УДК 621.396.946 https://doi.org/10.33099/2304-2745/2025-3-86/33-37

Гордієнко С. Б. – кандидат технічних наук, доцент[1] (0000-0001-2345-6789)
Ворович Б. О., кандидат військових наук, доцент[2] (0000-0002-4083-3707)
Прийма Я. О.[2] (0000-0001-7783-2698)

[1] - Кафедра технологій захисту кіберпростору Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України Київ;
[1] - Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Питання системного підходу щодо забезпечення безпеки інформації об’єктів інформаційної інфраструктури

Резюме. В статті розглянуті аспекти системного підходу щодо створення та впровадження системи безпеки інформації стосовно об’єктів інформаційної інфраструктури.

Ключові слова: системний підхід; управління безпекою інформації; об’єкт інформаційної інфраструктури; реалізація рішення.

Постановка проблеми. За умов складних загальносуспільних відносин, воєнного стану та постійних деструктивних посилів з боку держави агресора – Російської Федерації (РФ) застосування системного підходу до наукових та організаційних спрямувань щодо забезпечення та підтримання ефективних заходів безпекового характеру інформаційної та технологічної складової функціонування об’єктів інфраструктури є найбільш актуальним з точки зору їх розробки та подальшого використання.

Оскільки управлінська діяльність тісно пов’язана із системним підходом, то саме необхідність виконання управлінських завдань змушує широко застосовувати системні ідеї, переводячи їх на рівень технологічних схем керування. Тому потреби управління виступають найважливішою рушійною силою застосування системного підходу. При цьому, розширення сфери використання в управлінських процесах інформаційних систем та їх ускладнення спричиняє загострення проблеми безпеки інформації (загалом інформаційних ресурсів) у таких системах та викликає потребу її забезпечення шляхом побудови (впровадження) підсистем безпеки інформації та управління ними на принципі системного підходу.

Аналіз останніх досліджень і публікацій. З часів інтенсивного розвитку інформаційних відносин в Україні та до сьогодні, за умов воєнного стану, питання безпеки інформації досліджувалися та розвивалися, зокрема, провідними вітчизняними науковцями переважно під кутом забезпечення інформаційної безпеки. На особливу увагу в цій сфері заслуговують праці [1-5]. Характер їх досліджень в галузі інформаційної безпеки спрямований на досягнення ефективних методів та підходів щодо забезпечення вимог політики безпеки, системи управління інформаційною безпекою (СУІБ) на об’єктах інформаційної інфраструктури. Також значна увага спрямовувалася на розробку питань застосування сучасних безпекових технологій та окремих методик комплексної системи безпеки та управління нею за умов активної інформаційної агресії з боку РФ з деструктивним впливом на стійкість функціонування процесів життєзабезпечення нашої країни. Проте, у наведених джерелах недостатньо уваги приділено питанням застосування системного підходу щодо розробки технологій забезпечення безпеки інформації, створення перспективних засобів управління безпекою інформації.

Між тим, аналіз показує, що міжнародними стандартами серії ISO/IEC2700, які імплементовані в Україні як державні стандарти [6-8], де ключовим є словосполучення “*information security*”, що може перекладатися як “*інформаційна безпека*” або “*безпека інформації*” (що не є еквівалентними [9,10]), у повному обсязі на основі системного підходу забезпечується викладення методологічних засад створення та застосування технологій якраз *безпеки інформації*, що передбачає сукупність процедур її всебічного захисту. Але питання порядку (шляхів) практичного впровадження таких технологій на об’єктах інформаційної діяльності значною мірою ще залишається сьогодні поза увагою наукового обґрунтування.

Метою статті є обґрунтування застосування системного підходу щодо створення та забезпечення ефективного

процесу функціонування системи безпеки інформації на об'єктах інформаційної інфраструктури на основі положень ДСТУ серії ISO/IEC 2700.

Виклад основного матеріалу. Забезпечення безпеки інформації на об'єктах інформаційної інфраструктури полягає в організації та реалізації відповідного процесу управління, що включає планування, виконання (побудову), контроль і технічне обслуговування всієї інфраструктури безпеки та дотримання вимог політики безпеки. Тобто, це необхідна сфера впливу на шляху побудови захищеного простору обігу інформації. Це передбачає обов'язковий етап діагностичного обстеження інформаційної інфраструктури (системи) з оцінкою її вразливостей і загроз, на основі чого проводиться проєктування підсистеми безпеки інформації, впровадження, супровід та обслуговування, а в подальшому управління нею. Системне вирішення комплексу цих питань передбачено, зокрема, національним стандартом ДСТУ ISO/IEC 27001:2023 [6], яким регламентується створення та використання *системи управління безпекою інформації* як частини загальної системи управління підприємством (організацією), що ґрунтується на врахуванні бізнес-ризиків та інших ризиків антикризового менеджменту і призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення *політик безпеки інформації*. Іншими словами, система управління безпекою інформації складається з політик, процедур, інструкцій, практик та технологій, які дозволяють захищати конфіденційну інформацію від загроз та ризиківОтже, реалізація загроз і ризиків для інформації може суттєво вплинути на такі її властивості як конфіденційність цілісність та доступність.

