МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

БАЛТОВСЬКИЙ О. О.,
ФОРОС Г. В., ПЯДИШЕВ В. Г.

БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ

Навчальний посібник

Одеса
2025

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

БАЛТОВСЬКИЙ О. О., ФОРОС Г. В., ПЯДИШЕВ В. Г.

«БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ»

Навчальний посібник

Одеса 2025

УДК 681.518:004.056(075.8)

Схвалено та рекомендовано до друку науково-методичною радою Одеського державного університету внутрішніх справ (протокол № 6 від 19.06.2025 р.)

Авторський колектив:
Балтовський О.О. – доктор технічних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій ОДУВС;
Форос Г.В. – кандидат юридичних наук, доцент, доцент кафедри кримінального аналізу та інформаційних технологій ОДУВС;
Пядишев В.Г. – доктор юридичних наук, професор, професор кафедри кримінального аналізу та інформаційних технологій ОДУВС
Рецензенти:
Афонін Д.С. – завідувач науково-дослідної лабораторії з актуальних питань кримінального аналізу ННІАФПКП НПУ ОДУВС, кандидат юридичних наук, доцент;
Логінова Н.І. – завідувачка кафедри інформаційних технологій Національного університету «Юридична академія», кандидат педагогічних наук, доцент.

Б39 **Балтовський О.О., Форос Г.В, Пядишев В. Г.**
Безпека технічних систем: навчальний посібник / За заг. ред. д.т.н., доц. О.А. Балтовського. — Одеса: ОДУВС, 2025. — 138 с.

Навчальний посібник «Безпека технічних систем» висвітлює теоретичні основи, практичні підходи і сучасні технологічні рішення у сфері забезпечення безпеки технічних систем різного призначення. Посібник охоплює широкий спектр питань від класифікації технічних систем і типології загроз до аналізу вразливостей, управління ризиками, нормативно-правового регулювання та застосування інновацій у сфері безпеки.

Матеріал структуровано за принципами логічної послідовності та міждисциплінарності. Особливу увагу приділено системному підходу до захисту технічних систем, принципам оборони, а також адаптації рішень до сучасних викликів, зумовлених застосуванням штучного інтелекту, Інтернету речей, блокчейн-технологій та кіберфізичних систем.

Посібник спрямовано на формування у здобувачів вищої освіти фахових компетентностей, зокрема здатності до проектування, аналізу та впровадження технічних систем із вбудованими засобами безпеки, а також розвитку навичок міждисциплінарного мислення.

Видання призначене для здобувачів вищої освіти технічних, інженерних, інформаційних та кібернетичних спеціальностей, а також може бути корисним для практикуючих інженерів, аналітиків безпеки, фахівців із захисту інформації та розробників технічних рішень.

УДК 681.518:004.056(075.8)
© О. А. Балтовський, Г. В. Форос, В. Г. Пядишев

ВСТУП

У сучасному світі, де стрімкий розвиток технологій змінює спосіб життя, комунікацій і виробництва, безпека технічних систем набуває стратегічного значення. Інформаційні технології, кіберфізичні системи, Інтернет речей (IoT), штучний інтелект і автоматизовані виробничі лінії сьогодні складають основу інфраструктури держав, корпорацій і окремих громадян. Водночас зростає кількість загроз, пов'язаних із уразливістю цих систем до зовнішніх і внутрішніх атак, помилок проєктування, недосконалості програмного забезпечення, соціальної інженерії та недотримання вимог безпеки.

Технічні системи, незалежно від галузі застосування — енергетика, транспорт, оборонна промисловість, охорона здоров'я чи комунікації — вимагають всебічного аналізу ризиків та ефективного захисту. Уразливість одного компонента може призвести до масштабних наслідків, включно з людськими жертвами, економічними збитками, втратами інформації або порушенням національної безпеки. У цьому контексті необхідність формування системного підходу до забезпечення безпеки технічних систем є не лише актуальною, а й критичною умовою їх стійкості, надійності та функціональної цілісності.

Крім того, інтеграція передових технологій — таких як блокчейн, машинне навчання, квантова криптографія та біометричні системи контролю доступу — створює як нові можливості, так і нові ризики. Забезпечення безпеки технічних систем вимагає поєднання знань з інженерії, інформатики, кібербезпеки, права та управління ризиками.

Метою цього навчального посібника є формування у здобувачів вищої освіти комплексного уявлення про теоретичні засади, методології та практичні підходи до забезпечення безпеки технічних систем. Посібник розкриває як фундаментальні основи, так і сучасні інструменти та технології, що застосовуються для запобігання, виявлення, локалізації та мінімізації загроз технічного характеру.

Для досягнення цієї мети окреслено такі ключові завдання:

1. Формування уявлення про технічну систему як об'єкт аналізу безпеки.

Посібник має на меті надати поглиблене розуміння сутності технічних систем — їхньої структури, функціональних характеристик, взаємозв'язків між складовими компонентами (апаратними, програм-

ними, кібернетичними, енергетичними тощо). Передбачено опрацювання класифікацій технічних систем відповідно до функціонального призначення, рівня автоматизації, ступеня інтегрованості в інформаційно-комунікаційне середовище, а також архітектурних особливостей. Особлива увага приділяється технічним системам, які є частиною критичної інфраструктури або мають підвищені вимоги до стійкості та захищеності.

2. Висвітлення природи, джерел та типології загроз безпеці технічних систем.

Значну увагу приділено аналізу зовнішніх і внутрішніх загроз, які можуть бути реалізовані як унаслідок навмисної дії (кібератаки, саботаж, інсайдерська діяльність), так і через випадкові чи природні чинники (збої, технічні помилки, стихійні лиха). Окремий акцент зроблено на класифікації загроз за рівнем впливу, вектором атаки, джерелом ініціації та потенційними наслідками для цілісності, доступності та конфіденційності систем.

3. Вивчення базових принципів побудови безпечних технічних систем. У посібнику детально розглядаються методологічні основи безпеки, зокрема принцип системного підходу, що передбачає інтеграцію безпеки на всіх етапах життєвого циклу системи – від проектування до експлуатації. Описуються концепції глибокоешелонованого захисту (defense-in-depth), принципи мінімізації довіри, забезпечення відмовостійкості, адаптивності до змін середовища та відповідності чинним регуляторним, галузевим і міжнародним стандартам.

4. Опанування інструментарію аналізу уразливостей і управління ризиками. Здобувачі вищої освіти отримають практичні навички ідентифікації вразливих місць технічних систем, застосування моделей аналізу загроз (наприклад, STRIDE, DREAD), оцінювання ризиків за допомогою кількісних і якісних методів, а також використання методів оптимального управління ризиками на основі концепції ALARP (As Low As Reasonably Practicable).

5. Ознайомлення з міжнародними стандартами та нормативно-правовими засадами безпеки. Навчальний матеріал охоплює ключові міжнародні стандарти, які регулюють питання інформаційної та технічної безпеки, серед яких ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 15408 (Common Criteria), NIST SP 800-53 (Security and Privacy Controls), IEC 62443 (Industrial

Automation and Control Systems Security) тощо. Аналізуються принципи їх імплементації в національних системах технічного регулювання.

6. Висвітлення інноваційних технологій захисту технічних систем. Посібник приділяє увагу сучасним підходам до проектування захищених технічних систем із використанням новітніх технологій: Інтернету речей (IoT), штучного інтелекту (AI), блокчейн-рішень (забезпечення довіри, цілісності та контролю доступу), кіберфізичних систем (CPS), технологій доповненої реальності (AR) для інженерної діагностики, а також систем виявлення аномалій на основі машинного навчання.

7. Формування міждисциплінарних компетентностей у майбутніх фахівців. Особлива увага приділяється розвитку здатності інтегрувати знання з суміжних галузей — кібербезпеки, інженерії, математики, права та управління — для розв'язання складних задач у сфері безпеки технічних систем. Посібник сприяє формуванню мислення, орієнтованого на системну оцінку, комплексну інтеграцію рішень та адаптацію до динамічного техногенного середовища.

Посібник структуровано відповідно до логіки поступового занурення в предметну область — від загальнотеоретичних засад до прикладних інструментів та інновацій. Структура складається з трьох логічно взаємопов'язаних розділів:

Розділ 1. Теоретичні основи безпеки технічних систем — присвячено базовим поняттям, класифікації технічних систем, джерелам загроз, основним принципам безпеки та нормативно-правовій базі. Цей розділ формує методологічну основу розуміння предмета.

Розділ 2. Аналіз вразливостей та засоби захисту технічних систем — подає практичні методики ідентифікації ризиків, оцінювання вразливостей, описує технічні та програмні засоби безпеки, стандартизаційні підходи, а також розглядає специфіку інформаційної безпеки на різних рівнях.

Розділ 3. Інноваційні технології та тренди в забезпеченні безпеки технічних систем — висвітлює сучасні тенденції у сфері захисту складних технічних об'єктів, зокрема питання безпеки IoT, застосування AI та ML, використання блокчейн-технологій, а також концепцію Security by Design як запоруку безпеки на етапі проектування.

Кожен розділ містить відповідні підрозділи, приклади, ілюстрації, тести для самоконтролю знань та список рекомендованої літератури, що дозволяє глибше опрацювати матеріал.

Після опрацювання змісту навчального посібника «Безпека технічних систем» здобувачі вищої освіти мають сформувати комплексну систему знань, умінь та навичок, необхідних для професійного аналізу, проектування, експлуатації та вдосконалення технічних систем з урахуванням чинників безпеки.

Основні результати навчання охоплюють наступні компетентності:

1. Розуміння принципів функціонування технічних систем та їх класифікація. Здобувач вищої освіти повинен глибоко усвідомлювати архітектуру, функціональні механізми та структурні компоненти технічних систем різного типу — від автономних до розподілених і кіберфізичних. Передбачається здатність класифікувати технічні системи за функціональними, конструктивними, технологічними, інформаційними та експлуатаційними ознаками, а також розуміти їхній життєвий цикл у контексті безпеки.

2. Ідентифікація джерел загроз, вразливостей та аналіз ризиків.

Очікується, що здобувач вищої освіти буде здатен ідентифікувати потенційні джерела загроз — як антропогенного, так і природного характеру — для технічних систем, визначати та класифікувати вразливості, оцінювати їх критичність, а також здійснювати багаторівневий аналіз ризиків з використанням сучасних методик (наприклад, SWOT-аналізу, FMEA, Fault Tree Analysis, STRIDE, DREAD, OCTAVE). Важливим результатом є здатність обґрунтовано визначати пріоритети у впровадженні захисних заходів.

3. Опанування практичних навичок розробки заходів безпеки. Здобувач вищої освіти має вміти комплексно планувати та реалізовувати заходи з безпеки, які охоплюють технічну, програмно-апаратну та організаційну складові. Це передбачає знання принципів побудови захищених інформаційних каналів, систем резервування, контролю доступу, криптографічного захисту, систем виявлення вторгнень, а також навички розробки політик безпеки, процедур реагування на інциденти та безпечної поведінки користувачів.

4. Орієнтація у законодавчо-нормативному та стандартному середовищі.

Здобувач вищої освіти повинен мати сформоване уявлення про сучасне нормативне регулювання безпеки технічних систем як у

національному, так і в міжнародному контексті. Це включає знання положень українського законодавства (зокрема, ЗУ «Про основні засади забезпечення кібербезпеки України», ДСТУ) та міжнародних стандартів (ISO/IEC 27001, IEC 62443, NIST, GDPR тощо), а також здатність адаптувати вимоги цих документів до конкретних проектів і ситуацій.

5. Аналіз інноваційних технологій крізь призму безпеки.

Здобувач має вміти критично оцінювати інноваційні технології — такі як штучний інтелект, Інтернет речей (IoT), блокчейн, автономні системи, квантові обчислення — з точки зору їх впливу на рівень технічної безпеки. Важливою складовою є розуміння потенційних ризиків, пов'язаних із впровадженням нових технологій, та розробка рекомендацій щодо їхньої безпечної інтеграції у функціонування складних технічних систем.

6. Проєктування технічних систем з урахуванням принципу "безпека за замовчуванням" (Security by Design).

Очікується, що здобувач буде спроможний впроваджувати безпеку як базовий елемент при проектуванні нових технічних систем. Це передбачає урахування вимог до безпеки на етапі технічного завдання, включення засобів контролю на всіх рівнях (апаратному, програмному, мережевому, користувацькому), використання принципів мінімальних привілеїв, сегментації систем, забезпечення наглядності та трасування подій.

7. Застосування міждисциплінарного підходу у вирішенні проблем безпеки.

Важливим результатом навчання є здатність інтегрувати знання з галузей технічної інженерії, інформаційних технологій, математики, соціальних наук, менеджменту та права для розв'язання комплексних завдань у сфері безпеки технічних систем. Здобувач повинен уміти ефективно працювати в мультидисциплінарних командах, розуміти професійні обмеження суміжних сфер, формулювати системні рішення та здійснювати комунікацію в технічно складних середовищах.

Таким чином, даний посібник є не лише навчальним ресурсом, а й інструментом формування професійної компетентності у сфері технічної безпеки, критичного мислення та навичок адаптації до викликів сучасного техногенного середовища.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ ТЕХНІЧНИХ СИСТЕМ

1.1. Поняття та класифікація технічних систем.

1.1.1. Витоки та еволюція поняття «технічна система»

Поняття «технічна система» виникла на перетині розвитку інженерних наук, кібернетики та загальної теорії систем. Його становлення супроводжувалося зростаючим ускладненням об'єктів технічної діяльності людини, поглибленням розуміння взаємозв'язків між елементами техніки та необхідністю формалізованого опису складних технічних комплексів [31, с. 22].

Історично поняття системи почало формуватися ще у працях філософів античності, зокрема у концепціях Платона й Арістотеля, де вже проглядалося уявлення про цілісність і взаємозв'язок частин. Проте в технічному значенні термін «система» отримав активне використання у XX столітті — у контексті системного підходу, розробленого Людвігом фон Берталанфі та закріпленого в межах загальної теорії систем (General Systems Theory, 1950-ті роки). З цього моменту системність технічних об'єктів розглядається як ключова характеристика, яка дозволяє охоплювати як структурні, так і функціональні аспекти складних інженерних рішень [38, с. 40].

У рамках кібернетики Норберта Вінера технічні системи почали розглядатися не лише як матеріальні конструкції, а й як носії інформаційного обміну та керування. Це поклало початок вивченню технічних систем з позицій інформаційних процесів, що в подальшому дало поштовх до розвитку автоматизованих систем управління, робототехніки та комп'ютерно-орієнтованого інжинірингу.

У радянській школі системного аналізу значний внесок у формування поняття технічної системи здійснили академіки В.М. Глушков, А.А. Ляпунов, Ю.А. Шрейдер. Їхні підходи підкреслювали багаторівневу ієрархічність технічних систем, їхню взаємодію із зовнішнім середовищем і потребу в математичному моделюванні процесів, що відбуваються в таких системах.

У сучасному науково-технічному дискурсі технічна система визначається як інтегрована сукупність взаємопов'язаних елементів — технічних, інформаційних, програмних, іноді й біоте-

хнічних, — яка функціонує як єдине ціле задля досягнення певної цілі або виконання функцій у межах певного середовища [35, с. 29]. Така система має чітко структуровану архітектуру, передбачає процеси взаємодії між складовими та з навколишнім середовищем, а також характеризується певним життєвим циклом.

На сьогодні визначення технічної системи також суттєво варіюється залежно від галузі її застосування.

Наприклад:

a) у мехатроніці — це сукупність механічних, електронних та інформаційних модулів, які діють узгоджено;

b) у промислових АСУ — комплекс апаратно-програмних засобів для управління процесами;

c) у комп'ютерних мережах — інфраструктура взаємодіючих пристроїв для обміну даними;

d) у біоінженерії — симбіоз технічних і біологічних компонентів (нейроінтерфейси, біомеханічні протези).

Іншою важливою віхою в еволюції концепту технічної системи стала поява концепції «техносфери» — штучного середовища, яке створюється і підтримується сукупністю технічних систем, що функціонують на глобальному рівні. З цього погляду кожна технічна система розглядається як елемент більшого техногенного середовища, що підлягає оцінці з позицій екологічності, сталого розвитку, ризиків і надійності.

Сьогодні поняття технічної системи дедалі частіше розглядається не в ізоляції, а в контексті соціотехнічних систем, де технологія взаємодіє з людськими, організаційними та культурними факторами. Це розширює сферу застосування поняття — від традиційних механізмів до складних інтелектуальних комплексів, здатних до самонавчання, адаптації та автономного функціонування.

1.1.2. Міждисциплінарна природа технічних систем

У сучасній науковій думці технічна система розглядається не лише як результат інженерного конструювання, але як феномен, що перебуває на стику багатьох дисциплін: кібернетики, інформатики, соціології, фізики, біоінженерії, екології та навіть когнітивістики. Саме міждисциплінарний підхід дає змогу глибше

осмислити природу технічних систем, їхні властивості, функціонування та перспективи розвитку.

1) Системний підхід

Системний підхід є одним з основних методологічних інструментів для розуміння і аналізу технічних систем, що дозволяє розглядати ці складні об'єкти як цілісні утворення, в яких окремі компоненти взаємодіють між собою з метою досягнення загальної мети функціонування. Це дає змогу подивитися на технічні системи не як на сукупність елементів, а як на органічне ціле, у якому кожен елемент має свою роль і функцію, але всі вони разом виконують завдання, що не можуть бути досягнуті без взаємодії між собою.

Однією з основних характеристик технічних систем, що визначається через системний підхід, є ***ієрархічність***. Це означає, що компоненти технічної системи можуть бути організовані в різні рівні, де на кожному з них виконуються різні функції, що відповідають за забезпечення загальної мети. На вищих рівнях ієрархії можна виділити більш загальні функції, в той час як нижчі рівні займаються більш специфічними операціями. Ієрархія дозволяє не тільки організувати компоненти системи, але й ефективно управляти ними, оптимізувати роботу і забезпечувати більш високий рівень ефективності.

Інтеграція є ще однією важливою характеристикою. Вона передбачає, що всі елементи системи повинні бути взаємопов'язаними та працювати як єдине ціле. Це дозволяє досягти максимального рівня ефективності в реалізації загальної мети, при цьому кожен компонент може виконувати свої спеціалізовані функції, не порушуючи цілісність системи. Інтеграція дозволяє технічним системам бути більш гнучкими і адаптивними до змін, забезпечуючи більш стабільну роботу в умовах змінного зовнішнього середовища.

Емерджентність (виникнення нових властивостей на рівні системи) є ще однією важливою особливістю, притаманною технічним системам, що розглядаються через системний підхід. Вона вказує на те, що при взаємодії компонентів системи можуть виникати нові властивості, які не властиві окремим її елементам. Ці нові властивості часто неможливо передбачити, оскільки вони виникають лише в результаті інтегрованої взає-

модії різних компонентів. Це є важливим фактором при проектуванні складних технічних систем, оскільки еміржентні властивості можуть суттєво впливати на їх функціонування і ефективність.

Відкритість системи є ще однією важливою характеристикою. Відкрита система постійно взаємодіє із зовнішнім середовищем, приймаючи від нього інформацію, енергію, матеріали або інші ресурси. Зовнішнє середовище також може впливати на поведінку системи, тому відкритість дає можливість технічній системі адаптуватися до змінюваних умов та викликів. Це підкреслює важливість системного підходу, оскільки він дозволяє аналізувати взаємодію системи з її оточенням, що є критичним для ефективної роботи у складних і динамічних умовах.

Нарешті, *здатність до саморегуляції* є ключовою характеристикою, яка дозволяє системі підтримувати стабільність і ефективність функціонування без зовнішнього втручання. Це передбачає, що система може автоматично коригувати свої параметри та поведінку в залежності від змін, що відбуваються у її внутрішньому чи зовнішньому середовищі. Саморегуляція може бути забезпечена різними механізмами, такими як зворотний зв'язок, що є основним елементом системної теорії.

В рамках системного підходу розглядаються кілька ключових аспектів, які дозволяють детально вивчити технічні системи та їх функціонування. Зокрема, *структура* системи включає в себе елементи, зв’язки та функції, де кожен елемент має свою конкретну роль, а зв'язки між елементами визначають їх взаємодію. *Взаємодія з зовнішнім середовищем* визначає, як система отримує і обробляє ресурси, а також як вона реагує на зміни в оточенні. *Поведінкові моделі* включають аналіз статичних та динамічних характеристик системи, що дозволяє прогнозувати її роботу в різних умовах.

Основними принципами, які лежать в основі системного підходу, є принципи *цілісності***,** *декомпозиції***,** *ієрархії та зворотного зв'язку***.** Принцип цілісності підкреслює важливість взаємозв’язку всіх елементів системи, декомпозиція дозволяє поділити складну систему на простіші підсистеми, принцип ієрархії визначає рівні взаємодії компонентів, а зворотний зв'язок дає змогу системі реагувати на зміни і підтримувати стабільність.

Усі ці аспекти є основою *системної інженерії***,** дисципліни, яка займається проектуванням, реалізацією та управлінням технічними системами на всіх етапах їх життєвого циклу. Вона застосовує системний підхід для оптимізації роботи технічних систем, що дозволяє не тільки створювати нові інженерні рішення, але й ефективно управляти існуючими системами, забезпечуючи їхню безпеку, надійність та ефективність в умовах змінного середовища.

2) Кібернетичний підхід

Кібернетика, як наука, що вивчає процеси керування в складних системах, відіграє важливу роль у розвитку розуміння технічних систем. Вона дозволила розширити погляд на ці системи не лише як на набори механічних або електронних компонентів, а й як на складні структури, що здатні до збирання, оброблення, зберігання та передавання інформації. Таким чином, технічна система почала сприйматися не лише як фізичний об'єкт, а й як інтерактивна система, здатна реагувати на зміни як внутрішнього, так і зовнішнього середовища завдяки інформаційним потокам, що циркулюють між її елементами.

У кібернетичному підході технічна система розглядається як контур керування, де поєднуються прямі і зворотні зв'язки, що забезпечують зворотній контроль над поведінкою системи та дозволяють здійснювати її адаптацію до змінних умов. Цей контур управляє різними процесами всередині системи, забезпечуючи виконання поставлених завдань у заданих межах, а також реагує на впливи ззовні. Таке розуміння дозволяє формулювати концепцію ***адаптивності*** та ***саморегуляції*** технічних систем, що є необхідними властивостями для забезпечення їх стійкості та ефективної роботи в умовах динамічних змін.

Однією з основних характеристик кібернетичного підходу є *категоріальність*, що дозволяє здійснювати системний аналіз через виділення кількох ключових категорій, важливих для розуміння функціонування технічних систем:

a) Система управління — це елемент, що виконує роль директиви, управлінця, що організовує і контролює діяльність технічної системи. У контексті кібернетики система управління визначає, які ресурси і в якій формі повинні бути надані об’єкту управління для виконання його функцій.

b) Об’єкт управління — це технічна система або її складова частина, яка підлягає управлінню. Це можуть бути як фізичні

компоненти (механізми, пристрої, технічні пристрої), так і процеси, які відбуваються в цих компонентах (наприклад, обробка інформації або виконання математичних обчислень).

c) Сигнал/інформація — категорія, яка відповідає за передачу даних, що використовуються для регулювання та контролю. Це можуть бути електричні сигнали, цифрові дані, сенсори або інші форми передачі інформації, що є необхідними для здійснення керування.

d) Зворотний зв'язок — механізм, завдяки якому система отримує інформацію про результат своїх дій, що дозволяє коригувати її поведінку. Зворотний зв'язок може бути позитивним (коли зміни в системі сприяють її розвитку) або негативним (коли система коригує свої дії для збереження стабільності та уникнення помилок).

e) Алгоритм функціонування — це послідовність дій, яка визначає, як система повинна реагувати на вхідні сигнали та внутрішні стани, щоб досягти поставленої мети. Алгоритм може бути змінним або статичним залежно від типу системи та її складності.

Завдяки розвитку кібернетики стало можливим глибше розуміння принципів, що лежать в основі *автоматизації, робототехніки, штучного інтелекту* та *цифрових обчислювальних систем*.

Ці технології, засновані на кібернетичних принципах, стали не лише важливими складовими сучасних технічних систем, але й ключовими факторами їх розвитку та вдосконалення *за наступними напрямами*.

a) Автоматизація дозволяє виконувати повторювані або складні оп ерації без участі людини, що підвищує ефективність та точність систем.

b) Робототехніка дає змогу створювати механізми та машини, які здатні виконувати фізичні та інтелектуальні завдання, що раніше вимагали людської участі. Ці роботи оснащуються сенсорами та системами зворотного зв'язку, що дозволяє їм адаптуватися до змінюваних умов.

c) Штучний інтелект використовує алгоритми, які дають можливість системам «навчатися» на основі отриманого досвіду

і змінювати своє поведінкове рішення залежно від нових ситуацій, що виникають.

d) Цифрові обчислювальні системи, які здатні обробляти великі обсяги інформації, виконувати складні математичні операції та моделювати процеси, стали основою для створення складних технічних систем, таких як автоматичні управлінські системи, системи штучного інтелекту, цифрові виробничі лінії та інші.

Таким чином, кібернетичний підхід не лише змінив уявлення про технічні системи, але й став основою для створення новітніх технологій, які вже є важливими складовими частинами нашого повсякденного життя. Його принципи дозволяють розробляти більш ефективні, адаптивні та саморегулюючі системи, що відкриває нові горизонти в інженерії, інформаційних технологіях, робототехніці та багатьох інших галузях

3) Інформаційний та когнітивний підходи

Сучасні технічні системи зазнають значних змін під впливом технологічних досягнень, що орієнтуються на інтеграцію інформаційних процесів на всіх етапах їхнього функціонування. Інноваційні підходи, такі як обробка великих обсягів даних (Big Data), використання штучного інтелекту для прийняття рішень та здатність до самонавчання, формують нову парадигму розвитку технічних систем. Від традиційних механічних і електронних пристроїв ці системи тепер відрізняються можливістю самостійно обробляти та адаптуватися до різноманітних змінних умов, що значно розширює їхні функціональні можливості та сферу застосування.

У цьому контексті технічні системи перетворюються на когнітивні, що означає здатність до виконання більш складних інтелектуальних функцій. Когнітивні технічні системи мають можливість *перцепції* (розпізнавання та інтерпретація інформації з навколишнього середовища), *аналізу* (обробка та виведення корисних знань із зібраних даних), *планування* (визначення шляхів досягнення поставлених цілей), *прийняття рішень* (оцінка варіантів і вибір оптимальних стратегій) і *самокорекції* (автоматичне коригування своїх дій на основі отриманого зворотного зв’язку). Ці функції наближають технічні системи до рівня "штучного" мислення, дозволяючи їм працювати не лише за

заданими алгоритмами, але й адаптуватися до нових і змінних умов, навчатися з досвіду та робити висновки на основі попередніх результатів.

Когнітивний підхід відкриває можливості для моделювання технічних систем як суб'єктів з мінімальним рівнем «штучного» мислення, що дозволяє забезпечити вищу гнучкість, адаптивність і здатність до самонавчання без необхідності постійної участі людини в процесі прийняття рішень. Такі системи можуть не лише виконувати завдання на основі попередньо закладених програм, а й самостійно аналізувати дані, виявляти закономірності та приймати ефективні рішення у реальному часі. Це вимагає впровадження до складу систем складних компонентів, таких як *семантичний аналіз* — процес інтерпретації інформації на більш високому рівні, що дозволяє системам краще «розуміти» дані та використовувати їх для прийняття рішень.

Завдяки когнітивному підходу, технічні системи можуть працювати в умовах *невизначеності*. Це означає, що системи здатні адаптуватися до непередбачуваних ситуацій, змінюючи стратегії в реальному часі залежно від зміни обставин. Такий рівень гнучкості та автономності робить когнітивні системи надзвичайно потужними інструментами для виконання завдань, які раніше вимагали постійного людського контролю або були б надто складними для традиційних технічних рішень.

Практичні приклади когнітивних технічних систем вже сьогодні включають такі інноваційні технології, як *автономні транспортні засоби***.** Вони здатні не тільки оцінювати ситуацію на дорозі, а й прогнозувати потенційні небезпеки, приймати рішення в екстрених ситуаціях та вчитися на своєму досвіді. Аналогічні принципи застосовуються в **розумних мережах** (smart grid), де системи автоматично оптимізують споживання енергії, регулюючи її доставку та розподіл в залежності від змін на ринку та потреб користувачів.

Безпілотні бойові комплекси також використовують когнітивні системи для автономного прийняття рішень, аналізуючи ситуацію на полі бою та виконуючи завдання без безпосередньої участі людини. Крім того, в області *систем ситуаційної обізнаності* когнітивні технології дозволяють створювати платформи, які можуть зібрати, проаналізувати і представити інформацію про поточну ситуацію, допомагаючи оперативним підрозділам

приймати рішення на основі реальних даних у режимі реального часу.

Таким чином, когнітивні технічні системи перетворюються на інтеграційні компоненти складних, адаптивних та самонавчальних інфраструктур, здатних до ефективного управління та прийняття рішень у динамічних умовах. Вони відкривають нові горизонти в інженерії, транспорті, енергетиці, обороні та багатьох інших галузях, де автономність і швидкість реагування мають критичне значення для досягнення оптимальних результатів.

4) Біоінженерний та біонічний підходи

Інтенсивний розвиток інформаційних технологій (ІТ) та кібернетики, паралельно з революційними досягненнями в біології, створює нові можливості для інтеграції біологічних та технічних знань. Це дозволяє розвивати і вдосконалювати гібридні технічні системи, які поєднують властивості живих організмів і високі технології. Така інтеграція стала важливим етапом розвитку сучасних наукових напрямів, таких як біоінженерія та біоніка.

Біоінженерія, як наука, орієнтована на вирішення технічних задач за допомогою принципів, які застосовуються в організації живих систем. Вона спрямована на адаптацію біологічних принципів до технічних задач, що дає змогу створювати новітні матеріали та пристрої, що функціонують за принципами живих організмів. Ці рішення відкривають нові горизонти в області медицини, робототехніки та екології, дозволяючи розробляти такі інновації, як біоадаптивні протези та сенсори на основі біологічних рецепторів.

З іншого боку, біоніка є наукою, що вивчає механізми природи з метою їхнього технічного відтворення. Вивчення біологічних систем та процесів дозволяє створювати інженерні рішення, що імітують природні механізми для досягнення кращої ефективності та адаптивності. Наприклад, біонічні протези та імплантати здатні не лише відновлювати втрачені функції, але й інтегруватися з нервовою системою людини, реагуючи на сигнали та адаптуючись до змін навколишнього середовища.

Ці технології дозволяють створювати автономні системи, здатні працювати в реальному часі, реагуючи на зовнішні зміни та сигнали від організму. Наприклад, біоадаптивні протези мо-

жуть виявляти зміни в нервових імпульсах і автоматично коригувати свої параметри для покращення функціонування. Завдяки цьому можна досягти більш високої точності в роботі таких пристроїв, значно покращуючи якість життя людей з інвалідністю.

Одним із важливих результатів інтеграції біологічних і технічних знань є розробка нейроінтерфейсів, які дозволяють безпосередньо з'єднати мозок з комп'ютерними системами, а також біомеханічних імплантатів, що мають здатність відновлювати фізіологічні функції організму. Подібні інтерфейси дають змогу людям, які втратили здатність до руху або відчуття, знову взаємодіяти з навколишнім світом, використовуючи технології для управління пристроями безпосередньо за допомогою мозкових сигналів.

Розробка «розумного» одягу та пристроїв доповненої реальності є ще одним кроком у розвитку цих гібридних систем. Такий одяг може реагувати на фізіологічні зміни користувача, а також забезпечувати інтерактивний досвід, збільшуючи його фізіологічні можливості. Пристрої доповненої реальності дають можливість розширити межі сприйняття, збагачуючи реальний світ віртуальними об'єктами та створюючи нові можливості для навчання, роботи та взаємодії.

Таким чином, синергія біологічних і технічних наук відкриває нові горизонти для розвитку інновацій, що безпосередньо впливають на покращення якості життя людини та змінюють способи взаємодії з технологіями. Розробка гібридних систем, що поєднують найкраще з біології та інженерії, дозволяє створювати пристрої, які не лише відновлюють втрачені функції, а й розширюють можливості людини, забезпечуючи їй більшу свободу та автономність

5) Соціотехнічний підхід

Сучасні технічні системи мають одну з найважливіших характеристик — тісну взаємодію з людиною. Це призводить до інтеграції технічних та соціальних аспектів у межах соціотехнічних систем, де ефективність системи визначається не лише технічною досконалістю, але й соціальними факторами, такими як організаційна культура, рівень кваліфікації персоналу, правові обмеження та інші елементи соціального середовища. Такий підхід сприяє глибшому розумінню складності взаємодії між

людьми та технологіями, а також дає можливість оптимізувати роботу систем в реальних умовах.

Соціотехнічні системи, за визначенням, включають в себе не лише технічні компоненти, а й організаційні та соціальні структури. Це дозволяє максимально ефективно враховувати всі фактори, які можуть впливати на продуктивність і безпеку, а також забезпечити більш комплексний підхід до проектування й управління системами. Наприклад, у процесі впровадження нових технологій або розробки складних технічних систем важливо враховувати не тільки технічні характеристики, але й вплив на соціальну структуру організації, взаємодію людей у команді, а також інші соціальні й культурні аспекти, які можуть впливати на роботу системи в цілому.

Одним з важливих напрямків у вивченні соціотехнічних систем є аналіз взаємодії людини та машини (HMI), який фокусується на тому, як люди взаємодіють із технічними пристроями, яким чином ці пристрої адаптуються до людських можливостей та обмежень, а також як вплив людини на систему може бути оптимізований для досягнення кращих результатів. Такий підхід враховує як фізіологічні аспекти — наприклад, зручність використання інтерфейсів, так і психологічні: рівень стресу, втоми, а також емоційну складову взаємодії.

Врахування людського фактора є особливо важливим у контексті критичних інфраструктур, таких як енергетичні системи, транспорт, охорона здоров'я або національна безпека. У таких сферах нещасні випадки або помилки можуть мати катастрофічні наслідки, тому важливо враховувати, як вплив людського фактору може бути мінімізований за допомогою технологічних рішень. Це може включати розробку автоматизованих систем, які здатні підтримувати або навіть заміняти людину в небезпечних ситуаціях, а також надання користувачам інтуїтивно зрозумілих і зручних інтерфейсів для мінімізації ймовірності помилок.

Врахування людського фактору та його вплив на зайнятість є також важливим аспектом соціотехнічного аналізу, зокрема в контексті автоматизації та впровадження нових технологій, таких як штучний інтелект і робототехніка. Автоматизація виробничих процесів і технологічних операцій може змінювати стру-

ктуру ринку праці, знижуючи потребу в людських ресурсах у деяких сферах, водночас створюючи нові можливості для працевлаштування в інших. Задача соціотехнічного аналізу полягає в тому, щоб передбачити ці зміни та забезпечити баланс між автоматизацією та зайнятістю, а також підтримати кваліфікацію та перепідготовку персоналу для нових умов.

Таким чином, проектування складних технічних систем потребує всебічного підходу, що враховує не тільки технічні аспекти, але й соціальні, психологічні та етичні фактори. Важливими елементами такого проектування є безпека користувача, ергономіка (зручність та комфорт використання системи), етичні питання, що виникають через технологічний прогрес, а також створення довіри користувача до нових технологій. Проектування технологій з урахуванням цих факторів дозволяє значно підвищити ефективність і безпеку технічних систем, а також забезпечити їх адаптацію до потреб і можливостей людини.

1.1.3. Основні елементи та властивості технічної системи

Технічна система як складна організована структура складається з сукупності елементів, кожен з яких виконує певну функцію в досягненні загальної цілі [24, с. 48]. Залежно від рівня абстракції ці елементи можуть мати фізичну (матеріальну), логічну (функціональну) або інформаційну природу. Системний підхід до дослідження технічних систем передбачає ідентифікацію та опис основних складових і властивостей, що забезпечують ефективність, стабільність, адаптивність та безпечність функціонування.

1) Структурні елементи технічної системи

Універсальна модель технічної системи являє собою абстрактну структуру, яка дає можливість описати практично будь-яку систему незалежно від її конкретного призначення чи функціональних характеристик. Згідно з такою моделлю, технічна система складається з кількох основних компонентів, кожен з яких виконує свою специфічну роль, забезпечуючи ефективне функціонування і досягнення поставлених цілей. Ось більш детальний опис кожного з цих компонентів:

*а) Енергетичний компонент***.** Енергетичний компонент є основою для живлення і підтримки функціонування технічної сис-

теми. Його завдання полягає в тому, щоб забезпечити необхідну енергію для роботи всіх інших компонентів системи, включаючи механічну, електричну, теплову чи інші види енергії. Прикладами енергетичних компонентів є різноманітні двигуни, що перетворюють енергію в механічний рух, акумулятори та генератори, що зберігають і виробляють енергію, а також мережі живлення, які передають енергію до різних частин системи. Цей компонент забезпечує стабільність роботи технічної системи, перешкоджаючи її «виходу з ладу» через відсутність або неполадки в джерелах енергії.

b) Функціонально-операційний (виконавчий) компонент. Функціонально-операційний компонент є серцем будь-якої технічної системи, оскільки він безпосередньо реалізує основні технологічні чи фізичні процеси, задля яких створена система. Це можуть бути виробничі механізми, такі як верстати або автоматизовані лінії виробництва, оброблювальні машини, які виконують механічну чи хімічну обробку матеріалів, або виконавчі пристрої в автоматизованих комплексах, що здатні виконувати точно налаштовані операції. Цей компонент є відповідальним за реалізацію задачі системи і її ефективність.

c) Управлінський компонент. Управлінський компонент забезпечує координацію та регулювання діяльності інших компонентів системи, що дозволяє ефективно досягати поставлених цілей при певних умовах. Він включає в себе датчики, що збирають дані про стан різних частин системи, контролери та мікропроцесори, які на основі отриманої інформації здійснюють прийняття рішень і управляють роботою виконавчих пристроїв. Програмні засоби дозволяють задавати алгоритми управління і налаштовувати параметри роботи системи. Мережеві інтерфейси з'єднують різні елементи системи, дозволяючи здійснювати їх взаємодію в реальному часі. Цей компонент є основою для автоматизації та оптимізації процесів.

d) Інформаційний компонент. Інформаційний компонент технічної системи забезпечує збір, обробку, зберігання та передавання інформації, яка необхідна для її функціонування та адаптації до змін навколишнього середовища чи внутрішніх умов. Це можуть бути бази даних, що зберігають інформацію про стан елементів системи або результати виконаних операцій. Також

сюди входять сенсорні модулі, які здійснюють вимірювання параметрів системи, та алгоритми обробки сигналів, що дозволяють перетворювати дані в корисну інформацію для подальшого аналізу і прийняття рішень.

е) Комунікаційний компонент. Комунікаційний компонент забезпечує ефективну взаємодію як між елементами самої системи, так і між системою та зовнішнім середовищем. Він включає в себе різні види проводових та безпровідних каналів зв'язку, через які передається інформація, а також протоколи взаємодії, що регулюють обмін даними між компонентами. Системи введення-виведення дозволяють взаємодіяти з користувачами або іншими зовнішніми пристроями, таким чином забезпечуючи інтеграцію системи в більш широкий технологічний контекст.

f) Людино-машинний інтерфейс (HMI). Людино-машинний інтерфейс є тим компонентом, який забезпечує зручне і ефективне взаємодію людини з технічною системою. Це дозволяє оператору або користувачу контролювати систему, змінювати її параметри, здійснювати моніторинг її роботи і отримувати зворотний зв'язок. До цього компонента входять різноманітні дисплеї, панелі керування, елементи візуалізації, а також сучасні технології, такі як системи доповненої реальності, які дозволяють значно полегшити управління та знизити ймовірність помилок оператора при взаємодії з системою.

Усі ці компоненти взаємодіють між собою, утворюючи цілісну структуру технічної системи, де кожен з них виконує свою специфічну функцію. їх інтеграція дозволяє системі працювати ефективно та адаптуватися до змінних умов навколишнього середовища [51, с. 1-4].

2) Життєвий цикл технічної системи

Життєвий цикл технічної системи — це послідовність етапів, через які проходить система від моменту її концептуалізації до кінця експлуатації та утилізації. Кожен з цих етапів має своє значення та специфічні завдання, які сприяють успішному впровадженню, ефективному функціонуванню та безпеці системи. Крім того, на кожному етапі життєвого циклу важливо враховувати інтеграцію різних управлінських та технічних аспектів,

таких як управління якістю, оцінка ризиків, енергетична ефективність та кібербезпека.

a) Ідентифікація потреб (визначення проблеми або завдання)

Цей етап є початковим і є основою для формування всієї системи. Він включає в себе аналіз існуючих проблем, завдань або потреб, які повинна вирішити система. Ідентифікація потреб часто передбачає тісну взаємодію з кінцевими користувачами або замовниками, щоб зрозуміти їхні вимоги та критерії успіху. У цей період також здійснюється виявлення обмежень, таких як бюджет, час, ресурси, а також потенційні зовнішні та внутрішні фактори, які можуть вплинути на подальший процес проектування та виробництва.

На цьому етапі необхідно застосовувати методи оцінки ризиків, щоб вже на ранніх стадіях передбачити можливі загрози та забезпечити належний рівень безпеки. Також важливим є інтегрування енергетичної ефективності, оскільки багато сучасних технічних систем орієнтовані на мінімізацію витрат енергії з самого початку проектування.

b) Проектування (технічне та функціональне моделювання)

На етапі проектування створюється основна концепція технічної системи, яка включає в себе технічне та функціональне моделювання. Технічне моделювання передбачає детальну розробку архітектури системи, її складових елементів і їх взаємодії. Функціональне моделювання орієнтоване на визначення ролі кожного компонента системи та на реалізацію функцій, необхідних для виконання основних завдань.

Цей етап є критично важливим для створення ефективної системи, оскільки правильне проектування визначає її працездатність, надійність та безпеку. Одним із ключових аспектів є впровадження системи управління якістю, яка забезпечить високий рівень виконання проекту відповідно до стандартів. Також в процесі проєктування необхідно здійснювати оцінку та зменшення ризиків, які можуть виникнути в процесі виробництва та експлуатації системи.

c) Виробництво (збірка, налаштування, тестування)

Після того, як система спроектована, настає етап виробництва. Він включає в себе процеси зборки, налаштування та тестування. Збірка системи може бути як серійною, так і індивідуаль-

ною, в залежності від призначення системи та її складності. Після зборки відбувається налаштування, що передбачає конфігурацію системи відповідно до специфікацій і вимог, визначених на попередніх етапах.

Тестування є важливою частиною цього етапу, оскільки воно дозволяє перевірити працездатність системи, виявити можливі дефекти або несправності, а також оцінити відповідність системи заданим параметрам та вимогам. Під час тестування також перевіряється енергетична ефективність системи, її здатність працювати в умовах змінних навантажень та надійність в довгостроковій перспективі.

d) Експлуатація (основний етап роботи)

Етап експлуатації є основним у життєвому циклі технічної системи, оскільки на цьому етапі система виконує свої основні функції. Під час експлуатації здійснюється моніторинг її роботи, контроль параметрів, а також своєчасне виявлення і усунення неполадок. Важливою частиною цього етапу є збереження високого рівня безпеки, захист від кіберзагроз та забезпечення надійної роботи в умовах зовнішніх змін.

Впровадження кібербезпеки в цей період стає надзвичайно важливим, оскільки зростає кількість кіберзагроз та потенційних атак, що можуть вплинути на роботу системи. Також важливо постійно оцінювати та знижувати ризики, що виникають у процесі експлуатації, та реагувати на змінювані зовнішні фактори.

e) Обслуговування (технічна підтримка, модернізація, ремонт)

Обслуговування є етапом, який забезпечує тривалу та ефективну роботу технічної системи протягом її життєвого циклу. Він включає в себе різні аспекти, такі як технічна підтримка, модернізація та ремонт. Технічна підтримка передбачає надання консультацій і допомоги користувачам, вирішення проблем, що виникають під час експлуатації, а також регулярний моніторинг та аналіз роботи системи.

Модернізація полягає у вдосконаленні або оновленні технічних компонентів системи з урахуванням нових технологій або змін у вимогах. Ремонт, в свою чергу, забезпечує відновлення працездатності системи після виникнення несправностей або

поломок. На цьому етапі також необхідно звертати увагу на енергетичну ефективність, оскільки вдосконалення енергоспоживання може значно знизити витрати на експлуатацію системи.

f) Утилізація або рециклінг (зняття з експлуатації, переробка)

Останнім етапом є утилізація або рециклінг системи, коли вона більше не може бути використана для виконання своїх функцій. Цей процес включає в себе зняття системи з експлуатації, демонтаж та її утилізацію або переробку. Важливою частиною цього етапу є забезпечення екологічної безпеки, зокрема, правильне поводження з відходами, які можуть бути токсичними чи небезпечними для навколишнього середовища.

Цей етап також включає в себе аналіз використання ресурсів та енергетичної ефективності, щоб у майбутньому уникнути значних витрат при утилізації або переробці компонентів системи.

3) Інтеграція систем управління якістю, оцінки ризиків, енергетичної ефективності та кібербезпеки

На кожному етапі життєвого циклу важливо забезпечити інтеграцію різних аспектів управління, таких як системи управління якістю, що відповідають за підтримання високих стандартів на всіх етапах; оцінка ризиків, яка допомагає передбачити та мінімізувати потенційні загрози для системи; енергетична ефективність, яка дозволяє оптимізувати використання енергетичних ресурсів на всіх етапах життєвого циклу; і кібербезпека, яка має забезпечити захист від зовнішніх і внутрішніх кіберзагроз у процесі роботи системи.

Таким чином, кожен етап життєвого циклу технічної системи вимагає ретельного планування і інтеграції різних управлінських та технічних інструментів для досягнення максимальних результатів і забезпечення ефективності та безпеки на всіх етапах її існування.

4) Ключові характеристики, що визначають ефективність функціонування технічної системи

Для забезпечення ефективного функціонування технічної системи важливою є наявність низки ключових характеристик, які визначають її здатність до успішного виконання покладених на неї завдань в умовах змінного середовища. Ці характеристики не тільки забезпечують стабільну роботу системи, але й дозволяють адаптуватися до нових вимог і викликів. Розглянемо основ-

ні елементи, які складають ці характеристики, та їх значення для технічної системи.

a) Надійність

Надійність технічної системи визначається її здатністю підтримувати працездатність протягом визначеного інтервалу часу за умов, що описуються відповідними технічними параметрами та середовищем експлуатації. Це одна з найважливіших характеристик, оскільки система, яка не відповідає вимогам щодо надійності, може стати причиною значних втрат, як фінансових, так і часу, а також ризику для безпеки.

Надійність включає кілька ключових аспектів:

– *безвідмовність* — здатність системи працювати без збоїв протягом певного періоду.

– *довговічність* — здатність зберігати свої функціональні характеристики і ефективність протягом тривалого часу.

– *ремонтопридатність* — можливість ефективно відновлювати працездатність системи після її поломок або збоїв.

– *збережуваність* — здатність системи підтримувати працездатність навіть при несприятливих умовах або зношуванні елементів.

Надійність є основою для розробки ефективних технічних рішень, які забезпечують тривалу й безпечну експлуатацію систем.

b) Адаптивність

Адаптивність є важливою характеристикою для технічних систем, які функціонують в умовах змінного середовища або при змінних внутрішніх параметрах. Вона визначає здатність системи змінювати свій режим роботи в залежності від зовнішніх або внутрішніх змін, таких як зміна навантаження, температури, вологості чи інших умов середовища.

Адаптивність дозволяє системі:

– *змінювати* свої параметри роботи в реальному часі, щоб підтримувати оптимальний рівень ефективності.

– *реагувати* на зміни умов або зовнішні втручання, що дозволяє продовжити стабільну роботу, навіть при коливаннях у навантаженні або наявності непередбачених обставин.

– *мінімізувати* ризики збоїв або аварій через оперативну зміну режиму роботи.

Ця характеристика є критично важливою в умовах динамічних та непередбачуваних умов експлуатації, таких як автоматизовані системи або інтелектуальні мережі.

c) Масштабованість

Масштабованість характеризує можливість технічної системи збільшувати свою потужність або розширювати функціональність без необхідності значних змін в архітектурі системи. Це важлива характеристика для систем, які мають рости або змінюватися відповідно до потреб користувачів чи організацій, що їх експлуатують.

Масштабованість включає в себе:

– легкість інтеграції нових компонентів — здатність системи додавати нові функції або збільшувати обсяг обробки без порушення її загальної структури.

– гнучкість в масштабуванні — можливість розширювати потужності без втрат у стабільності або якості роботи.

– підвищення потужності — можливість збільшення ресурсів, таких як процесорна потужність, пам'ять, зберігання даних.

Ця характеристика особливо важлива для великих розподілених систем, таких як хмарні обчислення або інфраструктура IoT.

d) Інтероперабельність

Інтероперабельність — це здатність технічної системи ефективно взаємодіяти з іншими системами через стандартизовані протоколи, інтерфейси та механізми. Це одна з основних характеристик для систем, що мають працювати в багатокомпонентних середовищах, де важлива взаємодія різних технічних рішень.

Основні аспекти інтероперабельності включають:

– *сумісність із іншими системами* — здатність працювати з різними апаратними та програмними рішеннями.

– *стандартизовані протоколи* — використання загальноприйнятих стандартів для забезпечення ефективної взаємодії.

– *взаємодія через інтерфейси* — забезпечення зручних і ефективних способів зв'язку між різними компонентами або підсистемами.

Інтероперабельність є важливою для інтеграції різних технологічних платформ у єдину систему, що дозволяє створювати розподілені або гібридні інфраструктури.

е) Інтелектуальність

Інтелектуальність технічної системи відноситься до наявності вбудованих або зовнішніх механізмів, які дозволяють системі приймати рішення, навчатися з досвіду та здійснювати діагностику. Система з високим рівнем інтелекту здатна автоматично адаптувати свою поведінку, реагувати на зміни і виконувати складні функції без постійного втручання людини.

Це включає:

– *самонавчання* — здатність системи покращувати свою ефективність на основі отриманих даних і досвіду.

– *прийняття рішень* — наявність алгоритмів для автоматичного ухвалення рішень на основі аналізу даних.

– *діагностика* — здатність системи виявляти і усувати неполадки в роботі.

Інтелектуальність дозволяє системам функціонувати більш автономно і ефективно, що особливо важливо для таких технологій, як штучний інтелект, машинне навчання або автоматизація.

f) Кіберфізична інтеграція

Кіберфізична інтеграція стосується здатності технічної системи взаємодіяти з фізичним світом через цифрові сервіси, вбудовані сенсори та інші системи IoT. Це дозволяє системам здійснювати взаємодію між реальними об'єктами і їх цифровими копіями для аналізу, моніторингу та оптимізації роботи.

Основні аспекти кіберфізичної інтеграції включають:

– *Взаємодія з фізичними об'єктами* — здійснення збору даних через сенсори та їх передавання для подальшої обробки.

– *IoT-системи* — інтеграція в мережу Інтернет речей для збору та аналізу даних у реальному часі.

– *Цифрові сервіси* — використання цифрових інструментів для взаємодії з фізичними елементами та їх управління.

Ця характеристика дозволяє створювати високотехнологічні системи для моніторингу та управління фізичними процесами через цифрові платформи.

g) Безпека

Безпека є необхідною умовою для успішної роботи технічної системи в умовах зовнішніх та внутрішніх загроз. Вона включає в себе захист від помилок користувачів, зловмисних атак, кіберзагроз, а також мінімізацію техногенних ризиків.

Основні аспекти безпеки включають:

– *захист від кіберзагроз* — використання методів криптографії, аутентифікації, захисту даних.

– *захист від техногенних ризиків* — забезпечення безпеки апаратних і програмних компонентів системи.

– *помилки користувача* — мінімізація впливу людського фактора на роботу системи.

Забезпечення безпеки є необхідною умовою для підтримки стабільної і безпечної роботи системи, а також для запобігання збоїв і атак.

Таким чином, ефективне функціонування технічної системи залежить від цих характеристик, кожна з яких забезпечує її здатність адаптуватися, масштабуватися, працювати в інтегрованому середовищі та виконувати завдання в умовах безпеки і стабільності

5) Взаємозв'язок структури і властивостей

Проектування технічної системи є складним та багатоаспектним процесом, що вимагає не тільки раціонального вибору елементів, але й всебічного аналізу їх взаємодії, сценаріїв експлуатації, а також оцінки зовнішніх впливів та ризиків. Структура технічної системи формує основу для реалізації її ключових властивостей, що значною мірою визначає експлуатаційні можливості, надійність та безпеку.

6) Децентралізація та модульність: масштабованість та ремонтопридатність

Одним із важливих принципів структурування технічних систем є децентралізація з модульною архітектурою. Такий підхід дозволяє забезпечити гнучкість та адаптивність до змінних умов експлуатації. Децентралізована структура забезпечує високу масштабованість за рахунок можливості незалежного збільшення функціональних блоків без порушення загальної цілісності системи. Наприклад, у системах Інтернету речей (IoT) застосовується модульна архітектура з можливістю підключення нових пристроїв без переривання роботи основної мережі.

Модульність також сприяє ремонтопридатності: у разі виходу з ладу окремого компонента його можна замінити або відключити без значного впливу на функціонування всієї системи. Це особливо важливо в умовах промислових або критично важливих технічних комплексів, де простої неприпустимі.

7) Зворотні зв'язки як основа адаптивності та інтелектуальності

Інтелектуальні технічні системи характеризуються наявністю зворотних зв’язків, що дозволяє адаптуватися до зміни параметрів середовища або вимог користувача. Зворотний зв'язок забезпечує можливість автоматичного коригування дій системи залежно від поточного стану. Наприклад, у системах автоматичного керування зворотні зв’язки дозволяють підтримувати стабільність функціонування при зовнішніх збуреннях.

У кіберфізичних системах (КФС) зворотний зв'язок забезпечує інтеграцію фізичних процесів та обчислювальних елементів, що сприяє створенню адаптивних та самонавчальних механізмів. Таким чином, наявність зворотних зв’язків є ключовою умовою інтелектуальності технічної системи.

8) Резервування як запорука надійності

Надійність технічної системи прямо залежить від резервування критичних компонентів. Резервування передбачає наявність дублюючих елементів, які автоматично активуються у разі відмови основного вузла. Це дозволяє знизити ризики простою або втрати функціональності внаслідок апаратних чи програмних збоїв.

У складних технічних системах, таких як авіоніка або енергетичні комплекси, використовуються багаторівневі резервні механізми: від дублювання окремих сенсорів до побудови паралельних обчислювальних контурів. Такий підхід дозволяє забезпечити безперервність функціонування навіть у критичних ситуаціях.

9) Ізоляція та кібербезпека

У сучасних умовах кібербезпека є одним з ключових аспектів проектування технічних систем. Ступінь ізоляції ключових елементів та програмний захист визначають здатність системи протистояти кібератакам та іншим загрозам. Наприклад, у розподілених системах управління ізоляція критичних модулів від зовнішніх мереж мінімізує ризики несанкціонованого втручання.

Крім того, використання вбудованих механізмів шифрування, багаторівневої аутентифікації та моніторингу аномалій дозволяє своєчасно виявляти спроби компрометації системи. У контексті інтелектуальних інфраструктур необхідно приділяти увагу сегментації мереж та впровадженню ізольованих обчислювальних середовищ для захисту критичних компонентів.

10) Комплексний підхід до проектування

З огляду на вищезазначене, проектування технічної системи не обмежується лише вибором відповідних елементів. Необхідно здійснювати комплексний аналіз їх взаємодії, моделювати різні сценарії експлуатації та враховувати зовнішні чинники ризику. Такий підхід дозволяє створити структуру, яка є не тільки функціональною, але й адаптивною, надійною та захищеною від зовнішніх загроз.

Таким чином, успішна реалізація технічної системи потребує балансу між інноваційністю архітектури, надійністю компонентів та захищеністю від сучасних кіберзагроз. Використання децентралізованих, модульних та адаптивних принципів дозволяє формувати інфраструктури, що здатні до довготривалої ефективної експлуатації.

1.1.4. Класифікація технічних систем за ознаками та сферами застосування

Класифікація технічних систем — ключовий інструмент для їх аналізу, проектування, вибору та оцінки. Вона ґрунтується на визначенні спільних ознак і критеріїв, які дозволяють впорядкувати різноманітні технічні об’єкти в ієрархічні, функціональні, структурні або прикладні категорії. Правильно розроблена класифікація дозволяє виявити закономірності, уніфікувати процеси управління, стандартизувати підходи до створення та експлуатації технічних рішень.

1) Класифікація за ступенем складності

У сучасному технічному світі системи класифікують за різними критеріями, одним із найважливіших з яких є ступінь складності. Така класифікація дозволяє ефективно структурувати різноманітні технічні рішення та розуміти їх особливості з точки зору функціонування та управління. Основні категорії технічних систем за ступенем складності включають прості, складні та ультраскладні системи.

a) Прості технічні системи

Прості технічні системи характеризуються обмеженою кількістю функціональних елементів та прямолінійною структурою. Їхні компоненти здебільшого взаємодіють за принципом послідовності, без складних зворотних зв'язків чи механізмів саморегуляції. Такі системи зазвичай виконують одну або декілька базових функцій без значного взаємного впливу компонентів. Наприклад, кишеньковий ліхтар складається з джерела енергії (батарейки), лампочки та вимикача. Інші приклади включають механічні важелі, термометри тощо. Через простоту своєї структури подібні системи є передбачуваними та легко керованими.

b) Складні технічні системи

На відміну від простих, складні технічні системи мають значну кількість взаємозалежних компонентів, які утворюють складні функціональні зв'язки. Основною рисою складних систем є наявність зворотних зв'язків, інформаційної взаємодії та емерджентних властивостей — тобто характеристик, що виникають внаслідок взаємодії елементів і не зводяться до їхніх окремих властивостей. Наприклад, сучасний літак є складною системою, що об'єднує авіоніку, механічні, енергетичні та інформаційні підсистеми. Інші приклади включають енергетичні станції та телекомунікаційні мережі. Складність таких систем вимагає використання інтегрованих підходів до управління та контролю.

b) Ускладнені технічні системи

Ультраскладні технічні системи вирізняються високим рівнем інтеграції, гетерогенністю та когнітивними можливостями. Вони здатні адаптуватися до змінного середовища завдяки наявності механізмів самонавчання та адаптації. Такі системи функціонують у середовищах з високим рівнем невизначеності та є автономними в прийнятті рішень. Наприклад, автономні транспортні системи використовують штучний інтелект для адаптації до змін дорожньої обстановки. Інші приклади включають хмарні обчислювальні мережі та бойові системи управління. Високий рівень складності потребує розробки спеціалізованих методів аналізу та оптимізації для забезпечення надійності та безпеки.

Таким чином, класифікація технічних систем за ступенем складності дозволяє чітко структурувати підходи до їхнього проектування, управління та експлуатації. Розуміння особливос-

тей кожного класу систем забезпечує вибір адекватних методів контролю та адаптації в умовах сучасного технологічного розвитку.

2) Класифікація за функціональним призначенням

Функціональне призначення технічних систем визначає їхню основну мету та специфічні завдання, які вони виконують у певному середовищі. Така класифікація дозволяє впорядкувати різноманіття технічних рішень відповідно до їх призначення та сфери застосування. Основні категорії технічних систем за функціональним призначенням включають вимірювальні, управлінські, виконавчі, інформаційні та захисні системи.

a) Вимірювальні системи

Вимірювальні системи призначені для збору, обробки та аналізу параметрів середовища. Основу вимірювальних систем складають сенсори, що фіксують фізичні величини (температуру, тиск, швидкість тощо) та передають інформацію на обчислювальні модулі. Сучасні вимірювальні системи часто інтегровані з аналітичними платформами, що дозволяє здійснювати моніторинг в реальному часі. Наприклад, системи моніторингу стану будівельного обладнання дозволяють своєчасно виявляти зношення компонентів. Інші приклади включають геодезичні прилади та автоматизовані метеостанції.

b) Управлінські системи

Управлінські системи виконують функції автоматичного або напівавтоматичного регулювання різних технологічних та виробничих процесів. Основною метою таких систем є підтримання стабільності та оптимізації функціонування об’єкта управління. Наприклад, програмовані логічні контролери (ПЛК) забезпечують контроль над промисловими процесами, тоді як системи SCADA (Supervisory Control and Data Acquisition) здійснюють моніторинг і управління інженерними мережами. Також до управлінських систем можна віднести штучний інтелект, що адаптує алгоритми управління залежно від змінних факторів.

c) Виконавчі системи

Основна функція виконавчих систем полягає у фізичній реалізації команд управління. Це можуть бути роботи, верстати, актуатори та інші механізми, що перетворюють керуючий сигнал у дію. Наприклад, промислові роботи здійснюють складаль-

ні операції на конвеєрі, використовуючи команди з ПЛК. Інші приклади включають автоматизовані виробничі лінії та гідравлічні приводи, що виконують точні механічні операції.

d) Інформаційні системи

Інформаційні системи зосереджені на збереженні, передачі та аналізі даних. Вони забезпечують інформаційну підтримку управлінських рішень та взаємодію між компонентами складних технічних об'єктів. Прикладом є дата-центри, які забезпечують централізоване зберігання та обробку великих обсягів даних. Інформаційно-аналітичні платформи дозволяють аналізувати тренди та прогнозувати показники діяльності, тоді як ERP-системи об'єднують різні аспекти управління підприємством у єдиній базі даних.

e) Захисні системи

Захисні системи забезпечують безпеку об'єктів та користувачів шляхом попередження або локалізації потенційних загроз. Сучасні захисні системи інтегрують апаратні та програмні компоненти для контролю доступу, захисту інформації та моніторингу середовища. Наприклад, протипожежні системи включають датчики диму та системи автоматичного пожежогасіння. Системи відеоспостереження забезпечують візуальний контроль за об'єктами, а кіберзахист запобігає несанкціонованому доступу до критичної інфраструктури.

Класифікація технічних систем за функціональним призначенням дозволяє ефективно організувати підходи до їхнього проектування, розробки та експлуатації. Розуміння призначення кожного типу системи сприяє підвищенню ефективності управління, моніторингу та захисту об'єктів у різних галузях.

3) Класифікація за сферою застосування

Класифікація технічних систем за сферою застосування дозволяє виокремити їх на основі функціонального призначення, галузі використання та специфічних технологічних вимог. Розглянемо основні групи технічних систем залежно від сфери їх застосування:

a) Промислові технічні системи

Ці системи активно використовуються у виробничих процесах, машинобудуванні, хімічній та харчовій промисловості. Основне призначення промислових технічних систем — автомати-

зація та оптимізація виробництва, підвищення ефективності роботи обладнання, зменшення впливу людського фактора.

Приклади: Автоматизовані виробничі лінії — забезпечують безперервність технологічного процесу за допомогою систем керування на основі ПЛК (програмованих логічних контролерів). Системи з числовим програмним управлінням (ЧПУ) — застосовуються в металообробці та механічній обробці для прецизійного керування верстатами. Робототехнічні комплекси — роботи-зварювальники, складальні модулі на конвеєрних лініях.

b) Транспортні технічні системи

Транспортні системи призначені для управління транспортними засобами та інфраструктурою. Вони спрямовані на забезпечення безпеки, оптимізацію маршрутів та підвищення комфорту користувачів.

Приклади: Системи GPS-навігації — використовуються для позиціонування та навігації автомобілів, суден, літаків. *Системи стабілізації та контролю руху* — забезпечують курсову стійкість, адаптивне регулювання швидкості та гальмування (наприклад, ABS у автомобілях). Автопілоти — керують літальними апаратами в автоматичному режимі, забезпечуючи стабільний політ.

c) Енергетичні технічні системи

Ця категорія охоплює системи генерації, передачі та споживання енергії. Вони забезпечують стабільне та ефективне управління енергоресурсами.

Приклади: Smart Grid — інтелектуальні енергетичні мережі, що забезпечують автоматизований розподіл електроенергії. *Трансформаторні підстанції з автоматичним керуванням* — регулюють напругу в енергомережі. *Вітрові та сонячні генератори* — використовують відновлювані джерела енергії з оптимізованими алгоритмами керування.

c) Медичні технічні системи

Використовуються в медичній сфері для діагностики, лікування та моніторингу стану пацієнтів. Такі системи підвищують точність медичних процедур та знижують ризик людських помилок.

Приклади: Комп'ютерна томографія (КТ) та магнітно-резонансна томографія (МРТ) — дозволяють отримувати детальні зображення внутрішніх органів. *Кардіомонітори* — безперервно контролюють серцеву активність. *Біопротези та ім-*

плантовані сенсори — забезпечують моніторинг та управління фізіологічними параметрами.

е) Військові технічні системи

Забезпечують безпеку та оборону, використовуючи передові технології для збору, обробки та аналізу даних у реальному часі.

Приклади: Безпілотні літальні апарати (дрони) — проводять розвідку та бойові дії. *Системи протиповітряної оборони (ППО)* — відстежують повітряні цілі та координують перехоплення. *Радіоелектронна боротьба (РЕБ)* — придушення сигналів супротивника.

f) Будівельні технічні системи

Спрямовані на забезпечення безпеки будівельних об'єктів та автоматизацію інфраструктурних процесів.

Приклади: Автоматизовані системи контролю конструкцій — моніторинг вібрацій та деформацій у реальному часі. *«Розумні» будинки* — комплексні системи управління енергоспоживанням, безпекою та комфортом. *Протисейсмічний моніторинг* — виявлення коливань ґрунту та адаптація конструкцій.

g) Космічні технічні системи

Використовуються для управління космічними апаратами, збору даних та забезпечення життєдіяльності у космосі.

Приклади: Навігаційні супутники — забезпечують глобальне позиціонування. *Системи життєзабезпечення* — підтримка кисневого балансу на орбітальних станціях. *Телеметричні платформи* — збір та передача даних про стан космічного апарата.

h) Побутові технічні системи

Забезпечують комфорт та автоматизацію домашніх процесів, використовуючи технології Інтернету речей (IoT).

Приклади: «Розумна» техніка — пральні машини та холодильники з можливістю віддаленого керування. *Персональні гаджети* – фітнес-трекери, смарт-годинники. *Голосові асистенти* — системи управління голосом, що інтегруються з домашніми пристроями.

Класифікація технічних систем за сферою застосування дозволяє структурувати різноманітні технології на основі їх цільового використання. Це сприяє ефективному вибору та інтеграції систем в різні галузі, забезпечуючи комплексний підхід до вирішення технологічних завдань.

4) Класифікація за типом керування

– ручні — керуються людиною в повному обсязі.

– напівавтоматичні — мають автоматизовані частини, але потребують участі людини.

– автоматичні — працюють за алгоритмом без втручання оператора, але без можливості самонавчання.

– автономні — мають елементи штучного інтелекту, здатні самостійно приймати рішення на основі аналізу середовища.

5) Класифікація за ступенем відкритості

– Закриті системи — мають мінімальні зв'язки із зовнішнім середовищем, працюють за жорстко визначеними алгоритмами;

– Відкриті системи — активно обмінюються інформацією, енергією, матеріалами з оточенням, здатні адаптуватися.

6) Інтегративна класифікація

У сучасному світі технічний прогрес та глобалізація технологій призвели до появи складних систем, що поєднують функції з різних галузей. Такі системи отримали назву *інтегративних технічних систем***.** Їх особливістю є мультифункціональність, здатність адаптуватися до різноманітних умов експлуатації та високий рівень взаємодії компонентів.

Інтегративна класифікація технічних систем дозволяє враховувати складність сучасних технологій та їх мультифункціональність. В умовах цифрової трансформації та розвитку концепцій на кшталт Індустрії 4.0 стає актуальним об'єднання різних систем в єдині комплексні рішення. Це сприяє підвищенню ефективності та надійності технічних процесів, створюючи нові можливості для їх впровадження у різних галузях.

Наприклад Автономний електромобіль Tesla — це транспортна, інформаційна, когнітивна, відкрито-адаптивна система з елементами штучного інтелекту та медичний імплантат з біодатчиками — біотехнічна, сенсорна, частково автономна система з високими вимогами до безпеки й надійності.

7) Проблеми та виклики класифікації

Класифікація технічних систем не є сталою. З появою нових технологій (нейромережі, квантові обчислення, біоінтерфейси, метавсесвітні структури) виникає потреба перегляду класифікаційної логіки що включає до себе гібридизація функцій унеможливлює однозначне віднесення до однієї категорії, також поява

когнітивних властивостей ставить під сумнів розмежування «технічна – біологічна» система, і технологічна сингулярність потребує створення нових класифікацій з акцентом на поведінкові й етичні характеристики.

Таким чином, класифікація технічних систем повинна розглядатися як динамічний процес, що постійно уточнюється з урахуванням техноеволюційних змін, цифрової трансформації та нових вимог до безпеки, сталості й гуманізації техніки.

1.1.5. Тенденції розвитку технічних систем у XXI столітті

У XXI столітті технічні системи зазнають глибоких трансформацій під впливом таких мегатрендів, як цифровізація, глобалізація, урбанізація, сталий розвиток, мініатюризація, розвиток штучного інтелекту та зростання ролі даних. Сучасна техніка стає дедалі більш автономною, інтелектуальною, взаємопов'язаною й адаптивною [30, с. 36]. У цьому контексті важливо не лише відстежувати зміни, а й осмислювати загальні напрямки еволюції технічних систем, щоб забезпечити відповідність майбутнім викликам.

1) Кіберфізичні системи (CPS)

Одним з фундаментальних напрямів розвитку є **кіберфізичні системи**, які об'єднують цифрові обчислювальні процеси з фізичними об'єктами через сенсори, виконавчі механізми й мережеві технології. Вони є основою для таких концептів, як Індустрія 4.0, Інтернет речей (IoT), «розумні» міста та автономні виробництва.

Основні риси CPS включає до себе постійний обмін даними в реальному часі та автоматична адаптація до змін у середовищі. Можливість самодіагностики, прогнозування відмов і віддаленого керування та висока чутливість до загроз інформаційної безпеки.

Прикладом є автономні транспортні системи, які інтегрують GPS, сенсори руху, LIDAR, штучний інтелект і хмарні сервіси для аналізу дорожньої обстановки.

2) Інтелектуалізація та когнітивність систем

Завдяки розвитку штучного інтелекту (ШІ), технічні системи переходять від реактивної поведінки до когнітивної, тобто здатної аналізувати ситуації та виявляти закономірності; приймати

рішення в умовах невизначеності; навчатися з досвіду (машинне навчання); взаємодіяти з користувачем на основі мовних, візуальних, емоційних інтерфейсів.

Інтелектуалізація сприяє появі систем-помічників (наприклад, голосових асистентів), розумної автоматизації виробництва (predictive maintenance), когнітивних роботів, військових автономних платформ із навігаційним самонавчанням.

3) Технологічна конвергенція: мехатроніка, біотехніка, нанотехнології

Розвиток сучасних технологій та наукових досліджень все частіше призводить до виникнення гібридних технічних систем, що поєднують елементи з різних наукових галузей. На стику таких дисциплін, як механіка, електроніка, біологія, хімія та інформатика, формуються інноваційні рішення, здатні взаємодіяти з оточуючим середовищем на фізіологічному, молекулярному або когнітивному рівнях. Розглянемо ключові напрями розвитку таких гібридних систем.

Мехатроніка є міждисциплінарною галуззю, що об'єднує механіку, електроніку, інформаційні технології та керування. Основна мета мехатроніки — створення інтелектуальних систем, що здатні адаптуватися до змінних умов роботи та забезпечувати високу точність керування. Яскравим прикладом є роботизовані маніпулятори та автоматизовані виробничі лінії, які завдяки інтеграції механічних компонентів з електронними системами забезпечують автономну діяльність.

Біонічні системи ґрунтуються на принципах біоміметики та застосовують природні процеси для створення технічних рішень. Одним із прикладів є екзоскелети для реабілітації, що імітують рухи людини, або біоінспіровані сенсори, що копіюють здатність тварин до виявлення змін у середовищі. Завдяки біонічним системам можливе створення більш ефективних адаптивних пристроїв.

Нанотехнології дозволяють створювати технічні системи на рівні атомів і молекул, що забезпечує унікальні властивості матеріалів та нові функціональні можливості. Одним із перспективних напрямів є нанороботи в медицині, здатні доставляти лікарські препарати безпосередньо до уражених клітин. Крім того,

нанотехнології відіграють важливу роль у розробці сенсорних систем для контролю навколишнього середовища.

Нейроінтерфейси, або системи мозок-комп'ютер (BCI), забезпечують прямий зв'язок між мозком людини та технічними пристроями. Завдяки таким системам можливо керувати пристроями силою думки або відновлювати втрачені функції організму. Наприклад, використання нейроінтерфейсів у протезуванні дозволяє людям з інвалідністю здійснювати точні рухи штучними кінцівками.

Об'єднання різних наукових напрямів у межах гібридних технічних систем дозволяє створювати нові класи пристроїв, що функціонують на фізіологічному, молекулярному та когнітивному рівнях. Такі системи мають великий потенціал для застосування в медицині, промисловості, біоінженерії та багатьох інших сферах, забезпечуючи новий рівень адаптивності та інтелектуальної взаємодії з навколишнім світом.

4) Перехід до децентралізованих і самоорганізованих систем

Завдяки блокчейн-технологіям, peer-to-peer-протоколам, безсерверним архітектурам відбувається перехід від централізованих систем до децентралізованих, а саме: Мережі без єдиного центру управління та автономні пристрої, які приймають колективні рішення. Також DAO (децентралізовані автономні організації), де учасники системи визначають політику взаємодії.

Це особливо актуально для індустрій з високими вимогами до прозорості, довіри, стійкості до збоїв (фінтех, логістика, енергетика).

5) Орієнтація на сталий розвиток і енергоефективність

Технічні системи проектуються з урахуванням вимог екологічної сталості що включає до себе використання енергоефективних компонентів та можливість багаторазового використання, апгрейду, утилізації. Також переорієнтація на відновлювані джерела енергії та мінімізація вуглецевого сліду через цифрове моделювання (digital twin) і оптимізацію життєвого циклу.

Впровадження «зелених» технологій спостерігається у будівництві, транспорті, промисловості, логістиці.

6) Безпека як домінантна характеристика

Зі зростанням взаємопов'язаності зростають і ризики — кібератаки, фізичні збої, маніпуляція даними, втручання у автономні алгоритми. Тому технічні системи XXI століття мають враховувати, а саме: вбудовану безпеку на рівні архітектури (Security by

Design); захист від Zero-Day вразливостей; стійкість до атак на ШІ-алгоритми (adversarial attacks); відповідність регламентам, як-от GDPR, ISO/IEC 27001, NIS2.

Паралельно розвиваються системи цифрової етики, де враховуються етичні наслідки автономного прийняття рішень (наприклад, в самокерованих автомобілях або медичних системах).

7) Еволюція інтерфейсів: XR, HCI, віртуальні та доповнені середовища

Інтерфейс взаємодії між людиною та технічною системою еволюціонує від звичайного функціонального елемента до повноцінної просторово-сенсорної системи, яка не лише забезпечує обмін інформацією, але й створює новий рівень занурення та взаємодії. Сучасні технології активно використовують можливості віртуальної, доповненої та розширеної реальності, а також інноваційні інтерфейси типу HCI та HRI для побудови більш інтегрованих, адаптивних та чутливих до людських потреб систем.

8) Віртуальна реальність (VR)

Віртуальна реальність створює повністю штучне цифрове середовище, що дозволяє моделювати технічні процеси, проводити навчання та тестування в безпечних умовах. Наприклад, у промисловості VR використовується для тренажерів, що дозволяють операторам опановувати складні технологічні операції без ризику пошкодження обладнання або загрози безпеці. Цифрові лабораторії на базі VR дають змогу моделювати експерименти з точним відтворенням умов, які важко або неможливо створити в реальному житті. Завдяки цьому VR стає критично важливим у підготовці фахівців з експлуатації складних технічних систем.

9) Доповнена реальність (AR)

Доповнена реальність забезпечує поєднання реального світу з цифровими елементами, що дозволяє суттєво підвищити ефективність взаємодії з технічними системами. Наприклад, в умовах виробництва AR-системи використовуються для навігації у складних просторових структурах, надаючи працівникам візуальні інструкції безпосередньо на екрані окулярів або мобільного пристрою. Під час монтажу або обслуговування обладнання

фахівці можуть отримувати покрокові рекомендації, що виводяться на дисплей у режимі реального часу. Таким чином, AR не лише оптимізує робочий процес, але й мінімізує ризики помилок.

10) Розширена реальність (XR)

Розширена реальність представляє собою більш комплексне рішення, що об'єднує можливості VR, AR та змішаної реальності (MR). Основна мета XR — створення середовища, де фізичні та цифрові компоненти функціонують як єдина система. Наприклад, у сфері технічного обслуговування XR дозволяє виводити 3D-моделі складних механізмів безпосередньо на реальні об'єкти, що сприяє підвищенню точності операцій. Крім того, завдяки повній інтеграції фізичного та цифрового середовища XR сприяє створенню більш інтуїтивних та природних інтерфейсів взаємодії.

11) Інтерфейси взаємодії людини з комп'ютером (HCI)

Human-Computer Interaction (HCI) спрямований на створення зручних інтерфейсів, що враховують когнітивні та фізіологічні особливості користувача. Сучасні HCI-системи включають дотикові інтерфейси, що дозволяють керувати обладнанням за допомогою жестів або натискань, голосові команди, які суттєво спрощують контроль у динамічних середовищах, а також нейроінтерфейси, що дозволяють здійснювати контроль на основі мозкової активності. Завдяки поєднанню таких технологій HCI розширює можливості адаптації технічних систем до індивідуальних потреб користувачів.

12) Інтерфейси взаємодії людини з роботами (HRI)

Human-Robot Interaction (HRI) формує нову парадигму співпраці людини з роботами, створюючи симбіотичні системи з емоційним та сенсорним зворотним зв'язком. Наприклад, сучасні роботи оснащуються сенсорами для розпізнавання емоцій людини та зоровими системами для оцінки жестів. Крім того, HRI передбачає моторний зворотний зв'язок, що дозволяє роботам взаємодіяти з об'єктами з високою точністю, адаптуючи свої дії до непередбачуваних змін у навколишньому середовищі. Така інтеграція створює умови для більш гармонійної взаємодії в умовах промислових, логістичних та побутових завдань.

Таким чином, сучасний інтерфейс взаємодії між людиною та технічною системою не просто забезпечує передачу команд, а перетворюється на динамічний комунікативний простір, що адаптується до потреб користувача. Інтеграція технологій VR, AR, XR, а також інтерфейсів HCI та HRI створює нову якість у взаємодії з технічними системами, дозволяючи досягти вищого рівня безпеки, продуктивності та ефективності.

13) Прогноз на майбутнє: від технічних до техно-соціальних систем

У перспективі ми спостерігатимемо подальше розмиття межі між технічними й соціальними системами. З'являтимуться гуманізовані системи — з урахуванням емоцій, мови, індивідуального досвіду користувача; колективні технічні системи — дрони, роботи, сенсори, що функціонують у роях; морально-орієнтовані системи — здатні оцінювати дії за етичними критеріями; метасистеми — об'єднання кількох систем у єдиний функціональний кластер зі здатністю до саморефлексії (meta-learning).

1.2. Загрози безпеці технічних систем: природа, джерела та класифікація.

1.2.1. Загальні засади аналізу загроз у технічних системах

Загрози безпеці технічних систем становлять один із ключових предметів дослідження сучасної інженерії безпеки, інформаційної безпеки та системного аналізу. Вони являють собою сукупність реальних або потенційних впливів, які здатні завдати шкоди цілісності, доступності, конфіденційності, стійкості або функціональній ефективності технічної системи [29, с. 106]. У широкому значенні загроза — це обставина або подія, що має потенціал порушити нормальне функціонування системи або викликати збій у її структурно-функціональній архітектурі [53, с. 6].

Слід розрізняти такі споріднені поняття, як ризик, вразливість і інцидент. Якщо загроза є можливістю негативного впливу, то ризик – це міра ймовірності реалізації цієї загрози в поєднанні з оцінкою шкоди. Вразливість — це слабке місце в систе-

мі, через яке загроза може бути реалізована. Інцидент — вже реалізована загроза [45, с. 112].

З урахуванням трансформацій, які зазнають сучасні технічні системи — зокрема, переходу до кіберфізичних систем (Cyber-Physical Systems), розгалужених IoT-структур (Internet of Things) та інтелектуальних технологій — питання ідентифікації та класифікації загроз набуває все більш складного міждисциплінарного характеру. Воно потребує залучення знань з галузей прикладної математики, інформатики, когнітивних наук, технічної кібернетики, соціальної інженерії та права.

1.2.2. Класифікація джерел загроз технічним системам

Ефективне управління безпекою технічної системи вимагає системного підходу до класифікації загроз, що дає змогу не лише своєчасно ідентифікувати потенційні ризики, а й точно моделювати їх можливі варіанти виникнення та оцінювати їх вплив на функціонування системи. Сучасні методи класифікації загроз базуються на багатофакторному підході, який дозволяє створювати більш детальні та адаптивні стратегії захисту, враховуючи різноманітні аспекти, від джерел загроз до їхнього характеру та впливу на систему [55, с. 1-3]. Аналіз джерел загроз є важливим етапом у забезпеченні безпеки технічних систем. Він включає виявлення носіїв потенційного шкідливого впливу на систему, що може призвести до її порушення або знищення. Класифікація джерел загроз становить досить складну систему.

1) Класифікація джерел загроз за резидентністю.

Резидентність визначає: знаходяться джерела загроз в середині системи або поза її межами.

а) Зовнішні джерела загроз

Зовнішні джерела загроз становлять найбільшу частину непередбачуваних ризиків, оскільки вони можуть виникати поза межами організації або системи. Такі загрози зазвичай не піддаються прямому контролю, що ускладнює їх прогнозування і зниження ризиків. До зовнішніх джерел відносяться:

– *Стихійні лиха.* Природні катастрофи, такі як повені, землетруси, урагани, торнадо, можуть викликати серйозні порушення в роботі технічних систем і інфраструктури. Вони часто

призводять до фізичного пошкодження обладнання, відключень енергозабезпечення та порушення комунікацій.

– *Зміни кліматичних умов*. Зміни в кліматі можуть також становити загрозу для функціонування технічних систем, особливо для таких інфраструктурних елементів, як енергетичні мережі, системи охолодження, транспортні мережі. Неочікувані погодні умови, такі як сильні зливи чи температурні аномалії, можуть вивести з ладу критичні елементи систем.

– *Вплив суміжної інфраструктури*. Збої в одній частині інфраструктури, наприклад, в енергетичній мережі або водопостачанні, можуть спричинити порушення в роботі інших систем, зокрема IT-структур. Наприклад, перебої в електропостачанні можуть викликати відмови в серверах або спотворення даних, що знижує ефективність функціонування всіх залежних систем.

– *Цілеспрямовані зовнішні атаки.* Це можуть бути атаки хакерських угруповань, кіберзлочинців, конкурентів або навіть урядових структур, що мають на меті викрасти або знищити інформацію, порушити нормальне функціонування системи або отримати доступ до чутливої інформації. Ці атаки можуть мати різну форму — від DDoS-атак до складних хакерських вторгнень.

Зовнішні джерела є менш контрольованими, їх важко передбачити, і для їх виявлення необхідні складні моделі аномалій та багаторівневий моніторинг, що дозволяє швидко реагувати на непередбачувані загрози.

b) Внутрішні джерела загроз

Внутрішні джерела загроз виникають безпосередньо в середині організації або технічної системи. Це можуть бути загрози, викликані людським фактором, технічними проблемами або помилками в управлінні системами. Внутрішні загрози часто є більш важкими для виявлення, оскільки вони можуть розвиватися поступово і мати прихований характер. До внутрішніх джерел загроз відносяться:

– *Помилки адміністраторів*. Необережність або недосвідченість адміністраторів можуть призвести до серйозних проблем безпеки, таких як неправильні налаштування мережі, некоректне управління доступами або навіть випадкові помилки, що спричиняють порушення роботи систем.

– *Несумлінність персоналу*. Загроза з боку працівників, які навмисно або через недбалість сприяють проникненню зловмисників у систему, також є серйозною проблемою. Наприклад, співробітники можуть використовувати слабкі паролі, передавати чутливу інформацію або підключати несанкціоноване обладнання.

– *Втрати доступу до облікових даних*. Внутрішні загрози часто пов'язані з втратою доступу до важливих облікових даних, які використовуються для доступу до ресурсів і баз даних системи. Це може статися через несанкціоновану передачу паролів або неправомірний доступ до облікових записів.

– *Несанкціоноване підключення обладнання.* Підключення сторонніх пристроїв (наприклад, USB-флешок, персональних комп'ютерів або мобільних пристроїв) до корпоративної мережі без відповідного контролю може призвести до зараження системи шкідливим програмним забезпеченням або витоку даних.

– *Використання застарілого ПЗ.* Системи, що не отримують регулярних оновлень, стають вразливими до атак. Використання застарілих версій програмного забезпечення може стати серйозною проблемою для організації, адже на таких системах можуть бути відомі вразливості, які легко використовуються зловмисниками.

За статистикою, понад 60% серйозних інцидентів з безпекою трапляються через внутрішні джерела загроз. Причиною цього є недостатнє усвідомлення загроз з боку співробітників, недотримання політик безпеки або недоліки в управлінні доступами.

c) Гібридні джерела загроз

Гібридні джерела загроз є особливо складними для виявлення і управління, оскільки поєднують елементи як зовнішніх, так і внутрішніх загроз. Вони можуть бути результатом зовнішнього нападу, який реалізується з використанням внутрішніх вразливостей або співробітників організації. Це може бути:

– *Атака ззовні з участю внутрішніх осіб*. Наприклад, хакер може ініціювати атаку на систему, використовуючи внутрішнього співробітника для доставки шкідливого програмного забезпечення або доступу до облікових даних. В цьому випадку важко розмежувати, де закінчується зовнішня загроза і де починається внутрішня.

– *Заражені пристрої*. Зовнішні пристрої, такі як мобільні телефони або флешки, можуть бути заражені шкідливим програмним забезпеченням і, підключаючись до внутрішніх систем, спричиняти серйозні порушення безпеки.

– *Зловмисне використання довірених осіб*. Зловмисники можуть використати легітимного працівника або підрядника для проведення атаки або для отримання доступу до конфіденційної інформації, що створює додаткові складнощі в боротьбі з кіберзагрозами.

Управління гібридними загрозами потребує високого рівня аналітики та багаторівневого захисту, оскільки такі загрози можуть бути масковані та важко виявлені.

Таким чином, аналіз джерел загроз передбачає комплексний підхід до виявлення потенційних ризиків і загроз у системі, враховуючи як зовнішні, так і внутрішні фактори. Кожна категорія загроз вимагає специфічних методів моніторингу, прогнозування та впровадження заходів безпеки для забезпечення надійного захисту технічних систем.

2) Класифікація джерел загроз за джерелом виникнення.

a) Природні загрози — це явища, які не залежать від людської діяльності і можуть включати природні катастрофи, такі як землетруси, бурі, повені або інші екстремальні кліматичні умови. Характеризуються непередбачуваністю та величезними наслідками, що можуть впливати на фізичні компоненти технічної системи та зупиняти її роботу. Природні загрози охоплюють стихійні явища, що можуть безпосередньо або опосередковано впливати на технічні системи. До цього типу загроз належать землетруси, повені, шторми, блискавки, лісові пожежі та інші природні катастрофи. Такі загрози часто розглядаються як форс-мажорні події, проте сучасна інженерія безпеки передбачає врахування цих ризиків на етапі проектування систем. Для цього застосовуються методи сценарного аналізу та моделювання динаміки навколишнього середовища, що дозволяють прогнозувати наслідки впливу природних факторів на технічні об'єкти.

b) Антропогенні загрози виникають через людську діяльність і часто пов'язані з помилками або недбалістю. Це може бути несанкціонований доступ до системи, неправильне її налаштування або неконтрольоване використання ресурсів, а також акт

саботажу, коли порушуються правила безпеки навмисно, з метою шкоди. Антропогенні загрози пов’язані з людським фактором, що включає як ненавмисні помилки операторів або обслуговуючого персоналу, так і свідомі дії зловмисників. Людський фактор особливо впливає на надійність складних соціотехнічних систем, де прийняття рішень залежить від компетентності персоналу. Прикладами антропогенних загроз є порушення норм експлуатації, несанкціонований доступ до обладнання, саботаж або неуважність під час критичних операцій.

c) Техногенні загрози виникають з причин, обумовлених внутрішніми характеристиками технічних систем, такими як їх зношення, перегрів, несправності або інші проблеми, пов'язані з експлуатацією обладнання. Вони часто є наслідком недостатнього технічного обслуговування або недоліків проектування. Техногенні загрози виникають у результаті технічних або експлуатаційних помилок, зносу компонентів системи, відмов технічного обладнання або недотримання регламенту технічного обслуговування. Ризик техногенних загроз зростає у складних технологічних системах, що мають високу залежність від безперебійної роботи ключових компонентів. Зокрема, комбінація техногенних та природних факторів може спричинити каскадні відмови. Наприклад, вібраційне навантаження під час землетрусу може призвести до масових збоїв у роботі енергомереж або промислових комплексів.

d) Інформаційні загрози фокусуються на впливі на дані та IT-середовище, що включає віруси, шифрувальники, хакерські атаки, а також інші загрози, пов'язані з інформаційною безпекою. Ці загрози можуть серйозно порушити функціонування програмного забезпечення, а також призвести до витоку або модифікації важливих даних. Цей клас загроз виникає через інтенсивну цифровізацію технічних систем та їх інтеграцію з інформаційно-комунікаційними мережами. Основні ризики включають кібератаки, зловмисне втручання, маніпуляцію даними, DDoS-атаки, шкідливе програмне забезпечення та соціальну інженерію. Зокрема, компрометація систем промислового управління (SCADA) може призвести до руйнування об’єктів інфраструктури або збоїв у критично важливих процесах. Стратегія забезпечення кібербезпеки передбачає багаторівневий захист, включаючи

моніторинг, ідентифікацію вразливостей та миттєве реагування на інциденти.

Урахування природи загроз на етапі проектування технічних систем є важливою умовою забезпечення надійності та безпеки їх функціонування. Комплексний підхід до безпеки передбачає аналіз кожної категорії загроз та впровадження адекватних заходів захисту на основі передбачення можливих ризиків та оптимізації захисних механізмів.

3) Класифікація джерел загроз за характером впливу:

a) Активні загрози спрямовані на зміну фізичного або логічного стану технічної системи. Це можуть бути атаки, спрямовані на фізичні компоненти (наприклад, перегрів або зношення) або впливи на програмне забезпечення через вразливості, що дозволяють змінювати налаштування або функціональність системи.

b) Пасивні загрози зазвичай не змінюють стану системи безпосередньо, але мають на меті отримати конфіденційну інформацію. Це можуть бути різноманітні форми шпигунства або несанкціоноване спостереження, що дозволяє зібрати дані без виявлення втручання в систему.

***4) Класифікація джерел загроз за* ступенем передбачуваності:**

a) Неочікувані загрози (чорні лебеді) — це події, які малоймовірні, але мають величезний вплив на систему в разі їх реалізації. Через свою рідкість і високі наслідки вони є найбільш складними для прогнозування та запобігання. Для таких загроз необхідно розробляти гнучкі та універсальні механізми реагування.

b) Очікувані загрози. Без коментарів

***5) Класифікація джерел загроз за* рівнем проникнення:**

a) Фізичні загрози — це загрози, які впливають на матеріальні компоненти технічної системи. Вони можуть бути як зовнішніми (наприклад, пошкодження обладнання внаслідок стихійного лиха), так і внутрішніми (внаслідок зношення або дефектів апаратного забезпечення).

b) Логічні загрози реалізуються через програмне забезпечення, мережі та системи управління. Ці загрози часто пов'язані з

вразливостями в коді або в налаштуваннях мережевих протоколів, які можуть дозволити несанкціонований доступ або зміну налаштувань системи.

с) Організаційні загрози пов'язані з внутрішніми змінами в організації, зокрема з перерозподілом ролей, зміною політик доступу чи управлінських структур. Вони можуть виникнути, коли в організації відбуваються зміни, що не враховують безпеку інформаційних систем, що створює нові вразливості.

Ця багатофакторна класифікація загроз дозволяє не лише системно аналізувати ризики для технічної системи, але й створювати адаптивні стратегії захисту, орієнтуючись на різноманітні аспекти й можливі сценарії розвитку подій.

1.2.3. Методи і моделі аналізу та оцінки загроз

Для забезпечення належного рівня безпеки технічної системи необхідно не лише класифікувати загрози, а й оцінювати їх у контексті ризику, впливу, імовірності реалізації та варіантів протидії. Сучасна практика передбачає використання як детермінованих, так і імовірнісно-статистичних, експертних і інтелектуальних методів аналізу загроз [44, с. 214].

1) Метод дерева відмов (FTA – Fault Tree Analysis)

Застосовується для виявлення можливих причин відмов системи. Дає змогу побудувати ієрархічну модель, де кожна подія пов’язана з логічними операціями AND/OR, що дозволяє визначити слабкі місця у структурі. Особливо ефективна в галузях критичної інфраструктури (енергетика, транспорт).

2) Аналіз видів та наслідків відмов (FMEA – Failure Modes and Effects Analysis)

Цей метод орієнтований на превентивний аналіз функціональних блоків системи для виявлення потенційних точок відмов. Кожен потенційний збій оцінюється за трьома критеріями: імовірність, важливість і виявленість, після чого розраховується пріоритет ризику (RPN).

3) SWOT-аналіз у контексті кібербезпеки

Хоча класичний SWOT застосовується в менеджменті, він використовується також для стратегічного аналізу безпеки систем: сильні сторони (S), слабкості (W), можливості (O), загрози (T) до-

зволяють визначити стратегічні напрямки підвищення кіберстійкості.

4) Метод сценарного моделювання

Застосовується для прогнозування впливу загроз за умов невизначеності. Створюються сценарії на основі факторного аналізу: наприклад, «масова DDoS-атака + людський фактор = втрати даних». Це дозволяє виявити нелінійні ефекти, що виникають від комбінацій загроз.

5) Байєсівський підхід до оцінки ризиків

Методи байєсівських мереж довіри (Bayesian Belief Networks) дозволяють враховувати невизначеність і залежності між подіями. Ефективні в системах з високим рівнем складності, де неможливо побудувати повну детерміновану модель.

6) Машинне навчання та інтелектуальні системи

Сучасні технічні системи дедалі частіше інтегрують методи штучного інтелекту для виявлення аномалій, побудови моделей поведінки користувачів, оцінки кіберзагроз у реальному часі. Використовуються алгоритми кластеризації, дерев рішень, нейромережі, глибоке навчання.

7) Моделі оцінки вразливості

Існують стандартизовані підходи до оцінювання вразливостей – наприклад, CVSS (Common Vulnerability Scoring System), яка дозволяє класифікувати ризики за шкалою від 0 до 10 та описувати рівень впливу (низький, середній, критичний).

1.2.4. Комплексна аналітична модель управління загрозами.

На сучасному етапі розвитку безпекових технологій, з огляду на зростаючу складність та масштаб загроз, особливо в умовах постійної еволюції кіберзагроз та технологій, критично важливим є формування багаторівневої моделі управління загрозами [28, с. 99]. Така модель охоплює повний цикл від збору даних до оцінки ефективності заходів реагування, що дозволяє забезпечити належний рівень захисту технічних систем та своєчасну реакцію на загрози [40, с. 168]. Ключовими етапами цієї моделі є моніторинг, ідентифікація, оцінка, аналіз впливу, пріоритезація, реагування та ретроспектива [17, с. 80].

1) Моніторинг є першим етапом, на якому здійснюється постійний збір даних із різноманітних джерел, таких як сенсори, журнали (логи), канали зв'язку та інші інформаційні потоки. Це дозволяє отримувати цілісну картину стану технічної системи в реальному часі. Сенсори можуть фіксувати різноманітні параметри, включаючи зміну температури, навантаження на компоненти, аномальні мережеві запити або несанкціоновані спроби доступу. Логи дозволяють виявляти не лише критичні події, але й менші аномалії, що можуть вказувати на потенційну загрозу.

2) Ідентифікація передбачає виявлення аномалій та потенційних загроз. Цей етап може бути автоматизованим за допомогою систем, які використовують алгоритми на основі машинного навчання (ML) або статистичних методів, або ж здійснюватися вручну спеціалістами з безпеки. У автоматичному режимі ідентифікація аномалій базується на порівнянні поточних даних з нормою або історичними трендами. Це дозволяє оперативно виявляти невідповідності, які можуть свідчити про вторгнення, спроби маніпуляції з даними чи технічні неполадки.

3) Оцінка загроз є важливим етапом у визначенні рівня їх серйозності та потенційного впливу на систему. Для цього використовуються різноманітні моделі оцінювання, такі як *FTA (Fault Tree Analysis)**,** FMEA (Failure Mode and Effects Analysis)**,** CVSS (Common Vulnerability Scoring System)* ***та*** *машинне навчання (ML-алгоритми)**.*** Кожен з цих підходів дозволяє систематично оцінювати ймовірність та наслідки виникнення певних загроз. Наприклад, FTA дозволяє визначити найвірогідніші ланки поломки в системі, а CVSS оцінює вразливості за шкалою від 0 до 10, що дозволяє чітко визначити, які загрози є критичними і потребують негайного реагування.

4) Аналіз впливу фокусується на прогнозуванні можливих наслідків реалізації загрози для технічної системи. Він передбачає оцінку шкоди, яку загроза може завдати на основі її характеру, потенційної масштабу впливу та ймовірності. Це дозволяє вчасно зрозуміти, які елементи системи будуть найбільше вразливими і на які аспекти слід звернути увагу при формуванні заходів безпеки.

5) Пріоритезація загроз дозволяє визначити, які з них є найбільш критичними для безпеки системи. Цей етап включає ран-

жування загроз за ступенем їх критичності, що дає можливість визначити пріоритетні напрями для реакції та витрати ресурсів. За допомогою цієї процедури система безпеки може оптимізувати свої ресурси для нейтралізації найбільш небезпечних загроз.

6) Реагування на загрози є завершальним етапом, який включає запуск відповідних протоколів ліквідації або нейтралізації загрози. Це може включати автоматичне блокування доступу, активацію процедур відновлення системи або інші методи захисту. Для цього використовуються заздалегідь розроблені плани та алгоритми, які дозволяють оперативно реагувати на інциденти та мінімізувати їхні наслідки.

7) Ретроспектива — це процес аудиту та формування політик для попередження подібних загроз у майбутньому. Після кожного інциденту важливо здійснити детальний аналіз ідентифікованих загроз і реакцій на них, а також вдосконалити заходи захисту на основі отриманих знань. Це дозволяє забезпечити більш ефективну готовність до майбутніх атак та знизити ймовірність виникнення подібних загроз у майбутньому.

Таку багаторівневу модель управління загрозами реалізують сучасні технологічні рішення, зокрема *SIEM-системи* (Security Information and Event Management) та *SOAR-платформи* (Security Orchestration, Automation and Response), які стали основою для побудови кіберзахисту в складних технічних системах. SIEM-системи займаються централізованим збором і аналізом даних про безпеку, автоматично виявляючи та корелюючи загрози, тоді як SOAR-платформи забезпечують автоматизацію процесів реагування, оркеструючи дії між різними компонентами системи та координуючи швидку та ефективну відповідь на інциденти. Завдяки інтеграції цих технологій створюється гнучка та динамічна інфраструктура кіберзахисту, здатна швидко реагувати на нові загрози та адаптуватися до змін в кіберсередовищі.

1.3. Основні принципи забезпечення технічної безпеки.

1.3.1. Сутність технічної безпеки та її стратегічна важливість

У контексті сучасної техносфери технічна безпека постає як фундаментальна передумова стабільного функціонування соціально-економічних, інформаційних, енергетичних та інфраструктурних систем . Під технічною безпекою розуміють сукупність заходів, дій, нормативно-технологічних рішень та організаційних підходів, спрямованих на запобігання, виявлення та нейтралізацію загроз, що виникають унаслідок експлуатації або впливу технічних систем, пристроїв та процесів. Цей підхід базується на інтеграції знань з галузей інженерії, системного аналізу, кібербезпеки, надійності, а також управління ризиками [20, с. 18].

Сучасна парадигма технічної безпеки передбачає багаторівневий підхід, у якому ключовими виступають як фізичні, так і інформаційні аспекти. Це зумовлено широким застосуванням кіберфізичних систем, Інтернету речей (IoT), систем автоматизації та роботизованих платформ, які формують нову архітектуру ризиків [37, с. 24]. Відтак технічна безпека є не лише інженерною проблемою, а й соціотехнічною категорією, що охоплює взаємодію людини, машини та навколишнього середовища.

1.3.2. Методологічні основи принципів технічної безпеки

Забезпечення технічної безпеки є ключовим аспектом управління сучасними інфраструктурами, де надійний захист від загроз залежить від низки методологічних принципів, що розроблені на перетині інженерії безпеки, системного аналізу та управління якістю [26, с. 16]. Ці принципи дозволяють формалізувати підхід до виявлення, оцінювання та мінімізації потенційних загроз, створюючи основу для побудови ефективних систем технічного захисту. Вони передбачають цілісний підхід, орієнтований на комплексне врахування всіх можливих факторів, що можуть впливати на безпеку об'єкта [49, с. 392].

Основні методологічні опори для забезпечення технічної безпеки включають такі принципи:

1) Системність є одним із основних принципів, що передбачає цілісне бачення технічного об'єкта як частини складної динамі-

чної системи. Це означає, що для забезпечення безпеки необхідно враховувати не лише окремі елементи або компоненти, але й їх взаємодію, взаємозалежність та вплив на загальний стан системи. У межах системного підходу розглядаються не лише технічні, а й організаційні аспекти безпеки, враховуються усі можливі зв'язки між елементами системи, а також вплив зовнішнього середовища. Такий підхід дозволяє виявляти потенційні слабкі місця на ранніх етапах та вчасно реагувати на зміну умов експлуатації.

2) Превентивність — це принцип, що акцентує увагу на випереджальному виявленні потенційно небезпечних чинників до того, як вони можуть призвести до негативних наслідків. Це включає в себе реалізацію заходів, спрямованих на попередження загроз ще на етапах проектування, розробки чи навіть під час нормальної експлуатації систем. Превентивний підхід дозволяє знизити ймовірність виникнення інцидентів безпеки шляхом регулярних моніторингів, оцінки ризиків, проведення аудитів та використання інструментів для виявлення вразливих місць. Він сприяє створенню адаптивних механізмів, здатних оперативно реагувати на зміни у зовнішніх умовах чи технологічному середовищі.

3) Адаптивність — принцип, що виражається в здатності систем безпеки пристосовуватись до зміни зовнішніх умов. Технічні системи безпеки повинні бути здатні до швидкої модифікації та оновлення у відповідь на зміни в технологіях, нормативно-правовому середовищі або у контексті нових загроз. Це вимагає від системи безпеки високої гнучкості та можливості інтеграції нових методів захисту. Адаптивні системи здатні виявляти нові типи загроз і застосовувати відповідні заходи для мінімізації їхнього впливу. Крім того, адаптивність дозволяє інтегрувати технології автоматизації та штучного інтелекту, що допомагають оперативно реагувати на зміни у реальному часі.

4) Надійність — принцип, орієнтований на забезпечення безперервного, стабільного функціонування систем технічного захисту як в умовах нормальної, так і аварійної експлуатації. Надійність передбачає здатність системи функціонувати без збоїв та відмов при впливі різноманітних зовнішніх чи внутрішніх чинників. Системи повинні бути спроектовані таким чином, щоб забезпечити максимальний рівень безпеки навіть при наявності несправностей або в умовах обмежених ресурсів. Для цьо-

го використовуються технології резервування, надлишковості та відновлення після збоїв, а також механізми постійного моніторингу для виявлення можливих проблем на ранніх етапах.

Ці методологічні принципи формуються в конкретні *технологічні та організаційні рішення*, які регламентуються відповідними стандартами, нормами безпеки та галузевими протоколами. У міжнародній практиці для забезпечення технічної безпеки розроблені численні нормативні документи, такі як ISO 27001, ISO 9001, NIST SP 800-53 та інші. Вони визначають вимоги до проектування, реалізації та моніторингу систем безпеки, а також регламентують процедури аудиту, тестування та верифікації технічних систем.

У результаті застосування цих принципів формується *комплексна стратегія безпеки,* яка дозволяє забезпечити високий рівень захисту від потенційних загроз та адаптувати систему до змін у технологічному середовищі [47, с. 2-4]. Цей підхід дозволяє ефективно управлінню безпекою на всіх етапах життєвого циклу технічної системи — від проектування до експлуатації та модернізації.

1.3.3. Базові принципи забезпечення технічної безпеки

До фундаментальних принципів технічної безпеки належать наступні [19, с. 122].

1) Принцип пріоритетності безпеки над функціональністю. У процесі проектування, експлуатації та модернізації технічних систем безпека повинна мати переважну вагу над іншими техніко-економічними критеріями. Це означає, що жодна інновація або підвищення ефективності не повинні реалізовуватись ціною потенційного збільшення рівня ризику.

2) Принцип ідентифікації та аналізу ризиків.

Формування систем безпеки має ґрунтуватися на систематичному процесі ідентифікації загроз та оцінювання ймовірності їх реалізації. У цьому контексті використовуються як класичні методи (FTA, HAZOP, FMEA), так і сучасні підходи з використанням штучного інтелекту та великих даних.

3) Принцип багаторівневої захищеності (defense-in-depth).

Ефективна система технічної безпеки має передбачати кілька незалежних рубежів захисту, які взаємно дублюють один одно-

го, забезпечуючи мінімізацію шкоди навіть у разі виходу з ладу окремих елементів системи.

Приклад 1.
Застосування принципу багаторівневої захищеності в енергетиці
При побудові системи безпеки гідроелектростанції застосовується щонайменше 4 рівні:
a) Контроль доступу до об'єкта (фізичний бар'єр + біометрія);
b) Механічні запобіжники турбін (автоматичне відключення при перевантаженні);
c) Системи раннього виявлення аварій (сенсори вібрації, температури);
d) Цифрове резервне управління (у разі втрати ручного контролю — алгоритмічне регулювання потоку).
Це зменшує ймовірність катастрофи в разі збою на окремому рівні на 75–92%.

4) Принцип невразливості до відмов (fail-safe / fail-operational design).

Конструкція та програмне забезпечення технічних систем повинні забезпечувати їх функціонування в безпечному режимі у випадку збоїв, відмов або зовнішніх впливів. Зокрема, це актуально для автоматизованих транспортних та енергетичних систем.

5) Принцип стандартизації та уніфікації.

Дотримання галузевих стандартів і протоколів безпеки (ISO 31000, IEC 61508, ISO/IEC 27001 тощо) дозволяє забезпечити сумісність, повторюваність і відтворюваність заходів безпеки, а також прискорює аудит та сертифікацію об'єктів.

6) Принцип неперервного моніторингу та аудиту.

Постійний контроль за параметрами функціонування систем, аналіз журналів подій, інспекції та діагностика дозволяють своєчасно виявляти девіації та оперативно реагувати на інциденти.

7) Принцип людиноцентричності.

Оскільки технічні системи експлуатуються людьми, критично важливо забезпечити зручний інтерфейс, логічність інструкцій, а також психологічну готовність операторів до дій в умовах небезпеки. Це включає ергономіку, психофізіологічну безпеку та управління людським фактором [49, с. 2-4].

1.3.4. Інтердисциплінарний аспект забезпечення технічної безпеки

Сучасний підхід до технічної безпеки неможливий без залучення знань із суміжних наукових галузей.

Зокрема:

1) Кібербезпека: поєднання IT-технологій із класичними підходами безпеки забезпечує захист від кібератак на інфраструктури критичного значення (SCADA, IoT, цифрові близнюки).

2) Штучний інтелект і машинне навчання: використовуються для прогнозування відмов, виявлення аномалій та автоматичного прийняття рішень у реальному часі.

3) Нанотехнології та нові матеріали: відкривають нові можливості для створення самовідновлюваних, стійких до пошкоджень матеріалів.

4) Поведінкова економіка та соціальна інженерія: дозволяють враховувати аспекти людської взаємодії з системами, моделювати ризики, пов'язані з несанкціонованим доступом або помилковими діями.

Приклад 2.

Використання штучного інтелекту в аналізі технічних загроз.

На підприємстві металургійного комплексу було впроваджено систему машинного навчання для прогнозування відмов електродвигунів. Збір даних від сенсорів вібрації, температури та шуму дозволив навчити модель передбачати потенційні збої з точністю 94%, що дозволило зменшити кількість аварійних простоїв на 36% протягом пів року.

1.3.5. Етапи реалізації принципів безпеки в технічних системах

Досягнення стійкого рівня безпеки технічних систем вимагає інтеграції безпекових принципів на кожному етапі їх життєвого циклу — від моменту проектування до остаточної утилізації. Такий підхід гарантує системність, комплексність та адаптивність заходів безпеки в умовах динамічних загроз.

1) Основні етапи забезпечення безпеки технічних систем.

a) Аналіз початкових умов.

На першому етапі здійснюється комплексне оцінювання середовища функціонування системи. Основними завданнями є: Ідентифікація потреб з урахуванням цільового призначення системи. Оцінка потенційних загроз та ризиків з урахуванням зовнішніх і внутрішніх факторів. Розробка моделей загроз з визначенням можливих векторів атак. Проведення попереднього аналізу впливу зовнішніх факторів (фізичних, кібернетичних, соціальних) на функціональність системи.

Цей етап є критичним для визначення базових параметрів безпеки, які впливатимуть на всі подальші рішення.

b) Інтеграція безпекових рішень у проекті

На етапі проектування формуються основи архітектури безпеки: Вибір технологій та протоколів, які забезпечують захист від виявлених ризиків. Розробка стратегії резервування та дублювання ключових компонентів системи. Моделювання можливих інцидентів для перевірки надійності вибраних рішень. Інтеграція елементів безпеки у функціональну структуру на ранніх етапах проектування.

Особлива увага приділяється принципу **Security by Design**, який передбачає закладення заходів безпеки на всіх рівнях архітектури.

c) Реалізація систем захисту.

На етапі реалізації здійснюється впровадження апаратних, програмних та організаційних заходів: Установка фізичних бар'єрів та систем доступу для забезпечення безпеки критичних компонентів. Інтеграція програмних модулів, що забезпечують виявлення аномалій та запобігання атакам. Розробка організаційних політик безпеки для мінімізації людського чинника. Практична реалізація вимагає гармонізації технічних та адміністративних заходів з урахуванням специфіки об'єкта.

d) Тестування та сертифікація.

На цьому етапі перевіряється відповідність реалізованих заходів безпеки нормативним вимогам та стандартам: Проведення функціонального тестування на витривалість та стійкість до кіберзагроз. Аудит на відповідність міжнародним стандартам безпеки (наприклад, ISO/IEC 27001, NIST). Оцінка захищеності

з боку незалежних експертів та сертифікаційних органів. Тестування дозволяє своєчасно виявити вразливості та внести коригування до системи безпеки.

е) Експлуатація з постійним моніторингом.

Забезпечення безпеки на етапі експлуатації передбачає: Постійний моніторинг стану системи для виявлення аномалій. Реалізацію механізмів збору та аналізу логів з метою раннього виявлення інцидентів. Впровадження систем реагування на інциденти та проведення навчань з персоналом. Регулярне оновлення захисних механізмів дозволяє підтримувати актуальність систем безпеки в умовах еволюції загроз.

f) Аналіз післяаварійної поведінки

У разі інциденту проводиться детальний аналіз для з'ясування причин та наслідків: Розробка звіту з докладним описом сценарію інциденту. Аналіз ефективності застосованих заходів безпеки. Корекція стратегій захисту з урахуванням нових загроз.

Цей етап сприяє вдосконаленню безпекової політики на основі практичного досвіду та аналізу наслідків.

2) Міждисциплінарний підхід до забезпечення безпеки

Принципи забезпечення технічної безпеки не обмежуються абстрактними положеннями. Вони формують чіткий алгоритм дій для мінімізації ризиків, збереження життя та здоров'я людей, а також захисту довкілля та підтримки критичних функцій систем. Ефективна реалізація можливостей забезпечення безпеки вимагає: Міждисциплінарної інтеграції знань з інженерії, кібербезпеки, соціології та права. Врахування людського чинника на кожному етапі життєвого циклу системи. Застосування сучасних технологій прогнозування та аналізу загроз. Чіткої нормативної регламентації з урахуванням актуальних стандартів.

Таким чином, забезпечення безпеки технічних систем — це складний та багатоетапний процес, який потребує системного підходу, інтеграції новітніх технологій та постійного вдосконалення на основі отриманого досвіду.

1.4. Нормативно-правове забезпечення безпеки технічних систем.

1.4.1. Засади правового регулювання у сфері технічної безпеки

Правове регулювання безпеки технічних систем (БТС) являє собою комплексну сукупність нормативно-правових актів, стандартів, технічних регламентів, інструкцій та процедур, спрямованих на забезпечення безпечного функціонування технічних об'єктів на всіх етапах їх життєвого циклу: проектування, виробництва, експлуатації, обслуговування та утилізації. Головною метою правового регулювання є забезпечення техногенної безпеки з урахуванням ризиків для людини, довкілля та критичної інфраструктури.

1) Основні складові правового регулювання БТС

a) Нормативно-правові акти: включають закони, постанови, накази та інші документи, що визначають загальні вимоги до безпеки технічних систем.

b) Стандарти та регламенти: технічні стандарти національного та міжнародного рівня (ISO, IEC, NIST), що встановлюють параметри безпеки та вимоги до якості технічних рішень.

c) Технічні умови та інструкції: документи, що конкретизують вимоги до окремих компонентів і технологій у технічних системах.

d) Процедури забезпечення безпеки: інструкції щодо управління ризиками, моніторингу та аудиту технічних систем у процесі експлуатації.

2) Міждисциплінарний характер правового регулювання

У сучасному контексті правове регулювання безпеки технічних систем інтегрує положення з різних сфер безпеки: інформаційної, екологічної, промислової, кіберфізичної, транспортної та інженерної. Це обумовлено комплексністю сучасних технічних систем, що все частіше є кіберфізичними об'єктами з високим рівнем автоматизації та цифровізації.

3) Інтеграція безпеки на етапі проєктування

Одним із ключових аспектів правового регулювання є впровадження принципу "безпека за дизайном" (Security by Design), який передбачає врахування аспектів безпеки на ранніх стадіях проєктування та розробки технічних систем. Це дозволяє мінімізувати ризики ще до початку їх експлуатації.

4) Вимоги до кібербезпеки технічних систем

З огляду на зростаючу роль кіберфізичних систем, правове регулювання охоплює вимоги до інформаційної безпеки, зокрема захисту даних, кіберзагроз та забезпечення безперебійного функціонування критичних компонентів. У міжнародній практиці широко використовуються рекомендації NIST та стандарти ISO/IEC 27000 щодо управління інформаційною безпекою.

5) Виклики та перспективи

Сучасне правове регулювання БТС стикається з викликами швидкого розвитку технологій, зокрема Інтернету речей (IoT) та штучного інтелекту (ШІ). Це вимагає постійного оновлення правової бази та адаптації до нових ризиків і загроз, що виникають унаслідок цифровізації та автоматизації виробничих і управлінських процесів.

У майбутньому правове забезпечення БТС повинно розвиватися з урахуванням глобальних стандартів та міждисциплінарного підходу, щоб забезпечити комплексний захист технічних систем у мінливих умовах технологічного прогресу.

6) Адаптація до нових викликів

Сучасні технічні системи часто мають глобальну інтеграцію та високу ступінь взаємозалежності з іншими системами, що зумовлює необхідність створення міжнародних угод та регламентів у сфері безпеки. Особливо актуальним є питання захисту кіберфізичних систем в умовах глобальної кіберзагрози та терористичної діяльності. Міжнародна співпраця та гармонізація стандартів сприятимуть підвищенню надійності технічних систем.

7) Стратегія безпеки на рівні державного управління

Необхідно створювати національні стратегії безпеки технічних систем, що передбачають синхронізацію правових вимог з міжнародними стандартами. Такі стратегії мають враховувати швидкі зміни технологій, що вимагає гнучких підходів до правового регулювання та його адаптації до нових умов.

1.4.2. Законодавча база України у сфері безпеки технічних систем та ключові законодавчі акти

а) Конституція України (ст. 16, 50, 66) – встановлює загальні права на безпечне довкілля, працю та життєдіяльність [1];

b) Закон України «Про охорону праці» – регулює безпеку праці на підприємствах, де використовуються технічні системи [8, с. 1-2];

c) Закон України «Про технічні регламенти та оцінку відповідності» – визначає загальні принципи регулювання технічної безпеки [10, с. 1-2];

d) Закон України «Про стандартизацію» – формує законодавче підґрунтя для впровадження національних стандартів [9];

e) Закон України «Про об'єкти підвищеної небезпеки» – містить положення про запобігання техногенним катастрофам [7, с. 1-2];

f) Кодекс цивільного захисту України – охоплює заходи щодо безпеки при надзвичайних ситуаціях, спричинених технічними несправностями [11];

g) Закон України «Про енергетичну ефективність та енергетичну безпеку» – впливає на вимоги до технічних систем в енергетиці [4];

h) Постанова Кабінету Міністрів України «Про затвердження переліку об'єктів та окремих територій, які підлягають постійному та обов'язковому на договірній основі обслуговуванню державними аварійно-рятувальними службами» [12, с. 1];

i) Постанова Кабінету Міністрів України «Про затвердження порядку ідентифікації та обліку об'єктів підвищеної небезпеки» [13, с. 2]

j) Закон України. Про Національну програму інформатизації [14, с. 1]

1.4.3. Система нормативно-технічних документів

1) Галузеві стандарти (ДСТУ, ISO, EN):

a) Національні стандарти ДСТУ та гармонізовані міжнародні (ISO, EN) регулюють [15, с. 1]:

b) Конструктивну безпеку (наприклад, ISO 12100 — загальні принципи проектування безпечних машин);

c) Функціональну безпеку (IEC 61508);

d) Захист від небезпечних впливів (ДСТУ EN 60204);

e) Кіберзахист технічних систем (ISO/IEC 27000-серія).

2) Технічні регламенти:

Обов'язкові до виконання документи, які визначають вимоги безпеки до електротехнічного обладнання; машин та механізмів; вибухонебезпечних середовищ; газового обладнання; засобів індивідуального захисту тощо.

3) Процедури оцінки відповідності технічних систем

Передбачають сертифікацію, декларування та аудит для підтвердження відповідності ТС чинним вимогам. Уповноваженими органами виступають ДП «УкрНДНЦ», Держпраці, ДСНС, НТЦ «Енергоефективність», а також незалежні акредитовані лабораторії.

1.4.4. Міжнародне нормативно-правове регулювання організації безпеки технічних систем

Основні міжнародні документи

a) Директиви ЄС (Machinery Directive 2006/42/EC, ATEX 2014/34/EU);

b) Конвенції МОП (№ 155, 176);

c) Стандарти ISO/IEC;

d) Регламенти МАГАТЕ (у сфері ядерної безпеки);

e) Рекомендації OECD щодо безпеки промислових об'єктів.

Україна адаптує своє законодавство до ACQUIS COMMUNAUTAIRE ЄС, зокрема в рамках Угоди про асоціацію. Сектор технічного регулювання в цьому контексті є ключовим для забезпечення технологічної безпеки та інноваційного розвитку.

1.4.5. Інституційно-правовий механізм забезпечення безпеки технічних систем

1) Головні суб'єкти щодо організації безпеки технічних систем

a) Кабінет Міністрів України – формує політику у сфері технічної безпеки.

b) Міністерство економіки, МОН, Держпраці, ДСНС, Держенергонагляд – здійснюють нормативне та наглядове регулювання.

c) Наукові установи (Інститут проблем машинобудування ім. А.Н. Подгорного, НАН України) – розробляють експертні оцінки, нові технічні регламенти.

d) Недержавні організації – Асоціація інженерів-безпекознавців, Громадська рада з безпеки технічних систем тощо.

2) Механізми контролю та санкцій містять наступне.

a) Технічний аудит;

b) Державний нагляд;

c) Експертиза ризиків [6, с. 2];

d) Призупинення діяльності чи накладення штрафів;

Застосування кримінальної та адміністративної відповідальності у разі порушення вимог технічної безпеки.

1.4.6. Актуальні виклики та тенденції у сфері нормативного регулювання безпеки технічних систем.

У сучасних умовах стрімкого технологічного розвитку виникає потреба у вдосконаленні нормативного регулювання безпеки технічних систем (БТС). Цей процес обумовлений численними викликами та тенденціями, які формуються під впливом глобальних змін у цифровій, екологічній та соціально-економічній сферах.

Однією з головних тенденцій є цифровізація та забезпечення smart-безпеки технічних систем. З розвитком кіберфізичних систем (КФС) та технологій штучного інтелекту (ШІ) з'являються нові вимоги до їхньої безпеки. Це зумовлює необхідність встановлення стандартів безпеки для Інтернету речей (IoT), які дозволяють забезпечити захист даних, відстеження технічного стану та контроль за змінами в системах.

Застосування технології блокчейн у цьому контексті є перспективним напрямом. Завдяки розподіленим реєстрам можна створити прозорі й надійні механізми моніторингу технічного стану компонентів БТС, що забезпечує підвищення надійності та зменшення ризику несанкціонованих втручань.

З огляду на глобальні кліматичні зміни виникає необхідність впровадження нових стандартів у сфері екологічної безпеки технічних систем. Особлива увага приділяється нормам щодо скорочення викидів парникових газів, утилізації технічних компонентів та енергоефективності систем.

Екомаркування технічних систем та впровадження вимог до енергоефективності сприяють зменшенню негативного впливу на довкілля. Важливим аспектом є також створення нормативних актів, що регулюють безпечну утилізацію обладнання після завершення його життєвого циклу.

Умови глобалізації формують потребу в мультинаціональній сертифікації технічних систем. Взаємне визнання сертифікатів безпеки між країнами дозволяє спростити процеси імпорту та експорту продукції, забезпечуючи при цьому високий рівень безпеки.

Використання загальновизнаних протоколів безпеки сприяє стандартизації на міжнародному рівні та дозволяє оптимізувати процеси тестування та сертифікації.

Останнім часом зростає увага до впровадження принципів ESG (екологічних, соціальних та управлінських аспектів) у нормативну базу безпеки технічних систем. Це дозволяє не лише враховувати екологічні ризики, а й забезпечувати соціально відповідальний підхід до управління безпекою.

Таким чином, нормативне регулювання безпеки технічних систем у сучасному світі стає багатовимірним процесом, що включає цифровізацію, екологічність, глобалізацію та

1.4.7. Приклади імплементації нормативів безпеки

З прикладами імплементації нормативів безпеки технічних систем можна ознайомитись у таблиці 1.1.

Таблиця 1.1. Приклади імплементації нормативів безпеки.

Приклад	Об’єкт	Норма/регламент	Ефект
1	Автоматизована система керування вентиляцією у шахті	ISO 13849-1 (PL)	Зменшено ризик вибуху метану на 70%
2	Розумна енергомережа	IEC 62351	Захищено обмін даними від зовнішніх атак
3	Виробнича лінія пакування харчів	ДСТУ EN 1672-2	Гігієнічна безпека, сертифі-

Приклад	Об’єкт	Норма/регламент	Ефект
			кація на експорт
4	Технічний аудит в агропромисловості	ДСТУ ISO 19011	Підвищено ефективність управління ризиками

Нормативно-правове забезпечення безпеки технічних систем є фундаментальним чинником у забезпеченні стабільного функціонування критичної інфраструктури, виробничих процесів і захисту життя громадян. Удосконалення нормативної бази має відбуватись із урахуванням науково-технічного прогресу, міжнародних тенденцій та національних пріоритетів безпеки.

Контрольні питання

1. Що розуміється під поняттям «технічна система»?
2. Які основні характеристики технічних систем?
3. Як класифікуються технічні системи за функціональним призначенням?
4. Які критерії використовуються для класифікації технічних систем за складністю?
5. У чому полягають відмінності між автоматизованими та автономними технічними системами?
6. Як впливає рівень інтеграції системи на її безпеку?
7. Які основні джерела загроз безпеці технічних систем?
8. Як класифікуються загрози за їхньою природою?
9. Які фактори впливають на ризик виникнення техногенних загроз?
10. Які основні типи інформаційних загроз у технічних системах?
11. У чому полягає різниця між внутрішніми та зовнішніми загрозами безпеці?
12. Яким чином соціальні фактори можуть впливати на безпеку технічних систем?

13. Які методи використовуються для ідентифікації загроз у технічних системах?

14. Як змінюється класифікація загроз при інтеграції систем із цифровими технологіями?

15. Які основні принципи забезпечення технічної безпеки?

16. Як принцип резервування сприяє підвищенню безпеки системи?

17. У чому полягає принцип надійності та як він реалізується в технічних системах?

18. Які заходи забезпечують принцип стійкості технічних систем до зовнішніх впливів?

19. Як принцип адаптивності впливає на безпеку технічних систем?

20. Які методи оцінки ризиків використовуються при забезпеченні технічної безпеки?

21. Як забезпечується принцип безперервності функціонування технічних систем?

22. Які міжнародні стандарти регулюють безпеку технічних систем?

23. Які національні нормативно-правові акти визначають вимоги до безпеки технічних систем?

24. У чому полягає роль технічних регламентів у забезпеченні безпеки?

25. Які основні вимоги до сертифікації технічних систем на відповідність безпековим стандартам?

РОЗДІЛ 2. АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА ЗАСОБИ ЗАХИСТУ ТЕХНІЧНИХ СИСТЕМ

2.1. Методи ідентифікації ризиків та оцінка вразливостей технічних систем

2.1.1. Поняття ризику та вразливості в технічних системах

У контексті технічних систем, ризик визначається як ймовірність того, що певна подія, що може мати негативні наслідки, відбудеться в межах функціонування системи. Ці наслідки можуть варіюватися від незначних збоїв до серйозних техногенних аварій або навіть загрози для безпеки життя людей. Ризик може виникнути через відмови окремих компонентів системи, порушення її нормальної роботи або через вплив зовнішніх факторів, таких як природні катастрофи, терористичні атаки або зловмисні вторгнення. У результаті таких подій система може вийти з ладу або стати неефективною, що призведе до матеріальних втрат, порушення нормальної діяльності організацій або навіть до загрози для життя та здоров'я людей [41, с. 8].

Уразливість технічної системи визначається як її здатність піддаватися негативним впливам з боку різноманітних загроз, будь-то внутрішні чи зовнішні фактори. Вона відображає слабкі місця в архітектурі, компонентах, процесах або методах управління системою, які можуть бути використані зловмисниками або можуть сприяти виникненню непередбачених ситуацій [58, с. 2]. Уразливість може проявлятися на різних рівнях, починаючи від фізичної частини системи (наприклад, слабкі точки у конструкції обладнання) до програмного забезпечення (де можуть виникати вразливості, які дозволяють здійснити несанкціонований доступ) або навіть у процесах управління та обслуговування системи (наприклад, недостатня увага до оновлення програмного забезпечення або неможливість вчасно відреагувати на зміни в середовищі).

Ідентифікація ризиків та оцінка вразливостей є ключовими етапами в управлінні безпекою технічних систем, оскільки вони дозволяють виявити потенційні загрози та проблеми на ранніх етапах їх виникнення. Зрозуміти, де система має слабкі місця, та прогнозувати, яким чином ці слабкості можуть бути використані для атаки або аварії, допомагає вжити своєчасних превентивних

заходів. Це може включати як технічні засоби захисту, так і організаційні чи управлінські зміни, що сприятимуть зменшенню ймовірності виникнення ризиків.

Зазначені етапи також є невід'ємною частиною процесу аналізу і керування безпекою впродовж життєвого циклу технічної системи. Постійна оцінка ризиків та вразливостей дає змогу адаптувати систему до нових викликів та змін у зовнішньому середовищі, підтримувати її на високому рівні безпеки та ефективності, а також мінімізувати потенційні негативні наслідки для її користувачів та оточення.

2.1.2. Методи ідентифікації ризиків

Методи ідентифікації ризиків є важливою складовою частиною управління безпекою технічних систем. Вони дозволяють не лише виявляти потенційні загрози, але й оцінювати ймовірність їх реалізації та можливі наслідки. Для цього використовуються різноманітні підходи, які можна умовно поділити на три основні категорії: якісні, кількісні та комбіновані методи. Кожен з цих методів має свої особливості, які дозволяють отримати як описові характеристики ризиків, так і числові показники, що допомагають більш точно оцінити ймовірність виникнення небезпек та їх вплив на функціонування систем.

1) Аналіз небезпек і критичних контрольних точок (HACCP)

Метод HACCP (Hazard Analysis and Critical Control Points) є системним підходом до управління ризиками, який широко використовується в різних галузях, зокрема у харчовій промисловості, медицині та екології. Основна мета цього методу — визначення потенційних небезпек на кожному етапі технологічного процесу та виокремлення критичних контрольних точок, на яких необхідно здійснювати спеціальне управління для мінімізації ризиків. При застосуванні HACCP здійснюється ретельний аналіз можливих загроз на кожному етапі роботи системи чи процесу, після чого визначаються ключові моменти, де збої можуть призвести до серйозних наслідків. Цей підхід дозволяє своєчасно вжити заходів для попередження небажаних подій.

2) Аналіз помилок та їх наслідків (FMEA)

Метод FMEA (Failure Modes and Effects Analysis) використовується для виявлення можливих помилок в окремих компонен-

тах системи та оцінки їхнього впливу на загальну функціональність. Основна мета цього методу — систематичне вивчення кожного елементу системи з метою виявлення потенційних відмов або дефектів, що можуть стати причиною збоїв у роботі. Після виявлення помилок проводиться оцінка їхнього потенційного впливу на загальну безпеку та ефективність системи. FMEA дозволяє не тільки ідентифікувати найбільш критичні проблеми, але й визначити пріоритетність їх усунення для зниження ймовірності виникнення катастрофічних наслідків.

3) Аналіз причинно-наслідкових зв'язків (FTA)

Метод FTA (Fault Tree Analysis) є графічним методом ідентифікації ризиків, який використовує дерево помилок для виявлення причинно-наслідкових зв'язків між подіями, що призводять до відмови або інциденту. Це дозволяє побудувати детальну модель ризиків, де кожна помилка є результатом певних факторів. FTA допомагає розібратися в складних механізмах взаємодії елементів системи та визначити, на якому етапі чи компоненті може статися збій, що призведе до аварії чи неполадки. Цей підхід дуже корисний для аналізу складних технічних систем, де важливо виявити не лише очевидні, а й приховані залежності між різними компонентами.

4) Аналіз ризиків з використанням сценаріїв (What-if Analysis)

Метод "What-if Analysis" є сценарним методом, який передбачає розгляд різноманітних можливих ситуацій і подій, що можуть виникнути в результаті змін умов чи параметрів системи. Цей метод дозволяє моделювати різні сценарії розвитку подій, зокрема ті, які є малоймовірними, але можуть мати катастрофічні наслідки. Наприклад, якщо зміни в одному з параметрів системи можуть призвести до серйозної аварії або збою, то аналіз таких сценаріїв дозволяє завчасно розробити заходи для нейтралізації потенційних загроз. Використання методу "What-if" також допомагає оцінити поведінку системи в умовах невизначеності або змін зовнішнього середовища.

5) Метод експертних оцінок

Метод експертних оцінок є якісним підходом до ідентифікації ризиків, що полягає в залученні фахівців, які на основі свого досвіду та знань оцінюють ймовірність виникнення різних загроз. Цей метод зазвичай використовується, коли кількісні дані

про ризики відсутні або недостатні. Експерти можуть оцінювати ймовірність певних подій, їх наслідки, а також надати рекомендації щодо заходів з мінімізації ризиків. Хоча цей метод є суб'єктивним, він є важливим інструментом для отримання більш глибоких інсайтів щодо можливих небезпек, особливо в тих випадках, коли немає достатньо даних для застосування більш точних кількісних методів.

Застосування різних методів ідентифікації ризиків, таких як HACCP, FMEA, FTA, What-if Analysis та експертні оцінки, дає змогу з різних точок зору оцінити можливі загрози для технічних систем. Кожен з цих методів дозволяє виявити специфічні аспекти ризиків, що, у свою чергу, дозволяє ефективно планувати стратегії їх усунення або мінімізації. Ключовим є те, що комбіноване використання якісних, кількісних та змішаних методів дозволяє досягнути найвищої точності в прогнозуванні і оцінці ризиків, що є критично важливим для безпеки та ефективності технічних систем.

З особливостями різних методів ідентифікації ризиків у технічних системах можна ознайомитись у таблиці 2.1.

Таблиця 2.1. Особливості методів ідентифікації ризиків у технічних системах.

Метод	**Опис**	**Переваги**	**Недоліки**
HACCP	Визначення критичних точок	Системний підхід, профілактика	Вимагає постійного моніторингу
FMEA	Оцінка помилок та їх наслідків	Рання ідентифікація проблем	Трудомісткість аналізу
FTA	Аналіз причин збоїв	Деталізація причинних зв’язків	Складність моделювання
What-if	Розгляд гіпотетичних сценаріїв	Гнучкість, варіативність	Суб’єктивність оцінки
Експертні оцінки	Досвід фахівців	Швидкість аналізу	Ризик упередженості

2.1.3. Методи оцінки вразливостей технічних систем

Оцінка вразливостей технічних систем є важливим етапом у забезпеченні їх надійності та безпеки. Вона спрямована на виявлення та аналіз слабких місць у конструкції, інженерних рішеннях, технологічних процесах, а також у програмному забезпеченні та взаємодії компонентів [36, с. 12]. Це дає змогу своєчасно вжити заходів для мінімізації ризиків, пов'язаних із можливими відмовами або атакою на систему, та забезпечити її стабільну роботу в умовах змінних навантажень, помилок або зовнішніх загроз.

Оцінка вразливостей здійснюється за допомогою низки методів, кожен з яких фокусується на певних аспектах системи. Вони дозволяють не лише виявляти потенційні слабкості, але й оцінювати їхній вплив на загальну ефективність, безпеку та функціональність системи [57, с. 1-4].

1) Аналіз стану технічних компонентів (Maintenance Assessment)

Аналіз стану технічних компонентів є одним із основних методів оцінки уразливостей, орієнтуючись на вивчення фізичного та функціонального стану окремих елементів системи. Це може включати діагностику обладнання, перевірку його зношеності, корозії, механічних або електричних дефектів. Зазвичай цей метод полягає в регулярному технічному обслуговуванні та плановому ремонті, що дає змогу запобігти виникненню відмов через неадекватний стан технічних компонентів. Крім того, аналіз стану включає виявлення слабких місць, де висока ймовірність виникнення збоїв, що може негативно позначитися на роботі всієї системи. Оцінка проводиться на основі даних про експлуатацію, історію ремонту та технічне обслуговування.

Цей метод допомагає визначити необхідні дії для покращення надійності системи, включаючи заміну зношених елементів, модернізацію застарілих компонентів або вдосконалення процесів технічного обслуговування.

2) Відмовостійкий аналіз (Reliability Assessment)

Відмовостійкий аналіз є методикою, яка дозволяє оцінити здатність технічних систем функціонувати належним чином протягом заданого періоду, незважаючи на можливі відмови окремих компонентів. Метод полягає в розрахунку ймовірності відмови компонентів системи та аналізі їхнього впливу на загальну функціональність. Відмовостійкість часто оцінюється за

допомогою статистичних методів, таких як моделі "час до відмови", що дозволяє точно передбачити терміни експлуатації обладнання та можливість його відмови при певних умовах.

Оцінка відмовостійкості включає в себе визначення критичних компонентів, що є найвразливішими до поломок, та оцінку їхнього впливу на працездатність усієї системи. Для цього проводяться тести, моделювання та аналіз ймовірностей, що дозволяє оптимізувати дизайн технічних систем і підвищити їхню надійність.

3) Кібербезпековий аудит вразливостей (Cyber Vulnerability Assessment)

Кібербезпековий аудит є важливою складовою частиною оцінки уразливостей для сучасних технічних систем, що включають інформаційні технології та програмне забезпечення. Цей метод дозволяє виявити потенційні вразливості в системах безпеки, мережах і програмному забезпеченні, що можуть бути використані для несанкціонованого доступу, атак або компрометації даних. Кібербезпековий аудит передбачає перевірку захисту від різних видів кіберзагроз, таких як хакерські атаки, вірусні програми, фішинг, атаки типу "відмова в обслуговуванні" (DDoS) та інші.

Аудит включає в себе перевірку фізичних і програмних бар'єрів, тестування на проникнення, перевірку політик безпеки, криптографічних засобів захисту даних і доступу до критичних інформаційних ресурсів. Виявлення кіберзагроз на ранніх етапах дозволяє своєчасно вжити заходів для посилення захисту та уникнути можливих серйозних наслідків.

4) Сценарний аналіз наслідків відмови (Consequence Analysis)

Сценарний аналіз наслідків відмови є методом, що орієнтований на оцінку потенційних наслідків відмови технічних компонентів або цілісних систем. У процесі такого аналізу розглядаються різні сценарії можливих відмов, що можуть відбутися в умовах змін або навантажень на систему. Цей метод дозволяє оцінити масштаби впливу конкретної відмови на загальну роботу системи, а також на безпеку та стабільність навколишнього середовища.

Сценарний аналіз допомагає визначити найгірші можливі наслідки відмови компонентів, зокрема втрати даних, пошкодження критичної інфраструктури, порушення функціонування тех-

нічної системи або навіть загрозу для здоров'я та життя людей. Аналіз сценаріїв допомагає виявити найбільш вразливі місця в системі, що потребують додаткових заходів захисту або модернізації для зниження ймовірності катастрофічних наслідків.

Оцінка уразливостей технічних систем є необхідною складовою для забезпечення їх безпеки та надійності. Використання різних методів, таких як аналіз стану технічних компонентів, відмовостійкий аналіз, кібербезпековий аудит та сценарний аналіз наслідків відмови, дозволяє всебічно оцінити слабкі місця системи та своєчасно вжити заходів для їх усунення або мінімізації. Це дає змогу запобігти можливим відмовам, знизити ризики технічних збоїв та забезпечити стабільну роботу системи навіть у складних або небезпечних умовах експлуатації. З різними методами оцінки слабких місць технічних систем можна ознайомитись у таблиці 2.2.

Таблиця 2.2. Методи оцінки слабких місць технічних систем.

Метод	**Опис**	**Галузь застосування**	**Приклади використання**
Maintenance Assessment	Перевірка технічного стану	Промисловість, транспорт	Ремонтні програми
Reliability Assessment	Оцінка надійності системи	Машинобудування	Моніторинг виробничих ліній
Cyber Vulnerability Assessment	Аналіз вразливостей кіберсистем	IT, автоматизація	Тестування захисту мереж
Consequence Analysis	Оцінка наслідків збоїв	Критична інфраструктура	Моделювання аварій

2.1.4. Сучасні підходи до ідентифікації ризиків та вразливостей

Сучасний розвиток технологій сприяє впровадженню інноваційних підходів до забезпечення безпеки технічних систем. З урахуванням стрімкої цифровізації та інтелектуалізації процесів,

нові методи забезпечення технічної безпеки орієнтовані на використання передових інформаційних технологій, що дозволяють не лише підвищити рівень захисту, але й оптимізувати процеси ідентифікації та оцінки ризиків. Ось кілька основних інструментів та підходів, що застосовуються в сучасній практиці:

1) Застосування штучного інтелекту для аналізу великих даних (Big Data Risk Assessment)

У зв'язку зі зростанням обсягів даних, що генеруються різними системами, включаючи інформацію про роботу технічних систем, спостереження за інфраструктурними об'єктами та моніторинг з пристроїв Інтернету речей, аналіз великих даних став важливим компонентом виявлення та оцінки ризиків. Штучний інтелект (ШІ), зокрема алгоритми машинного навчання, здатні здійснювати автоматизований аналіз великих масивів даних, виділяючи критичні тренди та патерни. Цей підхід дозволяє прогнозувати можливі загрози та вразливості в технічних системах на основі історичних даних та поточних показників. Наприклад, аналізуючи дані про температуру, навантаження або вібрації в складних інженерних системах, ШІ може виявити аномалії, що свідчать про потенційні несправності або загрози для безпеки.

2) Використання цифрових двійників для моделювання сценаріїв (Digital Twin Risk Analysis)

Цифрові двійники (Digital Twin) — це віртуальні копії фізичних об'єктів або систем, які дозволяють здійснювати їх моніторинг, аналіз та симуляцію в реальному часі. Моделювання сценаріїв за допомогою цифрових двійників дозволяє не лише відслідковувати поточний стан об'єкта, але й прогнозувати його поведінку при зміні умов або в разі виникнення аварійних ситуацій. Цей підхід застосовується для оцінки ризиків у складних технічних системах, таких як енергетичні комплекси, транспортні мережі або промислові виробництва. Завдяки цифровим двійникам можна створювати різноманітні сценарії, що включають як нормальні умови роботи, так і критичні ситуації, щоб виявити потенційні вразливості та загрози для безпеки.

3) Інтеграція даних із систем Інтернету речей (IoT Vulnerability Assessment)

Інтернет речей (IoT) об'єднує безліч пристроїв, які можуть збирати та обмінюватися даними, включаючи датчики, пристрої управління та різні технічні компоненти, що забезпечують фун-

кціонування технічних систем. Ці пристрої генерують величезну кількість даних, що може бути використано для оцінки потенційних загроз і вразливостей. Інтеграція цих даних у систему оцінки ризиків дозволяє здійснювати комплексну оцінку технічних загроз на всіх етапах функціонування системи. Наприклад, дані про рівень зношеності обладнання або показники роботи сенсорів можуть виявити збої, до яких може призвести атака або несправність. Оцінка вразливостей системи IoT дозволяє своєчасно реагувати на потенційні проблеми, знижуючи ризики для загальної безпеки технічної інфраструктури.

Застосування передових методів, таких як штучний інтелект для аналізу великих даних, цифрові двійники для моделювання сценаріїв, та інтеграція даних із систем Інтернету речей, дозволяє значно підвищити ефективність оцінки ризиків і виявлення вразливостей у складних технічних системах. Вони дозволяють не тільки отримувати більше даних для аналізу, а й робити цей процес більш точним, оперативним і адаптивним до зміни умов експлуатації

2.1.5. Приклади практичної реалізації методів

1) Застосування методу Fault Tree Analysis

Аналіз безпеки електроенергетичних систем є важливим інструментом для виявлення потенційних вразливостей та прийняття відповідних заходів для зниження ймовірності відмови в критичних елементах інфраструктури. Метод Fault Tree Analysis (FTA) активно застосовується для моделювання та вивчення причин відмов у системах, що можуть призвести до порушення їх функціонування. В умовах електроенергетики, де стабільність та надійність поставок енергії є критично важливими, FTA допомагає визначити найбільш вразливі точки в системі.

Один із прикладів практичного застосування FTA — це зменшення ризику відмов через резервування ключових елементів мережі. Використання додаткових ресурсів, таких як резервні генератори, трансформатори чи лінії зв'язку, дозволяє знизити ймовірність відмови шляхом забезпечення дублювання на випадок поломки основних елементів. Наприклад, у разі відмови головного генератора, включення резервного забезпечує безперервність енергопостачання, що знижує ризик виникнення масових відключень та збитків для споживачів.

Резервування елементів електричних систем також включає створення багаторівневих механізмів для автоматичного перемикання на резервні канали або обладнання, що є важливою складовою забезпечення безпеки системи.

2) Оцінка ризику кіберзагроз у промислових об'єктах (Cyber Assessment) — підвищення стійкості мережевих компонентів

У сучасних промислових об'єктах, де впроваджено складні автоматизовані системи та інформаційні технології, однією з найбільших загроз є кібербезпека. Оцінка ризику кіберзагроз (Cyber Assessment) дозволяє оцінити можливі вразливості в інформаційних та мережевих компонентах об'єкта, що може призвести до серйозних наслідків, таких як порушення роботи виробничих ліній, крадіжка даних чи маніпуляції з обладнанням.

Методика Cyber Assessment включає виявлення слабких місць в мережевих компонентах (маршрутизатори, сервіси, комп'ютерні системи) та їх захист за допомогою сучасних засобів кібербезпеки, таких як фаєрволи, системи виявлення вторгнень (IDS), шифрування даних, багатофакторна аутентифікація тощо. Завдяки таким заходам значно підвищується стійкість до потенційних атак, зокрема від кібератак, таких як DDoS, фішинг чи впровадження шкідливих програм.

Прикладом реалізації оцінки кіберризиків є проект, в рамках якого були проведені тестування на проникнення в мережу виробничого підприємства та встановлені додаткові засоби захисту для запобігання несанкціонованому доступу до важливих даних і систем. Це дозволило істотно знизити рівень вразливості та підвищити загальну кіберстійкість системи.

***3) Моніторинг стану технічних компонентів на транспорті (Maintenance Assessment) — зменшення аварійності на* 30%**

У галузі транспорту, де надійність технічних компонентів є критичним фактором для забезпечення безпеки перевезень, важливим є проведення моніторингу стану цих компонентів. Використання методів Maintenance Assessment дозволяє своєчасно виявляти можливі дефекти та несправності в технічних системах транспортних засобів чи інфраструктури. Це допомагає знижувати ризик виникнення аварійних ситуацій, а також оптимізувати процес обслуговування та ремонту техніки.

Зокрема, за допомогою методів моніторингу стану та аналізу наявних даних (збір статистики, застосування датчиків для вимірювання різних параметрів), можна визначити знос елементів, які потребують заміни чи ремонту. У разі, коли несправність виявляється на ранньому етапі, це дозволяє запобігти більш серйозним поломкам і зменшити ймовірність аварій.

Реалізація таких підходів на транспорті призводить до значного зменшення аварійності, як показують результати практичного застосування. Наприклад, на залізничному або авіаційному транспорті, де було впроваджено системи для моніторингу стану критичних компонентів (двигунів, підшипників, гальмівних систем), вдалося знизити аварійність на 30%. Це стало можливим завдяки своєчасному виявленню дефектів та зниженню ймовірності виникнення серйозних поломок, що в свою чергу підвищило загальний рівень безпеки транспорту.

Таким чином, кожен із зазначених методів забезпечує значне підвищення безпеки та ефективності роботи в критичних інфраструктурах, що важливо для запобігання аваріям, зниження ризиків та оптимізації витрат на обслуговування.

Методи ідентифікації ризиків та оцінки уразливостей технічних систем є необхідним інструментом управління безпекою. Удосконалення методів аналізу з використанням інноваційних підходів дозволяє підвищити стійкість систем до техногенних загроз і зменшити ймовірність виникнення аварійних ситуацій.

2.2. Технічні та програмні засоби захисту систем і компонентів технічних систем

Загальні положення технічного та програмного захисту технічних систем

У сучасному світі, з розвитком технологій, безпека технічних систем стала однією з найважливіших проблем, яка безпосередньо впливає на стабільність функціонування промислових підприємств, транспортних мереж та інших критично важливих інфраструктур. В умовах, коли автоматизація та інтеграція інформаційно-комунікаційних технологій (ІТ) стають невід'ємною частиною інфраструктури, забезпечення безпеки цих систем набуває особливої важливості.

Сучасні технічні системи, включаючи ті, що функціонують у виробничих і транспортних галузях, вимагають особливої уваги

до забезпечення безпеки на всіх етапах їх експлуатації. Високий рівень автоматизації та впровадження ІТ-рішень у такі системи робить їх уразливими до різноманітних загроз, як з боку збоїв у технічних компонентах, так і від потенційних кібератак. Тому вкрай важливою є наявність ефективних технічних і програмних засобів захисту, здатних гарантувати стабільну роботу систем та захистити критичні дані.

Захист технічних систем включає в себе широкий комплекс заходів, основною метою яких є забезпечення трьох ключових аспектів: конфіденційності, цілісності та доступності даних і функціональних компонентів. Ці три складові є основою для ефективної роботи систем, де будь-яка втрата або пошкодження даних може призвести до серйозних наслідків.

2.2.1. Технічні засоби захисту

Технічні засоби захисту забезпечують надійність роботи систем і мінімізують можливі наслідки аварійних ситуацій, а також сприяють зменшенню ймовірності технічних збоїв. Зокрема, вони включають в себе [22, с. 94]:

1) Засоби фізичного захисту.

Фізичний захист є основним елементом безпеки, оскільки він запобігає несанкціонованому доступу до важливих технічних компонентів. До таких засобів належать захисні бар'єри, які обмежують доступ до критичних об'єктів, а також системи контролю доступу, що дозволяють забезпечити високий рівень захисту на всіх етапах використання технічних засобів. Це можуть бути як біометричні системи, так і системи карткових доступів.

2) Системи моніторингу та діагностики:

Системи моніторингу та діагностики включають сенсори, контролери, а також автоматизовані системи оповіщення, які дозволяють в реальному часі відслідковувати стан усіх важливих компонентів системи. Вони здатні оперативно виявити несправності або потенційні загрози, що дозволяє прийняти заходи для запобігання аварійним ситуаціям. Наприклад, системи контролю температури, вологості, вібрації та інших параметрів критичних компонентів.

3) Засоби резервування та дублювання критичних компонентів:

Важливим елементом забезпечення безпеки є використання засобів резервування та дублювання, які дозволяють зберігати працездатність системи в разі відмови окремих її компонентів. Це можуть бути дублюючі блоки живлення, системи резервного зберігання даних або додаткові сервери, які автоматично активуються в разі виходу з ладу основних компонентів.

4) Аварійно-відновлювальні комплекси:

У разі виникнення аварійних ситуацій, таких як відключення електроенергії або інші непередбачувані обставини, аварійно-відновлювальні комплекси, до яких належать дизель-генератори, блоки безперебійного живлення (UPS) та інші подібні рішення, дозволяють забезпечити безперервність роботи систем. Це дозволяє не тільки мінімізувати час простою, а й забезпечити стабільну роботу критичних компонентів у періоди відмови основних джерел енергії.

Застосування всіх цих засобів в сукупності дозволяє створити багаторівневу систему захисту технічних і інформаційних систем, що гарантує їх стійкість до різноманітних загроз і збоїв. Комплексний підхід до захисту технічних систем є важливим фактором для забезпечення їх стабільного та безпечного функціонування в умовах сучасного технологічного прогресу.

2.2.2. Програмні засоби захисту

Програмні засоби захисту технічних систем є основним інструментом забезпечення інформаційної безпеки в сучасних інформаційних та технічних інфраструктурах. Їх функціональність спрямована на захист даних від різноманітних загроз, таких як несанкціонований доступ, маніпуляції з даними, їх втрата чи пошкодження, а також на запобігання впливу шкідливого програмного забезпечення. Вони є незамінними компонентами систем безпеки, що дозволяють забезпечити конфіденційність, цілісність та доступність інформації [22, с. 75].

Основні категорії програмних засобів захисту включають наступне.

1) Антивірусні програми та засоби захисту від шкідливого програмного забезпечення (ШПЗ).

Антивірусні програми є класичним елементом програмного захисту, спрямованим на виявлення, блокування та видалення шкідливого ПЗ. Їхня основна мета — виявлення та нейтралізація

вірусів, черв'яків, троянських програм, шпигунських та рекламних програм, а також програм-здирників. Окрім традиційних підходів до виявлення шкідливого ПЗ через сигнатури, сучасні антивірусні системи використовують методи поведінкового аналізу, машинного навчання та евристичного аналізу для запобігання впливу нових або невідомих загроз. Завдяки цьому, вони здатні виявляти навіть маловідомі чи ще не зафіксовані типи шкідливого ПЗ.

2) Системи виявлення та запобігання вторгненням (IDS/IPS)

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є потужними інструментами для виявлення та попередження атак на інформаційні системи. IDS здійснює моніторинг мережевого трафіку та активності в системах для виявлення підозрілих дій, таких як спроби несанкціонованого доступу чи інші аномалії, що можуть свідчити про можливу атаку. У свою чергу, IPS має додаткову функціональність блокування виявлених атак, активуючи механізми для припинення шкідливої активності в режимі реального часу. Вони можуть працювати як на рівні мережі, так і на рівні хостів, використовуючи різні методи виявлення: сигнатурний, аномалійний та базований на поведінці.

3) Програмні комплекси контролю доступу та аутентифікації користувачів

Контроль доступу та аутентифікація користувачів є критичними елементами в забезпеченні безпеки інформаційних систем. Програмні засоби цього класу регулюють, хто має право отримувати доступ до певних ресурсів та в якій мірі. Вони включають системи аутентифікації, що підтверджують особу користувача, використовуючи паролі, біометричні дані, токени чи багатофакторну аутентифікацію. Крім того, ці системи відповідають за контроль доступу на основі ролей (RBAC), визначаючи, який рівень доступу до ресурсів має кожен користувач чи група користувачів. Вони також можуть включати механізми журналювання та аудиту для відслідковування всіх дій користувачів в системі.

4) Засоби криптографічного захисту даних

Криптографія є важливим інструментом захисту даних як при зберіганні, так і при їх передачі через мережу. Засоби криптографії, включаючи алгоритми шифрування та цифрові підписи,

забезпечують захист від несанкціонованого доступу, маніпуляцій з даними, а також гарантують цілісність та аутентичність інформації. Шифрування даних дозволяє їх перетворювати в незрозумілий вигляд, що вимагає наявності ключа для відновлення початкової інформації. Окрім шифрування, цифрові підписи дозволяють підтвердити авторство та незмінність даних, що є надзвичайно важливим для забезпечення юридичної та організаційної безпеки в рамках різних типів транзакцій.

Таким чином, програмні засоби захисту технічних систем займають ключову роль у забезпеченні інформаційної безпеки, дозволяючи здійснювати контроль за доступом, виявляти та нейтралізувати загрози, а також захищати дані від втрати та пошкодження. Вони працюють у тісній інтеграції, створюючи багаторівневу систему захисту, яка є важливою для забезпечення стабільної роботи сучасних технічних систем.

2.2.3. Порівняльні особливості технічних та програмних засобів захисту

З'ясування особливостей технічних, програмних та комбінованих засобів захисту можна здійснити на підставі аналізу даних, наведених у таблиці 2.3.

Таблиця 2.3. Переваги та недоліки технічних, програмних та комбінованих засобів захисту

Засоби захисту	**Переваги**	**Недоліки**
Технічні засоби	Висока фізична надійність	Великі витрати на встановлення та обслуговування
Програмні засоби	Гнучкість, можливість оновлення	Уразливість до кібератак та програмних збоїв
Комбіновані рішення	Інтегрований підхід, висока ефективність	Складність управління та координації різнорідних систем

2.2.4. Інноваційні технології в забезпеченні безпеки технічних систем та графічне порівняння технічних та програмних засобів захисту

Застосування штучного інтелекту (ШІ) та машинного навчання (МН) в галузі кібербезпеки значно посилює можливості виявлення та реагування на загрози. Інтелектуальні системи, побудовані на цих технологіях, дозволяють здійснювати глибокий аналіз поведінки компонентів технічних систем, що є основою для виявлення аномалій та потенційно небезпечних ситуацій. Наприклад, алгоритми машинного навчання можуть навчатися на великій кількості даних про нормальну поведінку мережевих пристроїв, що дозволяє їм вчасно ідентифікувати відхилення від звичайних патернів поведінки. Це може бути корисно для виявлення атак, таких як DDoS-атаки, несанкціоновані спроби доступу або інші види зловмисної діяльності.

Машинне навчання, зокрема методи глибинного навчання та нейронні мережі, здатні виявляти більш складні та масковані загрози, які важко виявити традиційними методами безпеки. Завдяки здатності адаптуватися до нових ситуацій, ці системи можуть покращувати свою ефективність з часом, що робить їх ідеальними для застосування в умовах постійно змінюваного кіберпростору.

У поєднанні з технологією блокчейн, яка забезпечує незмінність і прозорість всіх записів, такі системи безпеки набувають ще більшої ефективності. Блокчейн гарантує, що всі дії та зміни, які відбуваються в системі безпеки, фіксуються в незмінних реєстрах. Це дає можливість забезпечити високий рівень довіри до системи, оскільки записи про будь-які спроби атаки або інші важливі події не можуть бути змінені або підроблені. Кожен запис про інцидент або дію зберігається в розподіленому реєстрі, що робить систему більш стійкою до атак, які можуть намагатися маніпулювати або видаляти сліди.

Таким чином, поєднання технологій ШІ, МН та блокчейну створює потужний інструмент для забезпечення безпеки технічних систем. ШІ та МН здатні швидко виявляти загрози та адаптуватися до нових умов, а блокчейн забезпечує повну прозорість та незмінність записів, що підвищує ефективність контролю за безпекою та запобігає спробам фальсифікації даних. Це дозволяє створити надійні, адаптивні і стійкі системи безпеки для

захисту від сучасних кіберзагроз. Порівняння ефективності застосування технічних та програмних заходів безпеки у різних середовищах можна здійснити по даних, наведених на Рис. 2.1.

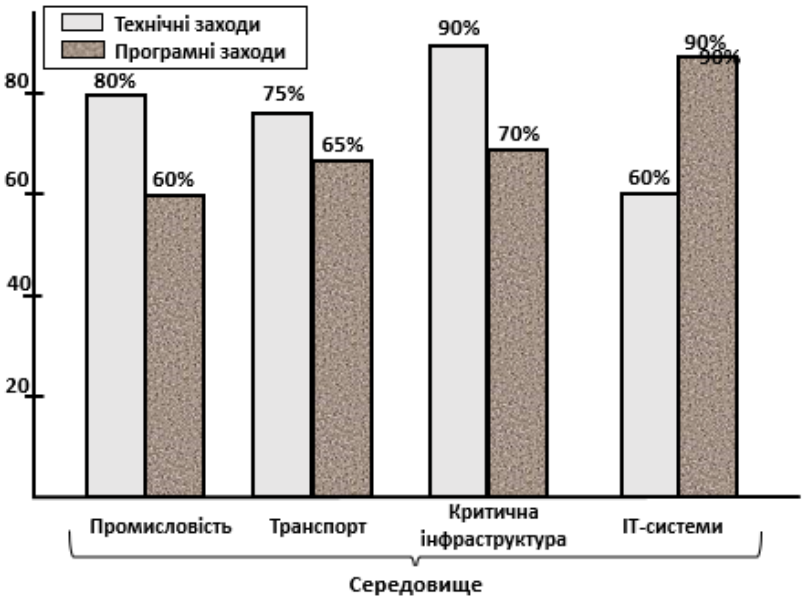

Рис. 2.1.Ефективність застосування технічних та програмних заходів безпеки у різних середовищах.

Комбінування технічних та програмних засобів дозволяє досягти більш високого рівня захищеності технічних систем. Постійний розвиток технологій вимагає адаптивних підходів до вибору та інтеграції засобів захисту.

2.3. Інформаційна безпека в технічних системах: апаратний та мережевий рівень

Інформаційна безпека в технічних системах є основою для забезпечення цілісності, конфіденційності та доступності даних, що обробляються такими системами. Безпека інформації виступає не лише як запобігання несанкціонованому доступу до да-

них, але й як захист від різноманітних загроз, які можуть вплинути на функціонування системи в цілому [33, с. 22]. Враховуючи постійне зростання кількості кібератак і зловмисних дій, стає очевидною необхідність комплексного підходу до забезпечення безпеки, який включає не лише захист програмних засобів, а й детальну увагу до специфіки апаратного та мережевого рівнів технічних систем.

Технічні системи, особливо критичні інфраструктури, такі як енергетичні, транспортні, телекомунікаційні та медичні мережі, мають особливу важливість у контексті забезпечення безпеки, адже їхнє порушення або виведення з ладу може призвести до серйозних економічних, соціальних та навіть гуманітарних наслідків [34, с. 18]. Такі системи повинні бути захищені від атак, які можуть не лише порушити їхнє функціонування, але й викликати витік або знищення чутливої інформації, що може мати фатальні наслідки для національної безпеки та стабільності суспільства в цілому.

Враховуючи складність сучасних технічних систем, забезпечення інформаційної безпеки потребує синергії на всіх рівнях архітектури системи. Апаратний рівень, на якому зберігаються та обробляються дані, потребує спеціальних засобів захисту, таких як апаратні модулі шифрування, захищені процесори, фізичні блокування доступу до серверів та мереж, а також системи моніторингу, що дозволяють вчасно виявити та локалізувати спроби несанкціонованого доступу. Ключовим аспектом на цьому рівні є також забезпечення цілісності обладнання, оскільки навіть найменші фізичні модифікації можуть привести до серйозних вразливостей у системі [42, с. 38].

Мережевий рівень є не менш важливим у контексті захисту технічних систем. Мережі є основним каналом для передавання даних і одночасно найбільш уразливою частиною системи, оскільки через них здійснюється доступ до різноманітних елементів та підсистем. Захист мережевого рівня включає в себе використання шифрування переданих даних, впровадження багатофакторної аутентифікації, виявлення та блокування мережевих атак (таких як DoS/DDoS, Man-in-the-Middle, MITM) за допомогою спеціалізованих засобів, зокрема систем виявлення та запобігання вторгненням (IDS/IPS). Також критично важливою є пра-

вильна конфігурація мережевих протоколів та налаштування безпеки на кожному рівні взаємодії мережевих пристроїв.

Інтеграція заходів безпеки на апаратному та мережевому рівнях є ключем до досягнення загальної безпеки технічних систем. Це включає в себе не лише індивідуальні заходи захисту, але й їхню взаємодію для створення надійної системи оборони [56, с. 1-3]. Наприклад, використання апаратного шифрування для зберігання даних в поєднанні з мережевими рішеннями для захисту передавання даних дозволяє забезпечити надійний захист на всіх етапах обробки інформації. Водночас, системи моніторингу повинні бути здатні здійснювати контроль за станом як апаратних, так і мережевих компонентів у реальному часі, що дозволяє своєчасно виявляти аномалії та потенційні загрози.

В умовах сучасних загроз інформаційній безпеці важливо враховувати, що кібератаки можуть бути настільки складними та різноманітними, що навіть найсучасніші засоби захисту повинні бути постійно оновлювані та вдосконалювані. Тому інтеграція програмних, апаратних та мережевих засобів безпеки має бути організована як динамічна та адаптивна система, яка реагує на нові загрози та вчасно коригує стратегію захисту. Це дозволяє забезпечити постійну готовність технічних систем до будь-яких викликів, що виникають в умовах глобальної цифрової трансформації та зростаючої кіберзагрози.

2.3.1. Апаратний рівень інформаційної безпеки

1) Фізичні засоби захисту

Апаратний рівень захисту є фундаментальним елементом загальної стратегії забезпечення безпеки технічних систем, оскільки він безпосередньо впливає на захист від фізичних загроз та несанкціонованого доступу до критично важливих компонентів [23, с. 78; 50, с. 2-3]. Оскільки саме на апаратному рівні здійснюється взаємодія між фізичними пристроями та іншими шарами безпеки (наприклад, програмними засобами), забезпечення належного рівня захисту на цьому рівні є необхідною умовою для ефективного функціонування всього системного комплексу [25, с. 46].

а) Контроль доступу

Одним із основних аспектів апаратного захисту є контроль доступу до фізичних пристроїв. Це забезпечується за допомогою систем, які відповідають за авторизацію та аутентифікацію користувачів перед наданням їм доступу до технічних компонентів системи. Механізми контролю доступу можуть включати такі технології, як біометричні системи, які здійснюють ідентифікацію за допомогою відбитків пальців, сканування райдужної оболонки ока чи розпізнавання обличчя. Такі системи значно підвищують рівень безпеки, оскільки вони ускладнюють доступ до пристроїв навіть за наявності фізичних ключів доступу.

Інші засоби контролю доступу, які також використовуються на апаратному рівні, включають смарт-карти та спеціальні ключі доступу. Смарт-карти, що вбудовуються в систему, дозволяють здійснити аутентифікацію користувача через криптографічний захист, який надає значно вищий рівень безпеки порівняно з традиційними паролями. Ключі доступу, як правило, використовуються для фізичної ідентифікації, що гарантує, що тільки уповноважена особа може отримати доступ до критичних системних компонентів.

b) Шифрування на рівні апаратних засобів

Для забезпечення безпеки даних на апаратному рівні важливим елементом є шифрування, яке здійснюється безпосередньо за допомогою апаратних засобів. Одним з найпоширеніших механізмів для цього є TPM (Trusted Platform Module) — апаратний чіп, який інтегрується в материнську плату або інший елемент апаратної системи. TPM дозволяє забезпечити збереження криптографічних ключів, що використовуються для захисту даних, таких як паролі, сертифікати або інші конфіденційні відомості. Завдяки цьому забезпечується захист на фізичному рівні, навіть якщо операційна система або програмне забезпечення були скомпрометовані.

Додатково, TPM може використовуватися для забезпечення цілісності системи під час завантаження операційної системи. Це означає, що кожен етап завантаження перевіряється на відповідність перед тим, як завантажувані компоненти будуть виконуватися. Така технологія здатна перешкодити атакам на стадії завантаження, коли зловмисники можуть намагатися втрутитися в роботу системи.

c) Фізичний захист носіїв інформації

Важливою частиною апаратного захисту є забезпечення безпеки фізичних носіїв інформації, таких як жорсткі диски, SSD, флеш-накопичувачі тощо. Оскільки ці носії можуть містити чутливу або критично важливу інформацію, необхідно використовувати спеціальні технології, які забезпечують їхню безпеку у разі фізичної втрати або викрадення пристроїв.

Одним з таких механізмів є шифрування дисків. Наприклад, програми, такі як BitLocker для Windows або LUKS для Linux, надають можливість здійснити шифрування всього вмісту диска. Вони використовують апаратні ресурси, такі як TPM-чіпи, для зберігання ключів шифрування, що ускладнює доступ до даних без належного дозволу. У разі втрати або крадіжки пристрою, дані залишаються зашифрованими і, відповідно, недоступними для неавторизованих користувачів. Схема моделей захисту на апаратному та мережевому рівнях наведена на Рис. 2.2.

Рис. 2.2. Схема моделей захисту на апаратному та мережевому рівнях.

Також важливою складовою захисту є використання **фізичних бар'єрів** та **антивандальних корпусів**, що робить неможливим доступ до внутрішніх компонентів пристроїв без їх пошкодження. Ці елементи фізичного захисту можуть включати

спеціальні корпуси, замки чи інші засоби, які забезпечують надійний захист від маніпуляцій.

Загалом, апаратний рівень захисту є не тільки необхідним етапом у забезпеченні безпеки, але й важливим інструментом для захисту даних від фізичних загроз, таких як крадіжка, маніпуляції або несанкціонований доступ

2) Безпека вбудованих систем

Вбудовані системи, зокрема ті, що працюють в рамках Інтернету речей (IoT), потребують особливої уваги до безпеки через їх взаємодію з фізичними об'єктами та їх безпосередній контакт з навколишнім середовищем. Ці системи часто обробляють конфіденційну інформацію і взаємодіють з критичними інфраструктурами, що робить їх вразливими до різноманітних загроз. Ось кілька основних аспектів, що визначають безпеку вбудованих систем.

a) Захист мікроконтролерів та сенсорів

Мікроконтролери та сенсори є основними компонентами вбудованих систем, і їх захист від несанкціонованого доступу є ключовим завданням. Враховуючи те, що ці елементи можуть працювати в умовах обмежених ресурсів і при цьому часто мають підключення до відкритих мереж, необхідно застосовувати багаторівневі методи захисту. Окрім стандартних методів шифрування, варто використовувати апаратні рішення, такі як безпечні мікросхеми або криптографічні процесори, які забезпечують захист на апаратному рівні. Програмні механізми, що використовують алгоритми шифрування та захищені канали зв'язку, додають додатковий рівень захисту, забезпечуючи безпеку при обміні даними між пристроями та хмарними сервісами або іншими системами.

b) Автентифікація пристроїв

У разі застосування IoT-систем важливо забезпечити механізми автентифікації пристроїв для запобігання несанкціонованому доступу або підміні пристроїв. Використання сильних криптографічних протоколів для аутентифікації забезпечує захист від спроб несанкціонованого підключення або атаки на рівні пристроїв. Такі системи, як mutual TLS (Transport Layer Security) або використання сертифікатів на основі PKI (Public Key Infrastructure), дозволяють забезпечити перевірку ідентичності

кожного пристрою в мережі, що є критичним для безпеки IoT. Окрім того, кожен пристрій повинен мати унікальні ідентифікатори для підвищення рівня безпеки та запобігання їх клону.

3) Захист даних на фізичних носіях

Дані, що зберігаються на фізичних носіях, завжди піддаються потенційному ризику втрати, крадіжки або маніпуляцій. Це особливо актуально для таких пристроїв, як жорсткі диски, USB-накопичувачі або сервери, на яких зберігаються конфіденційні дані. Для забезпечення належного рівня захисту необхідно застосовувати комплексний підхід до захисту даних, що включає як шифрування, так і фізичні заходи безпеки.

a) Шифрування даних

Шифрування є найефективнішим способом захисту даних на фізичних носіях. Алгоритми шифрування, такі як AES (Advanced Encryption Standard) або RSA, використовуються для забезпечення конфіденційності та цілісності інформації. Шифрування на рівні диска (Full Disk Encryption) забезпечує, що навіть у разі викрадення носія даних, доступ до інформації без наявності ключа шифрування буде неможливим. Вибір шифрувального алгоритму залежить від вимог до швидкості, рівня захисту та обмежень ресурсу.

b) Захист від фізичних пошкоджень

Окрім програмних методів шифрування, важливо застосовувати заходи для фізичного захисту носіїв інформації. Це можуть бути апаратні токени для доступу до даних, що гарантують лише авторизованим користувачам доступ до збережених даних. Також для забезпечення надійного захисту важливо використовувати захищені кабелі для підключення пристроїв, які унеможливлюють несанкціоновану перехоплення даних під час передачі. Спеціальні сейфи для зберігання важливих носіїв, а також використання технологій фізичної мітки, таких як RFID, додають ще один рівень захисту від фізичних загроз.

4) Аналіз загроз апаратного рівня

Загрози на апаратному рівні становлять серйозну небезпеку для безпеки технічних систем, оскільки фізичний доступ до пристроїв може призвести до значних порушень їх функціональності, а також до витоку конфіденційних даних або навіть маніпуляцій з ними. Ось основні загрози, що виникають на апаратному рівні:

a) Фізичний доступ до пристроїв

Найбільш очевидною загрозою є фізичний доступ до пристроїв, що дозволяє зловмисникам втручатися в роботу системи, змінювати її конфігурацію або навіть викрадати дані. Така загроза особливо актуальна для вбудованих систем, що працюють в обмежених або віддалених умовах. Захист від таких загроз включає використання спеціальних корпусів, які ускладнюють доступ до апаратних компонентів, а також застосування технологій замикання, які дозволяють виявляти спроби несанкціонованого доступу.

Фізичний доступ до комп'ютерної техніки є однією з найбільш серйозних загроз для безпеки інформаційних систем. Якщо зловмисник здатний отримати фізичний доступ до пристрою, він може здійснити низку атак, що виводять з ладу захисні механізми системи. Це може бути як прямий доступ до серверів чи комп'ютерів, так і до більш специфічних компонентів, таких як чіпи, процесори чи пам'ять.

Наприклад, зловмисник може скористатися можливістю перепрограмувати мікроконтролери або чипи, внаслідок чого з'являються ризики зміни функціональності пристрою або навіть створення "задніх дверей", через які він може знову отримати доступ до системи. Такі зміни можуть залишатися непоміченими для програмного забезпечення і викликати серйозні наслідки, включаючи викрадення або корупцію даних.

Один з класичних прикладів цієї загрози — використання апаратних чіпів для введення шкідливого коду. Цей код може бути активований після установки чіпа на цільовий пристрій і здійснити атаку на програмне забезпечення, приховуючи своє існування.

b) Маніпуляція з компонентами

Зловмисники можуть намагатися маніпулювати компонентами апаратного забезпечення, наприклад, шляхом зміни конфігурації мікросхем або встановлення шкідливого програмного забезпечення на рівні апаратного забезпечення. Захист від такої загрози включає використання апаратних засобів захисту, таких як Trusted Platform Module (TPM), що дозволяє перевіряти надійність системи та виявляти будь-які зміни на рівні апаратних компонентів.

c) Фізичні модифікації пристроїв

Інший важливий вид загрози — це фізичні модифікації пристроїв. Зловмисники можуть застосовувати різні методи для фізичного втручання в апаратне забезпечення, спричиняючи тим самим порушення його нормальної роботи або дозволяючи отримати доступ до даних. Це може включати в себе зміну компонентів або їх заміну, виведення з ладу системи живлення або встановлення сторонніх пристроїв, які можуть записувати або модифікувати інформацію.

Прикладом такої модифікації є встановлення "логічних шкідливих чіпів" (так званих "hardware implants"), які можуть бути вставлені в комп'ютер або інші пристрої під час виготовлення або ремонту. Ці чіпи можуть здобувати дані з пам'яті пристрою або навіть маніпулювати програмним забезпеченням, що працює на системі, надаючи зловмисникам доступ до важливої інформації.

Такі фізичні маніпуляції можуть бути складно виявлені, оскільки часто їх результат стає помітним лише в момент атаки. Вони можуть стати причиною серйозних уразливостей у системах, що використовують такі пристрої, зокрема, у системах з високими вимогами до безпеки, як от у фінансових або державних установах.

Загрози на апаратному рівні є особливо небезпечними, оскільки вони вимагають від зловмисників мінімуму технологічних знань і дозволяють обійти традиційні програмні засоби захисту. Важливим заходом для захисту від таких загроз є забезпечення фізичної безпеки технічних пристроїв, а також використання додаткових методів захисту, таких як шифрування на рівні апаратного забезпечення та регулярні перевірки компонентів на наявність можливих змін чи модифікацій.

2.3.2. Мережевий рівень інформаційної безпеки

1) Мережеві атаки

Мережеві атаки є одним із найпоширеніших видів загроз для інформаційної безпеки в сучасному цифровому середовищі [27, с. 52]. Вони спрямовані на порушення конфіденційності, цілісності та доступності інформації, що передається через мережеві канали [23, с. 152]. Оскільки кількість користувачів інтернету та мережевих пристроїв постійно зростає, ризик мереже-

вих атак значно збільшується. Нижче розглянемо основні типи мережевих атак та їх характерні риси [25, с. 88].

а) DDoS-атаки (розподілені атаки на відмову в обслуговуванні)

DDoS-атаки (Distributed Denial of Service) спрямовані на виснаження ресурсів цільового сервера або мережі шляхом одночасного надсилання великої кількості запитів з різних джерел. Мета таких атак — зробити онлайн-сервіс або вебсайт недоступним для користувачів.

Механізм реалізації

DDoS-атаки здійснюються шляхом залучення ботнетів — мереж зламаних пристроїв (ботів), які без відома власників генерують масові запити до цільового ресурсу. Це може призвести до перевантаження серверів, вичерпання пропускної здатності каналу або виснаження обчислювальних ресурсів системи.

Основні види DDoS-атак:

- Атаки на рівні мережі (UDP-флуд, ICMP-флуд): спрямовані на перевантаження мережевих каналів.
- Атаки на рівні прикладного програмного забезпечення (HTTP-флуд): спрямовані на виснаження ресурсів веб-сервера через надмірну кількість запитів.
- Атаки на протокольному рівні (SYN-флуд): створюють велику кількість незавершених з'єднань, блокуючи легітимний трафік.

Наслідки

Основний результат DDoS-атаки — часткова або повна недоступність ресурсу, що може призвести до фінансових втрат, втрати репутації та пошкодження інфраструктури.

b) Атаки типу «людина посередині» (MITM)

Атаки типу MITM (Man-in-the-Middle) дозволяють зловмиснику непомітно втрутитися в комунікацію між двома сторонами. Метою може бути перехоплення, зміна або спотворення даних, що передаються.

Механізм реалізації

Зловмисник встановлює контроль над каналом передачі даних, створюючи враження, що сторони спілкуються напряму. Це може бути досягнуто шляхом підробки сертифікатів SSL/TLS або використання підроблених точок доступу Wi-Fi.

Основні види MITM-атак:

a) ARP-спуфінг: підміна ARP-записів для перенаправлення трафіку.

b) DNS-спуфінг: зміна DNS-записів для перенаправлення користувачів на фальшиві сайти.

c) Wi-Fi-захоплення: злом бездротових мереж та створення підроблених точок доступу.

d) HTTP-проксі-атаки: використання шкідливих проксі-серверів для збору конфіденційних даних.

Наслідки

MITM-атаки призводять до крадіжки конфіденційної інформації (паролів, фінансових даних), фальсифікації транзакцій та компрометації систем безпеки.

c) SQL-ін'єкції

Ці атаки спрямовані на веб-додатки та бази даних з метою отримання несанкціонованого доступу або виконання шкідливого коду.

SQL-ін'єкція полягає у впровадженні шкідливих SQL-запитів через вразливі поля вводу даних на веб-сторінках. Це дозволяє зловмиснику отримати доступ до бази даних, модифікувати або видалити записи, обійти аутентифікацію. Приклад атаки наведено на Рис. 2.2.

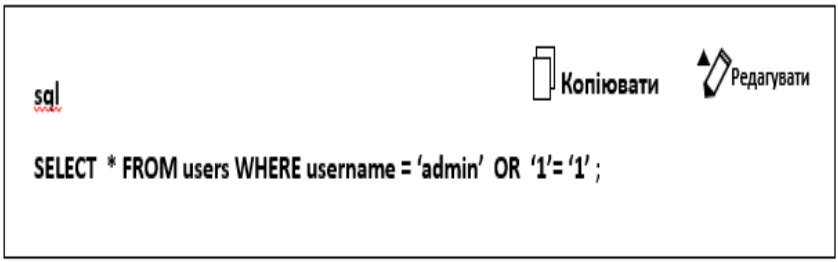

Рис. 2.2. Приклад атаки.

Такий запит дозволяє обійти перевірку на вході та отримати права адміністратора.

d) XSS-атаки (Cross-Site Scripting)

Ці атаки, як і SQL-ін'єкції, спрямовані на веб-додатки та бази даних з метою отримання несанкціонованого доступу або виконання шкідливого коду.

XSS-атака передбачає впровадження шкідливого коду (зазвичай JavaScript) у веб-сторінки, що дозволяє виконати скрипт на пристрої жертви. Зловмисники можуть отримати доступ до cookies, облікових даних або перенаправити користувача на шкідливий сайт.

Наслідки

SQL-ін'єкції призводять до витоку або модифікації даних, а XSS-атаки — до викрадення сесій користувачів та подальшого компрометування облікових записів.

2) Профілактика мережевих атак

a) Моніторинг та аналіз трафіку: використовувати системи виявлення та запобігання вторгненням (IDS/IPS).

b) Шифрування даних: впровадження сучасних протоколів (HTTPS, TLS) для захисту переданих даних.

c) Регулярні оновлення ПЗ: усунення вразливостей у програмному забезпеченні.

d) Фільтрація вхідних даних: використання підходів до безпечного введення, таких як регулярні вирази та перевірка на відповідність формату.

e) Використання міжмережевих екранів та проксі-серверів: для ізоляції внутрішньої мережі від зовнішніх загроз.

Мережеві атаки залишаються серйозною загрозою для інформаційної безпеки, вимагаючи комплексного підходу до захисту. Сучасні методи захисту включають як технічні засоби (IDS/IPS, міжмережеві екрани), так і організаційні заходи (підвищення кваліфікації співробітників та регулярний моніторинг інцидентів). Усвідомлення типів атак та способів їх запобігання є важливим аспектом забезпечення кібербезпеки сучасних технічних систем. З більш докладною картою мережевих атак можна ознайомитись на Рис. 2.3.

3) Мережеві протоколи і їх безпека

Для захисту даних, що передаються по мережах, використовуються різні протоколи:

a) VPN (Virtual Private Network): Забезпечує захищений канал для передачі даних між клієнтом і сервером, що дозволяє приховати трафік від сторонніх осіб;

b) SSL/TLS: Протоколи, які використовуються для захисту веб-з'єднань, шифруючи передану інформацію;

c) IPsec: Протокол, що забезпечує захист даних на мережевому рівні шляхом шифрування IP-пакетів;

d) IDS/IPS (Intrusion Detection/Prevention Systems): Системи для виявлення та запобігання несанкціонованим вторгненням.

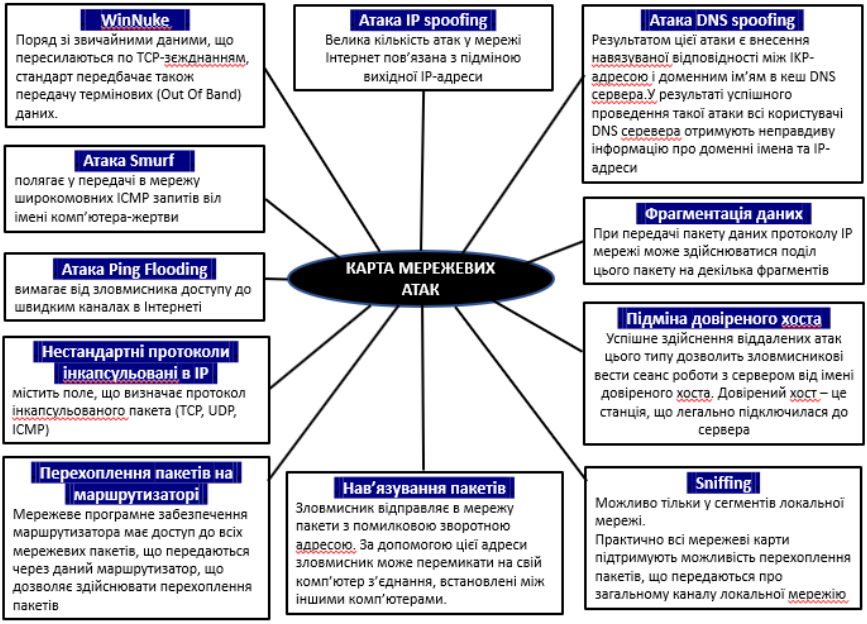

Рис. 2.3. Схеми мережевих атак.

d) IDS/IPS (Intrusion Detection/Prevention Systems): Системи для виявлення та запобігання несанкціонованим вторгненням.

4) Захист від атак на прикладному рівні

Атаки на прикладному рівні можуть серйозно порушити безпеку системи. Для їх запобігання використовуються різноманітні технічні заходи:

a) Антифішинг: захист від фальшивих веб-сайтів і електронних листів.

b) Аналіз вразливостей веб-додатків: використання механізмів безпеки для забезпечення захисту від SQL-ін'єкцій та XSS-атак.

***5) Ідентифікація* та автентифікація в мережах**

Для забезпечення доступу до мережевих ресурсів важливо використовувати такі методи:

a) Двофакторна аутентифікація (2FA): Методи подвійної перевірки користувачів перед наданням доступу до системи.

b) Рольова модель доступу: Забезпечує диференційований доступ до системних ресурсів залежно від ролі користувача.

6) Безпека при передаванні даних

Основні методи шифрування при передачі даних:

a) SSL/TLS для захисту веб-трафіку.

b) IPsec для захисту мережевого трафіку.

c) Зашифровані канали для обміну критично важливою інформацією (наприклад, для банківських або урядових органів).

2.3.3. Спільні питання апаратного та мережевого рівня інформаційної безпеки

1) Інтеграція безпеки на обох рівнях

Інтеграція апаратного і мережевого захисту дозволяє створити цілісну систему безпеки, що включає використання фаєрволів, IDS/IPS-систем, шифрування даних на всіх етапах — від пристроїв до мережевих каналів.

2) Безпека у контексті взаємодії мережевих і апаратних компонентів

Важливо забезпечити взаємодію між апаратними і мережевими компонентами для створення безпечних систем, які можуть ефективно захищатися від зовнішніх і внутрішніх загроз [48, с. 1-3].

Інструменти та технології для забезпечення інформаційної безпеки

Захист технічних систем потребує використання різних інструментів:

a) Програмне забезпечення для моніторингу та виявлення атак: Використовуються інструменти для моніторингу трафіку і виявлення аномалій.

b) Антивірусні та антивірусні програми: Засоби для виявлення і знешкодження шкідливих програм.

c) Шифрування даних: Використання сучасних криптографічних методів для захисту даних на всіх етапах їх обробки та передачі.

Цей підрозділ охоплює всі аспекти забезпечення інформаційної безпеки технічних систем на апаратному та мережевому рівнях, допомагаючи читачу зрозуміти ключові методи та інструменти для захисту критичних інфраструктур

2.4. Стандартизація безпеки технічних систем (ISO/IEC, NIST)

У сучасному світі забезпечення безпеки технічних систем є критично важливим завданням для будь-якої галузі діяльності. Технічні системи, що використовуються в промисловості, енергетиці, транспорті, інформаційних технологіях та інших сферах, є ключовими компонентами сучасної інфраструктури. Їхня безпека безпосередньо впливає на стійкість роботи організацій, національну безпеку та життя людей.

Стандартизація безпеки є невід'ємним елементом цього процесу, оскільки вона надає чіткі вимоги та рекомендації щодо захисту технічних об'єктів від загроз, вразливостей та ризиків. Завдяки стандартизації створюється єдиний підхід до забезпечення безпеки, що дозволяє мінімізувати ризики та ефективно керувати ними. Стандарти визначають критерії безпечної експлуатації систем, процедури ідентифікації ризиків, методи оцінки уразливостей та заходи з усунення небезпек.

Розробка ефективної системи забезпечення безпеки технічних систем передбачає використання міжнародних стандартів, що регламентують управління інформаційною безпекою та технічним захистом інфраструктури.

Застосування міжнародних стандартів дозволяє організаціям інтегрувати передові практики управління безпекою, що сприяє підвищенню довіри з боку клієнтів та партнерів. Таким чином, стандартизація стає основою забезпечення надійності та безпеки технічних систем, що є надзвичайно важливим у сучасному глобалізованому світі.

Найбільш визнаними та широко використовуваними є стандарти ISO/IEC та рекомендації NIST.

2.4.1. Система управління інформаційною безпекою ISO/IEC 27001:2013

Одним із ключових міжнародних стандартів у цій галузі є ISO/IEC 27001, який встановлює вимоги до систем управління інформаційною безпекою. Він включає принципи захисту конфіденційності, цілісності та доступності даних. Також важливими є стандарти серії NIST (National Institute of Standards and Technology), які регламентують технічні та організаційні заходи безпеки, включаючи управління ризиками та реагування на інциденти [15, с. 1; 52, с. 1].

ISO/IEC 27001:2013 є міжнародним стандартом, що визначає вимоги до створення, впровадження, підтримки та безперервного вдосконалення системи управління інформаційною безпекою (СУІБ). Основною метою цього стандарту є захист конфіденційності, цілісності та доступності інформації шляхом управління ризиками безпеки [16, с. 1].

Основні принципи стандарту:

a) Безперервне вдосконалення: впровадження циклу PDCA (Plan-Do-Check-Act) для постійного покращення системи.

b) Управління ризиками: ідентифікація, оцінка та мінімізація ризиків інформаційної безпеки.

c) Дотримання нормативних вимог: відповідність міжнародним та національним правовим актам.

***Застосування*:** Стандарт застосовується у корпоративному секторі, державних установах, фінансових організаціях, освітніх та наукових закладах. Він забезпечує єдину основу для управління ризиками інформаційної безпеки в умовах складної цифрової інфраструктури.

2.4.2. Система управління інформаційною безпекою NIST

Національний інститут стандартів і технологій США (NIST) розробляє рекомендації та настанови з безпеки технічних систем. Зокрема, у сфері управління ризиками та захисту інформаційної інфраструктури особливу увагу приділено серії спеціальних публікацій (SP).

***Основні документи*:**

a) NIST SP 800-53: містить перелік контролів безпеки для організацій урядового сектору США.

b) NIST SP 800-82: присвячений безпеці промислових систем, включаючи системи керування технологічними процесами (ICS).

***Застосування*:** Ці стандарти широко використовуються урядовими та комерційними організаціями США для побудови ефективної системи захисту інформації та технічних систем. Завдяки рекомендаціям NIST вдається мінімізувати ризики кібератак на критичну інфраструктуру.

Міжнародні стандарти ISO/IEC та рекомендації NIST забезпечують комплексний підхід до управління безпекою технічних систем. Їх впровадження дозволяє підвищити рівень захищеності інформаційних ресурсів як у державному, так і в приватному секторах. Порівняння зазначених стандартів безпеки можна здійснити на підставі даних, що наведені у таблиці 2.4.

Таблиця 2.4. Особливості основних стандартів безпеки

Стандарт	**Основна мета**	**Область застосування**	**Особливості**
ISO/IEC 27001	Управління інформаційною безпекою	Корпоративний сектор, державні установи	Управління ризиками, безперервне вдосконалення
NIST SP 800-53	Контроли безпеки для інформаційних систем	Урядові та комерційні організації США	Модель управління на основі ризиків

Стандартизація безпеки технічних систем є важливим аспектом сучасного управління ризиками та забезпечення надійності технічної інфраструктури. З огляду на зростання складності технічних систем та зростаючі загрози кібербезпеки, впровадження міжнародних стандартів стає обов'язковою умовою для підтримання високого рівня захисту.

Основною метою стандартизації є створення єдиних вимог до організації безпеки, що дозволяє уніфікувати підходи до захисту технічних систем. Міжнародні стандарти, такі як ISO/IEC 27001,

NIST SP 800-53 та інші, забезпечують комплексне охоплення різних аспектів безпеки, включаючи управління ризиками, безпеку інформаційних потоків, кіберзахист та фізичний захист об'єктів.

Інтеграція міжнародних стандартів у процеси забезпечення безпеки дозволяє створити комплексний захист на різних рівнях технічної інфраструктури. Зокрема, стандарти ISO/IEC серії 27000 охоплюють аспекти інформаційної безпеки, що дозволяє знизити ризики втрати конфіденційних даних. Стандарти NIST, у свою чергу, акцентують увагу на управлінні кіберризиками та безпеці критичної інфраструктури.

Однією з переваг стандартизації є можливість інтеграції системи управління безпекою в загальні процеси управління організацією. Це дозволяє ефективно поєднувати заходи захисту з іншими бізнес-процесами, що сприяє підвищенню надійності та стійкості технічних систем до зовнішніх та внутрішніх загроз.

Таким чином, стандартизація безпеки технічних систем сприяє ефективному управлінню ризиками та дозволяє формувати стійкі механізми захисту на різних рівнях технічної інфраструктури. Впровадження міжнародних стандартів підвищує надійність систем, забезпечуючи їхню адаптацію до сучасних викликів у сфері безпеки.

Контрольні питання

1. Які основні методи використовуються для ідентифікації ризиків у технічних системах?
2. У чому полягає відмінність між якісною та кількісною оцінкою уразливостей?
3. Які основні етапи включає аналіз ризиків технічних систем?
4. Як проводиться SWOT-аналіз у контексті оцінки ризиків?
5. Що таке метод дерев ризику і як він застосовується в аналізі безпеки?
6. Які критерії ефективності використовуються при оцінці уразливостей технічних систем?

7. Чим відрізняється метод аналізу ризику на основі сценаріїв від методу на основі статистичних даних?

8. Які методи оцінки ризиків є найбільш доцільними для складних технічних систем?

9. Які основні технічні засоби використовуються для захисту технічних систем?

10. Які програмні засоби є найбільш ефективними для виявлення кіберзагроз у технічних системах?

11. У чому полягає різниця між апаратними та програмними засобами захисту?

12. Як здійснюється моніторинг безпеки технічних систем у режимі реального часу?

13. Які методи застосовуються для виявлення та запобігання вторгненням у технічні системи?

14. Як антивірусні програми інтегруються з системами захисту на апаратному рівні?

15. Які фактори впливають на вибір засобів захисту технічних систем?

16. Які підходи застосовуються до тестування захисних систем на стійкість до атак?

17. Які основні загрози інформаційній безпеці на апаратному рівні технічних систем?

18. Які принципи побудови захищених мереж використовуються для забезпечення інформаційної безпеки?

19. Як здійснюється управління доступом на апаратному рівні?

20. Які методи захисту від атак типу "відмова в обслуговуванні" (DoS) застосовуються на мережевому рівні?

21. Які апаратні засоби захисту використовуються для запобігання витоку даних?

22. Яким чином шифрування впливає на безпеку технічних систем на мережевому рівні?

23. Які ризики виникають під час інтеграції різних апаратних засобів у єдину мережу безпеки?

24. Які основні стандарти ISO/IEC використовуються для забезпечення безпеки технічних систем?

25. Як підхід NIST до управління ризиками може бути адаптований для технічних систем?

РОЗДІЛ 3. ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ТА ТРЕНДИ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ТЕХНІЧНИХ СИСТЕМ

3.1. Інтернет речі та кіберфізичні системи: виклики безпеці технічних систем

Інтернет речі (IoT) та кіберфізичні системи (КФС) стають все більш поширеними у різних галузях, що призводить до суттєвих змін у структурі та функціонуванні технічних систем. Їх інтеграція створює нові можливості для підвищення ефективності процесів, автоматизації та моніторингу, але водночас формує нові виклики у сфері безпеки. Розглянемо основні аспекти, пов'язані з безпекою технічних систем в умовах широкого впровадження IoT та КФС.

Розробити більш розгорнутий текстовий опис щодо нижче вказаного матеріалу, а саме:

3.1.1. Поняття та архітектура інтернету речей та кіберфізичних систем

Інтернет речі (Internet of Things, IoT) — це мережа фізичних об'єктів (речей), які оснащені сенсорами, програмним забезпеченням та іншими технологіями для взаємодії та обміну даними з іншими пристроями та системами через інтернет [39, с. 12; 62, с. 1-4].

Кіберфізичні системи (КФС) являють собою інтеграцію обчислювальних, мережевих та фізичних процесів, де комп'ютерні алгоритми взаємодіють з фізичним середовищем у реальному часі.

1) Основні компоненти IoT:

a) Пристрої збору даних (сенсори та актуатори)

b) Мережеві інтерфейси та протоколи

c) Хмарні та периферійні обчислення

d) Аналітичні платформи та інтелектуальні системи

2) Основні компоненти кіберфізичних систем КФС:

a) Фізичні об'єкти з вбудованими обчислювальними модулями

b) Інтелектуальні керуючі системи

c) Захищені комунікаційні канали

d) Програмні модулі для аналізу та керування

3.1.2. Загрози безпеці інтернету речей та кіберфізичній системі.

Розглянемо основні ризики та уразливості, які виникають при використанні IoT та КФС у технічних системах.

1) Основні загрози інтернету речей:

a) Незахищені комунікаційні канали, що можуть призвести до перехоплення даних.

b) Використання небезпечних протоколів обміну інформацією.

c) Можливість фізичного доступу до пристроїв та їх компрометації.

d) Вразливості у вбудованому програмному забезпеченні та мікропрограмах.

2) Основні загрози кіберфізичній системі (КФС):

a) Кібератаки на інтелектуальні керуючі системи.

b) Підробка даних сенсорів або маніпуляція з фізичними параметрами.

c) Порушення інтеграції кібер- та фізичних компонентів.

d) Загрози безперебійного функціонування через збої в обчислювальних процесах.

3.1.3. Методи захисту інтернету речей та кіберфізичної системи.

Розробка методів захисту IoT та КФС є критично важливою для забезпечення безпеки технічних систем. Розглянемо основні підходи до забезпечення кібербезпеки в даних системах.

1) Технічні методи захисту технічних систем IoT та кіберфізичної системи:

a) Використання шифрування даних під час передачі та зберігання.

b) Аутентифікація та авторизація на основі багатоетапної верифікації.

c) Захист комунікаційних каналів за допомогою VPN та SSL/TLS протоколів.

d) Інтеграція інтелектуальних систем моніторингу та виявлення аномалій.

2) Організаційні методи захисту технічних систем IoT та кіберфізичної системи:

a) Розробка політик кібербезпеки з урахуванням специфіки IoT та кіберфізичної системи (КФС).

b) Підвищення обізнаності та навчання персоналу щодо безпеки.

c) Регулярний аудит та оцінка вразливостей системи.

d) Використання стандартів безпеки, таких як ISO/IEC 27001 та NIST SP 800-53.

IoT та КФС є важливими компонентами сучасних технічних систем, але їх впровадження супроводжується численними викликами у сфері безпеки. Розробка комплексних підходів до захисту є необхідною умовою забезпечення надійності та стійкості технічних систем у сучасних умовах.

3.2. Застосування штучного інтелекту та машинного навчання для виявлення загроз технічних систем

Розвиток штучного інтелекту (ШІ) та машинного навчання (МН) докорінно змінив підходи до забезпечення безпеки технічних систем. Завдяки здатності до автоматичного навчання, аналізу великих обсягів даних та виявлення складних шаблонів, ШІ та МН стали невід'ємною частиною сучасних методів захисту систем від кіберзагроз. В епоху кіберфізичних систем зростає значення динамічної адаптації засобів захисту до нових загроз. Це вимагає інтеграції ШІ та МН у всі рівні технічних систем [18, с. 1-3].

3.2.1. Основні напрями застосування штучного інтелекту та машинного навчання у технічних системах безпеки

***1) Виявлення кіберзагроз*:** ШІ аналізує потоки даних у режимі реального часу, виявляючи аномальні дії та можливі атаки. Машинне навчання використовується для ідентифікації шаблонів загроз на основі великих масивів даних.

2) Прогнозування атак: Використання глибоких нейронних мереж для виявлення прихованих загрозових факторів. Прогнозування на основі часових рядів із використанням рекурентних нейронних мереж (RNN).

***3) Автоматизоване реагування*:** Самонавчальні алгоритми забезпечують миттєву реакцію на виявлені загрози, блокуючи підозрілі дії.

5) Аналіз аномалій: Методи кластеризації та статистичного аналізу використовуються для виявлення відхилень від типової поведінки системи.

3.2.2. Алгоритми і моделі для виявлення загроз у технічних системах

1) Нейронні мережі: Використовуються для глибокого аналізу вхідних даних та виявлення складних патернів загроз.

2) Глибоке навчання: Забезпечує високу точність виявлення загроз на основі багаторівневої обробки даних.

3) Метод опорних векторів (SVM): Застосовується для класифікації нормальної та аномальної поведінки.

4) Кластерний аналіз: Дозволяє об'єднати подібні загрози в кластери для кращої ідентифікації.

5) Згорткові нейронні мережі (CNN): Ефективні для аналізу мережевого трафіку та виявлення атак на основі обробки візуалізованих даних.

6) Рекурентні нейронні мережі (RNN): Підходять для аналізу часових рядів безпеки, що дозволяє виявляти послідовні аномалії [60, с. 1-3].

3.2.3. Переваги використання ШІ та МН у технічних системах

1) Адаптивність: Системи постійно вдосконалюються завдяки навчанню на нових даних.

2) Швидкість реакції: Миттєве виявлення та блокування загроз.

3) Прогнозування нових загроз: Завдяки аналізу поведінкових патернів та автоматичному навчанні.

4) Інтелектуальне реагування: Використання алгоритмів з самонавчанням забезпечує високу ефективність реагування на нові виклики.

Застосування ШІ та МН у забезпеченні безпеки технічних систем є стратегічним кроком до побудови надійних та захищених інфраструктур. Інтелектуальні системи здатні оперативно адаптуватися до нових загроз, забезпечуючи високий рівень кіберзахисту. Інтеграція ШІ на всіх рівнях технічної системи сприяє підвищенню її стійкості та безперервному моніторингу можливих атак [21, с. 69; 63, с. 5].

3.2.4. Порівняльний аналіз ефективності методів штучного інтелекту та машинного навчання

Забезпечення безпеки технічних систем в умовах зростаючої кількості кіберзагроз потребує використання інноваційних технологій, серед яких особливу увагу привертають методи штучного інтелекту (ШІ) та машинного навчання (МН) [59, с. 1]. Одним із ключових завдань цих технологій є своєчасне виявлення загроз, що вимагає надійних методів аналізу великих обсягів даних у реальному часі.

1) Основні показники ефективності застосування ШІ та МН. Для об'єктивної оцінки ефективності застосування ШІ та МН у виявленні загроз використовуються кілька основних показників:

a) Точність (Accuracy) — показує відсоток правильно класифікованих випадків серед усіх розглянутих ситуацій. Висока точність свідчить про здатність алгоритму коректно ідентифікувати як загрозу, так і її відсутність.

b) Чутливість (Sensitivity) — відображає здатність системи виявляти всі реальні загрози, мінімізуючи кількість пропущених інцидентів. Висока чутливість є критичною при роботі з високоризиковими технічними системами.

c) Час реагування (Response Time) — характеризує швидкість прийняття рішення системою після отримання вхідних даних. Оптимальне значення цього показника особливо важливе для систем реального часу.

2) Порівняльний аналіз алгоритмів ШІ та МН

З огляду на різноманіття загроз, кожен алгоритм ШІ та МН демонструє різний рівень ефективності залежно від типу загрози та специфіки технічної системи. Проведення порівняльного аналізу алгоритмів дозволяє обрати найбільш оптимальні методи для конкретних завдань.

Методи та їх особливості:

a) Метод опорних векторів (Support Vector Machine, SVM) — ефективний при аналізі мережевих аномалій завдяки здатності класифікувати складні нелінійні дані. Висока точність досягається за рахунок побудови гіперплощин, що розділяють класи загроз.

b) Кластерний аналіз (Clustering Analysis) — добре підходить для виявлення нових та невідомих типів атак. Метод дозволяє

групувати дані за схожими ознаками, що сприяє виявленню аномалій без попереднього навчання на маркованих даних.

c) Глибоке навчання (Deep Learning) — застосовується для складних багатовимірних даних, наприклад, при аналізі поведінкових патернів користувачів у великих мережах. Завдяки нейронним мережам забезпечується гнучкість і висока адаптивність до нових загроз.

d) Байєсівський підхід (Bayesian Methods) — демонструє ефективність у прогнозуванні кіберзагроз на основі ймовірнісного аналізу. Найбільш результативний при оцінці ризиків на основі історичних даних.

Приклад практичного застосування алгоритмів.

У практичному середовищі, наприклад, для захисту мережевого сегмента критичної інфраструктури, доцільно використовувати комбінацію алгоритмів:

a) SVM забезпечує точність і швидкість реагування на відомі мережеві атаки.

b) Кластерний аналіз дозволяє оперативно виявляти нові аномалії, що можуть бути пов'язані з кібератаками типу Zero-Day.

c) Глибокі нейронні мережі використовуються для довгострокового аналізу змін у поведінці користувачів і виявлення потенційних внутрішніх загроз.

Вибір алгоритму ШІ та МН для виявлення загроз залежить від типу технічної системи, характеру загроз та вимог до часу реагування. Порівняльний аналіз ефективності алгоритмів дозволяє обрати оптимальне рішення, що забезпечує надійний захист технічних систем у динамічних умовах сучасного кіберпростору.

3.2.5. Виклики та обмеження впровадження штучного інтелекту та машинного навчання

1) Проблеми щодо впровадження штучного інтелекту (ШІ) та машинного навчання (МН)

Впровадження технологій штучного інтелекту (ШІ) та машинного навчання (МН) в технічні системи є потужним інструментом для забезпечення безпеки та ефективності роботи, однак цей процес супроводжується низкою викликів та обмежень. Одним з основних аспектів є складність навчання моделей на неповних або зашумлених даних. Моделі ШІ часто потребують вели-

ких обсягів даних для ефективного навчання, і якщо ці дані мають прогалини або містять шум (неважливу або зашумлену інформацію), то це може негативно впливати на точність і коректність результатів.

Ризик помилкових спрацьовувань також є важливою проблемою, особливо у критичних системах безпеки. Якщо система, що працює на основі ШІ, не здатна правильно класифікувати загрози або, навпаки, реагує на незначні, не шкідливі події як на серйозні загрози, це може призвести до фальшивих тривог або недостатньої реакції на реальні атаки. Це створює загрозу для ефективності функціонування системи та може спричинити значні втрати, особливо в умовах реального часу.

Потреба в ресурсах для обробки великих обсягів інформації також є суттєвим обмеженням. Навчання моделей ШІ та МН вимагає потужних обчислювальних ресурсів, зокрема графічних процесорів (GPU) та великих обсягів пам'яті. Це може бути економічно невигідним і складним для впровадження в певних сферах, особливо у мобільних або вбудованих системах, де доступ до потужних ресурсів обмежений.

Крім того, етичні питання відіграють важливу роль в розробці та впровадженні таких технологій. ШІ може ухвалювати рішення без участі людини, і при цьому виникає ризик ухвалення некоректних рішень, зокрема в ситуаціях, де важливі нюанси можуть бути непомітними для алгоритмів, а також у випадках, коли прийняття рішень є суб'єктивним. Тому необхідно розробляти механізми контролю та забезпечення прозорості алгоритмів, щоб гарантувати етичність їх застосування.

2) Приклади використання в реальних сценаріях штучного інтелекту (ШІ) та машинного навчання (МН)

У реальних умовах ШІ та МН активно використовуються для моніторингу та захисту технічних систем. Один із найбільш поширених сценаріїв застосування — це моніторинг мережевого трафіку. Моделі ШІ аналізують великі обсяги даних у реальному часі, дозволяючи виявляти аномалії, які можуть вказувати на спроби несанкціонованого доступу або зловмисні атаки. Це включає в себе виявлення спроб вторгнення, аналіз патернів поведінки в мережі, а також прогнозування можливих атак.

Іншим прикладом є аналіз логів системи. ШІ дозволяє автоматизувати процес вивчення великих обсягів системних журналів для виявлення аномалій, що можуть свідчити про шкідливу активність або внутрішні збої в роботі системи. Це значно підвищує ефективність та швидкість виявлення проблем, що критично важливо для забезпечення безпеки.

Також активно використовуються системи ШІ та МН для виявлення шкідливого програмного забезпечення. Глибоке навчання дозволяє розпізнавати нові, невідомі до цього види шкідливих програм, що може бути складним завданням для традиційних методів детекції. Системи, засновані на глибокому навчанні, здатні виявляти навіть найбільш складні типи атак, включаючи DDoS-атаки, в режимі реального часу, що дає можливість оперативно реагувати на загрози.

3) Перспективи розвитку технологій виявлення загроз із використанням штучного інтелекту (ШІ) в технічних системах

У майбутньому розвиток технологій ШІ у сфері виявлення загроз обіцяє значні покращення. Одним з найбільш перспективних напрямків є розробка автономних систем реагування на загрози, здатних адаптуватися до нових викликів з мінімальною участю людини. Такі системи зможуть самостійно аналізувати ситуацію, приймати рішення та виконувати відповідні дії для нейтралізації загроз, що значно підвищить оперативність та ефективність захисту.

Особлива увага приділяється розробці моделей з низьким енергоспоживанням, що є важливим для мобільних та вбудованих систем. Враховуючи зростаючі вимоги до мобільних технологій, створення енергоефективних алгоритмів дозволить забезпечити більш широкий спектр застосувань ШІ у технічних системах з обмеженими ресурсами. Це стане особливо важливим для сфер, де енергоспоживання є критичним фактором, таких як Інтернет речей (IoT) та вбудовані пристрої.

Також в майбутньому очікується зростання інтеграції ШІ з іншими передовими технологіями, такими як блокчейн, що дозволить створювати більш захищені та прозорі системи для виявлення та нейтралізації загроз. Інтеграція різних технологій дозволить створювати більш надійні та стійкі системи безпеки, що здатні адаптуватися до постійно змінюваних умов.

3.3. Технології блокчейн у технічному захисті технічних систем

У сучасному світі технічні системи стають дедалі складнішими, що призводить до зростання потреби в їх захисті.

Технології блокчейн, що зародилися у контексті криптовалют, все більше інтегруються у сферу технічної безпеки. Завдяки своїм унікальним характеристикам — децентралізації, криптографічному захисту та незмінності даних — блокчейн здатний забезпечити високий рівень безпеки технічних систем. Даний підрозділ досліджує можливості використання блокчейн-рішень для захисту технічних систем, аналізує їх переваги, недоліки, ризики та перспективи впровадження.

3.3.1. Застосування блокчейну у технічних системах

1) Основні принципи технології блокчейн у захисті систем

Технологія блокчейн представляє собою інноваційний підхід до зберігання і обробки даних, що базується на дистрибутивній структурі без єдиної точки відмови. Це забезпечує високу стійкість до атак, оскільки відсутність централізованого контролю знижує ризики, пов'язані з порушенням цілісності даних. Основний принцип блокчейну полягає у формуванні ланцюга блоків, кожен з яких містить певну кількість транзакцій, зашифрованих з використанням передових криптографічних методів. Це дозволяє забезпечити незмінність записів у реєстрі, що є важливим аспектом у контексті безпеки технічних систем, оскільки кожна спроба зміни даних буде виявлена.

Крім того, використання консенсусних алгоритмів, таких як Proof of Work (PoW) або Proof of Stake (PoS), дозволяє учасникам мережі погоджуватися щодо правдивості та достовірності даних, що зберігаються у блоках. Це гарантує цілісність інформації та відсутність підробок, оскільки кожен учасник мережі має доступ до копії реєстру, і будь-яка зміна в одному з блоків вимагатиме перерахунку даних у всіх інших. Ці принципи забезпечують надійний захист від маніпуляцій та атак, що може бути критичним для захисту важливих технічних інфраструктур.

2) Приклади використання блокчейну у технічному захисті

Одним із значущих застосувань технології блокчейн є управління доступом до промислових Інтернет речей (IoT) та різноманітних технічних систем. Зокрема, блокчейн може використовуватися для створення децентралізованих систем доступу, де всі записи про зміну статусу доступу будуть зафіксовані у вигляді блоків, що дає змогу проводити прозорий та незмінний аудит прав доступу. Такі системи дозволяють значно підвищити рівень безпеки, оскільки кожен доступ буде записано в реєстрі і неможливо буде змінити чи підробити інформацію без виявлення.

Крім того, блокчейн може бути застосований для захисту від фальсифікації даних у системах моніторингу технічного стану обладнання. Наприклад, у великих розподілених мережах, що здійснюють моніторинг роботи виробничих ліній або інших технічних інфраструктур, технологія дозволяє створювати надійний та прозорий реєстр зведених даних про стан обладнання. У випадку будь-якої спроби зміни або маніпуляції даними про технічний стан, така дія буде виявлена завдяки криптографічним методам захисту блокчейну, що дозволить оперативно відреагувати та запобігти непередбачуваним наслідкам.

3) Інтеграція блокчейн-технологій у сучасні технічні системи

Інтеграція блокчейн-технологій у вже існуючі технічні системи потребує значних зусиль не тільки в частині оновлення апаратної інфраструктури, але й адаптації програмного забезпечення, що супроводжує ці системи. Одним із основних викликів є забезпечення ефективної обробки великих обсягів даних у режимі реального часу. Блокчейн може стати потужним інструментом для обробки таких даних, але вимагає адаптації алгоритмів для забезпечення високої швидкості транзакцій і обробки даних.

У цьому контексті використання приватних або консорціумних блокчейнів може стати оптимальним рішенням для вузькоспеціалізованих завдань безпеки. Приватні блокчейни, на відміну від публічних, дозволяють обмежити доступ до даних лише для авторизованих учасників мережі, що забезпечує більшу конфіденційність і контроль за інформацією. Вони можуть викорис-

товуватися для специфічних завдань, де є необхідність в швидкій обробці даних і високій надійності системи. Таким чином, інтеграція блокчейну в сучасні технічні системи є перспективним напрямком, що дозволяє забезпечити ще вищий рівень безпеки та ефективності при збереженні цілісності і прозорості даних.

3.3.2. Порівняння блокчейну з іншими методами захисту

1) Криптографічний захист та блокчейн: спільне та відмінності

Криптографія є основним інструментом захисту інформації в сучасних цифрових технологіях, що забезпечує конфіденційність, цілісність та автентичність даних. Традиційні криптографічні методи, такі як симетричне та асиметричне шифрування, цифрові підписи, хеш-функції, використовуються для захисту переданих або збережених даних шляхом їх шифрування та автентифікації. Основними завданнями традиційної криптографії є гарантування того, що тільки уповноважені користувачі мають доступ до даних, а також підтвердження того, що дані не були змінені з моменту їх відправлення або збереження.

У цьому контексті блокчейн представляє собою новітній підхід до забезпечення захисту даних. Блокчейн поєднує традиційні принципи криптографії з інноваційними механізмами, такими як дистрибуція, консенсус та розподілене зберігання. Основна відмінність між традиційними криптографічними методами та блокчейном полягає в тому, що блокчейн, на відміну від централізованих систем, зберігає дані не в одному місці, а розподіляє їх серед численних учасників мережі [61, с. 2]. Це дозволяє забезпечити високий рівень прозорості, оскільки кожна зміна в даних реєструється в кожному з блоків, що є частиною блокчейн-мережі, і не може бути змінена без підтвердження більшості учасників.

З точки зору криптографії, блокчейн використовує хешування для забезпечення цілісності даних, цифрові підписи для автентифікації учасників мережі, а також консенсусні алгоритми для підтвердження транзакцій. Таким чином, блокчейн не лише шифрує та автентифікує дані, але й забезпечує прозорість і незмінність записів, що робить його потужним інструментом для досягнення високої надійності операцій.

2) Централізовані та децентралізовані підходи: блокчейн у контексті безпеки

Централізовані системи є однією з найбільш поширених архітектур для забезпечення обміну інформацією в сучасних організаціях. Вони передбачають наявність єдиного центра, який відповідає за зберігання, обробку та передачу даних. Такі системи зазвичай мають високу продуктивність, оскільки всі операції здійснюються через єдину точку, що спрощує їх координацію та виконання. Проте централізовані рішення мають суттєвий недолік — існує ризик єдиної точки відмови. Якщо цей центр буде зламаний або зазнає збою, то всі дані і операції можуть бути знищені або піддані маніпуляціям.

Відмінність між централізованими та децентралізованими системами полягає в способі зберігання та обробки даних. У децентралізованих системах, таких як блокчейн, дані розподіляються серед численних учасників мережі, що значно знижує ризик одночасного виведення з ладу всієї системи. Кожен учасник мережі зберігає копії даних та має можливість перевіряти їх цілісність та автентичність, що ускладнює можливість здійснення зловмисних дій.

З точки зору безпеки, децентралізовані підходи, як блокчейн, мають велику перевагу в запобіганні атакам, оскільки для того, щоб змінити інформацію в блокчейні, зловмисник повинен змінити всі копії даних на кожному з учасників мережі, що є практично неможливим. Однак, попри свої переваги, блокчейн має і недоліки, найголовнішим з яких є знижена продуктивність. Висока ступінь дистрибуції та необхідність консенсусу серед учасників мережі значно сповільнює процес обробки транзакцій, порівняно з централізованими системами, що може бути проблемою для завдань з інтенсивним обміном інформацією або великими обсягами даних.

Таким чином, хоча блокчейн пропонує значні переваги в контексті безпеки та зменшення ризиків від єдиної точки відмови, його використання може бути менш ефективним у випадках, коли важлива висока швидкість обробки або великий обсяг транзакцій. Вибір між централізованими і децентралізованими підходами залежить від конкретних вимог системи та завдань, які потрібно вирішити.

3.3.3. Переваги та недоліки застосування блокчейну

1) Висока стійкість до атак та компрометації даних

Однією з ключових переваг технології блокчейн у технічних системах є її висока стійкість до атак та компрометації даних. Децентралізована архітектура блокчейну забезпечує унікальний підхід до захисту інформації, усуваючи основні вразливості централізованих систем. Зокрема, децентралізація значно ускладнює реалізацію атак типу «людина посередині» (Man-in-the-Middle, MitM), які зазвичай спрямовані на перехоплення та зміну даних під час їх передачі.

Децентралізована архітектура як основа захисту

На відміну від централізованих систем, де один сервер або вузол може стати ціллю для атакуючого, у блокчейн-системі кожен учасник мережі зберігає копію всієї бази даних. Таким чином, щоб змінити хоча б один запис у блокчейні, атакуючий повинен одночасно скомпрометувати більшість вузлів, що є надзвичайно складним завданням з обчислювальної точки зору.

Захист від підробки даних та змін записів

Незмінність даних є основним принципом блокчейн-технології, що гарантується криптографічними методами хешування та зв'язування блоків. Кожен блок містить хеш попереднього блоку, що створює ланцюжок, будь-яка зміна якого призводить до порушення цілісності всієї структури. Завдяки цьому кожна спроба модифікації даних стає очевидною всім учасникам системи.

Протидія атакам на цілісність інформації

Захист цілісності реалізується через механізм консенсусу, що забезпечує одностайне підтвердження транзакцій усіма учасниками. Такі алгоритми, як Proof of Work (PoW) або Proof of Stake (PoS), створюють додатковий бар'єр для потенційних зловмисників, адже для успішної атаки на блокчейн необхідно контролювати значну частку обчислювальної потужності або активів мережі.

Переваги незмінності блоків

Незмінність блоків забезпечує можливість ведення безпечного журналу подій, що є особливо важливим у контексті кібербезпеки. У випадку атаки або спроби підробки, історія змін залишається прозорою та доступною для аудиту, що підвищує довіру до системи в цілому.

2) Проблеми масштабованості та продуктивності

Незважаючи на високий рівень безпеки, блокчейн-технології стикаються з проблемою масштабованості, яка безпосередньо впливає на продуктивність системи. Збільшення кількості транзакцій у мережі часто призводить до зниження швидкості їх обробки, що особливо помітно у глобальних розподілених системах.

Основні виклики масштабування

Класичні блокчейн-мережі, побудовані на основі Proof of Work (PoW), вимагають значних обчислювальних ресурсів для підтвердження транзакцій. Зі зростанням кількості користувачів та транзакцій швидкість обробки істотно зменшується. Наприклад, у мережі Біткоїн максимальна пропускна здатність становить близько 7 транзакцій за секунду (TPS), що недостатньо для застосування в інтенсивних системах реального часу.

Proof of Stake як альтернатива

Для підвищення продуктивності використовуються альтернативні алгоритми консенсусу, зокрема Proof of Stake (PoS). