з авторизації. Для проведення авторизації формується пакет відповідних документів (пакет авторизації), що подається до уповноваженого органу з авторизації. Порядок проведення державної авторизації встановлюється нормативним документом «Порядок авторизації безпеки інформаційних систем».

## 8.7 Етап постійного моніторингу безпеки

Моніторинг безпеки є важливим етапом відстеження змін стану безпеки ІС та Організації та реагування на нові виклики (загрози) безпеки. З цією метою в Організації розробляється стратегія постійного моніторингу. Відповідний Порядок проведення встановлюється окремим нормативним документом «Порядок моніторингу безпеки інформаційних систем».