Конфіденційна інформація - це інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Цілісність інформації - це внутрішня єдність, пов'язаність усіх частин інформаційного продукту в єдине ціле. В інформаційній системі – стан даних та програм, що забезпечує: стійку роботу системи. Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи, захист від несанкціонованої модифікації даних і таке інше. Інформація повинна залишатися недоторканою та не піддається змінам без дозволу.

Доступність інформації - це властивість інформації бути захищеною від несанкціонованого блокування, що гарантує можливість її використання уповноваженими користувачами, коли це необхідно.

Послаблення або нівелювання реалізації загроз і викликів може бути досягнено шляхом застосування певних заходів.

Аутентифікація та авторизація - перевірка ідентичності користувачів та надання їм відповідних прав доступу до інформації. Аутентифікация – підтвердження ідентичності користувача. Авторизация – підтвердження системою безпеки, що користувачу надано дозвіл до визначених дій.

Управління ризиками - це оцінка потенційних загроз для інформації та впровадження заходів для їх запобігання або зменшення впливу.

Шифрування - захист інформації шляхом перетворення її в нечитабельний формат, який може бути розкодований тільки з використанням відповідного ключа.

Аудит та моніторинг - систематичний контроль за подіями та діяльністю для виявлення несправностей системи або потенційних загроз інформації.

Усвідомлення та навчання - забезпечення освіченості персоналу та навчання його правилам дотримання безпеки інформації.

Приймаючи до уваги вище зазначене, організація підсистеми (системи) управління безпекою інформації відповідно до стандарту [6] потребує також дотримання ряду вимог та потреб, зокрема:

врахування *контексту організації (Context of the organization)* – розуміння організаційного контексту, потреб і очікувань "зацікавлених сторін" та визначення сфери застосування системи управління безпекою інформації;

лідерства (Leadership) - вище керівництво має продемонструвати лідерство та відданість СУІБ, визначити політику та призначити ролі, обов'язки та повноваження щодо безпеки інформації;

планування (Planning) - описує процес виявлення, аналізу та планування усунення інформаційних ризиків, уточнення цілей

інформаційної безпеки та управління змінами системи управління безпекою інформації;

підтримки (Support) - мають бути виділені відповідні, компетентні ресурси, підвищена обізнаність, підготовлена та контрольована документація;

операційності (Operation) – більш детальніше оцінювання та усунення інформаційних ризиків, керування змінами та документування речей (частково для того, щоб їх могли перевірити аудитори сертифікації);

оцінки ефективності (Performance evaluation) – моніторинг, вимірювання, аналіз та оцінка/аудит/перегляд засобів контролю, процесів і системи управління безпекою інформації, систематично вдосконалюючи речі, де це необхідно;

удосконалення (Improvement) – звернутись до висновків аудитів та оглядів (наприклад, невідповідності та коригувальні дії), систематично удосконалюючи систему управління безпекою інформації.

Зазначене засвідчує системність підходу у цьому стандарті до управління і забезпечення безпеки інформації в процесі практичної діяльності будь-якого суб'єкта.

Постановку задачі та прийняття рішення щодо застосування системи управління безпекою інформації організації (установи) на основі системного підходу у кожному конкретному випадку необхідно розглядати відповідно до *принципів системного аналізу* [11], таких як:

процес прийняття рішень починається з аналізу та визначення важливих проблем і чіткого формулювання конкретної мети системи;

при розгляді проблеми в цілому слід виявити всі наслідки і взаємозв'язки кожного окремого рішення;

визначити і дослідити всі можливі альтернативи шляхів рішення проблеми і досягнення мети;

цілі окремих підсистем повинні бути узгоджені з метою всієї системи;

в процесі аналізу доцільно перейти від абстрактного до конкретного;

необхідно виявити зв'язки між елементами системи, дослідити їх взаємодію.

Застосування елементів системного аналізу не замінює сутності політики безпеки інформації об'єктів інформаційної діяльності, а істотним чином доповнює розгляд її особливостей. Зокрема, деталізується вплив ризиків щодо системи безпеки, які змінюються, сприяючи появі нових вразливостей та нових загроз безпеці [11, 12], що становить основу реалізації політики безпеки об'єктів та потребує розширення аналізу, як-то:

явищ безпекового характеру, технологічних процесів та господарсько-фінансової діяльності організації (установи) в цілому;

окремих сторін управлінської діяльності та стратегічного планування розвитку організації (установи);

також діяльності окремих специфічних підрозділів матеріального, фінансового, безпекового та іншого забезпечення.

При цьому, також враховуються показники, які обґрунтовані даними обліку, звітності і плану. Але для повного і глибокого вивчення проблеми необхідно не тільки використовувати дані, отримані в результаті вивчення технічних, економічних, фінансових, безпекових та інших сторін діяльності організації (установи), а також психологічний клімат і соціальні явища, які виявлені при здійсненні загального ризик-менеджменту.

Таким чином, системний аналіз дає можливість дослідити питання безпеки інформації організації (установи) більш глибоко і всебічно, ніж при спрощеному аналізі ризиків безпекового характеру, оскільки він передбачає використання як жорстких кількісних методів, так і логічних суджень, досвіду та інтуїції.

Переходячи безпосередньо до побудови системи безпеки з позиції системного аналізу, також необхідно передбачити виконання наступних завдань.

1. Визначення меж оптимізації системи – управління безпекою інформації може бути здійснено лише в межах безпосереднього впливу та дії зовнішніх та внутрішніх факторів системи, що підлягає оптимізації. Межі системи відносно критеріїв безпеки інформації визначаються охопленням методами і засобами забезпечення політики безпеки конкретного об'єкту інформаційної діяльності;

2. Визначення головного показника (критерію) ефективності, за яким можна оцінити характеристики рішення, що відшукується – доцільно застосовувати найбільш прийнятний і зрозумілий для керівництва показник, яким може бути безпековий, фінансовий, репутаційний або матеріальний критерій, також рівень прогнозованих затрат щодо створення ефективної системи управління безпекою інформації.

3. Вибір внутрішньосистемних незалежних змінних, які мають адекватно описувати функціонування системи управління безпекою інформації – мають адекватно описувати та характеризувати ефективність функціонування системи за напрямком управління безпекою інформації, мають бути дієвими складовими зв'язків (відносин) між елементами системи. Визначення цих незалежних змінних конкретно може бути характерним проявом та ознакою тільки індивідуального підходу до функціонування системи або її окремого елементу.

4. Побудова моделі, що має описувати взаємозв'язки між змінними та відображати вплив незалежних змінних на рівень показника ефективност – на етапі побудови і дослідження конкретних моделей безпеки інформації, які характерні для застосування на конкретних об'єктах (в організаціях), реалізуються такі три базові функції:

оцінювання цілей і засобів їх досягнення;

вибір оптимального варіанту рішення;

впровадження рішення і оцінювання його ризиків та наслідків.

При цьому доцільно відзначити і питання про відповідність (адекватність) моделей реальності. У реальних системах цілком можливе логічне обґрунтування моделей елементів (складових) системи управління безпекою інформації. Ці моделі саме і необхідно будувати мінімально-достатніми, тобто простими настільки, наскільки це можливо без втрати сутності та ефективності процесів управління в такій системі.

Зважаючи на вищевикладене, процес прийняття рішення на основі системного підходу щодо створення та забезпечення ефективного функціонування системи безпеки інформації інформаційної інфраструктури організації (установи) як невід'ємної складової її загальної системи управління, можна подати послідовність виконання відповідного набору фаз (етапів) дій як представлено в Табл. 1.

Таблиця 1

Зміст основних етапів прийняття та реалізації рішень щодо забезпечення безпеки інформації організації (установи) на основі системного підходу

№	Фаза прийняття рішення	Зміст фази прийняття рішення
1	Збір інформації про можливі проблеми забезпечення безпеки інформації.	Спостереження за внутрішнім та зовнішнім середовищем діяльності організації (установи).
2	З'ясування та визначення причин виникнення проблем щодо порушення політики безпеки.	Опис проблемної ситуації Формулювання проблеми, оцінювання її важливості та з'ясування причин виникнення проблеми.
3	Формулювання цілей вирішення проблеми щодо забезпечення безпеки інформації.	Визначення контексту інформаційної складової діяльності організації. Формулювання критеріїв вирішення проблеми, щодо політики безпеки.
4	Діагностичне обстеження з оцінкою вразливостей (ризиків) інформаційної системи і загроз.	Детальний опис об'єкту захисту. Визначення розмаху варіації факторів пливу (ризиків). Визначення обмежень.
5	Розробка відповідних кроків забезпечення політики безпеки інформації в організації (установі)	Формулювання актуальних задач, пошук ідей розв'язання кожної задачі. Визначення та знаходження можливих варіантів (моделей) рішення безпекової проблеми. Узагальнення результатів розв'язання по окремих рішеннях. Прогнозування наслідків прийняття раціональних рішень по забезпеченню системи безпеки.
6	Вибір кращого варіанту вирішення проблеми	Прогнозування наслідків прийняття раціональних рішень по забезпеченню системи безпеки.
7	Коригування та узгодження рішення	Аналіз рішення з виконавцями (операторами безпеки інформації). Узгодження рішення з функціонально взаємодіючими службами. Затвердження рішення.
8	Реалізація рішення	Підготовка робочого плану реалізації. Реалізація. Внесення змін у робочий план у ході реалізації рішення. Оцінювання ефективності реалізації прийнятого рішення.

Висновки. Показано можливість отримання рішення щодо побудови системи безпеки інформації інформаційної інфраструктури організації (установи) на основі системного підходу, закладеного в положеннях державного стандарту ДСТУ ISO/IEC 27001: 2023, а також з використанням елементів системного аналізу. Запропоновано загальну схему (послідовність) дій в інтересах ухвалення рішення керівництвом щодо

побудови системи безпеки інформації інформаційної інфраструктури як невід'ємної складової загальної системи управління організації (установи).

Подальші дослідження доцільно зосередити на розвитку системи управління безпекою інформації, що буде пов'язано з інтеграцією в цілісну форму системного підходу до управління організацією в цілому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. В.О. Богуш. Технічний захист інформації./ В.О. Богуш, В. Бровко, О. Кобус.– К.: Ліра-К, 2022 – 508 с.

2. Домарєв В.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k). Донецьк: Велстар, 2012, 146с.

3. С.В. Толюпа, В.Л. Бурячок, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник К.:ДУТ, 2015. – 345 с.

4. Інформаційна безпека держави: підручник: в 2 т / В.М. Петрик та ін., за заг. ред.. В.В. Остроухова. – .К.: Кн. палата України, 2016. Т. 1 – 387 с. Т. 2 – 328 с.

5. Інформаційна безпека. Підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей та ін.; під ред. В.В. Остроухова. – К.: Ліра-К, 2021. – 412 с.

6. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

7. ДСТУ ISO/IEC 27005:2023. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

8. ДСТУ ISO/IEC 27006:2023. Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2011, IDT).

9. О. Архипов, Є. Архипова. Особливості розуміння понять "інформаційна безпека" та "безпека інформації". / Матеріали XI міжнародної науково-практичної конференції. – К.: ІПРІ НАН України, 2014. – С. 18-30.

10. Інформаційна безпека України у воєнній сфері: засадничі елементи становлення теоретичних основ її забезпечення: монографія / Кол. авторів, за заг. ред. П.М. Сніцаренка. – К.: НУОУ, 2025. – 300 с.

11. Теорія систем і системний аналіз : конспект лекцій /укладач С.В. Соколов. – Суми : Сумський державний університет, 2020. 171 с.

12. Гордієнко С.Б. Актуальні питання управління ІТ ризиками на об'єктах критичної інформаційної інфраструктури // Вісник Державного університету телекомунікацій "Телекомунікаційні та інформаційні технології" №1 (74) - 2022. С.29-35.

Стаття надійшла до редакції 06.10.2025

Issues of the Systems Approach to Ensuring Information Security of Information Infrastructure Objects

Annotation

The expansion of the use of information systems in management processes and their increasing complexity lead to the exacerbation of the problem of information security and information resources in general. This necessitates ensuring information security through the construction (implementation) of information security subsystems and their management.

The purpose of the article is to substantiate the application of a systems approach to the creation and ensuring of an effective functioning process of the information security system at information infrastructure objects, based on the provisions of the DSTU ISO/IEC 27000 series standards.

Systems analysis allows for a deeper and more comprehensive examination of the organization's (institution's) information security issues compared to a simplified analysis of security risks, as it involves the use of both rigorous quantitative methods and logical judgments, experience, and intuition.

The decision-making process based on the systems approach to the creation and ensuring of effective functioning of the information security system within the organization's (institution's) information infrastructure, as an integral component of its overall management system, is presented as a sequence of corresponding stages.

The possibility of obtaining a solution for building an information security system for the organization's (institution's) information infrastructure based on the systems approach embedded in the provisions of the national standard DSTU ISO/IEC 27001:2023 is demonstrated.

Keywords: systems approach; information security management; information infrastructure object; decision implementation.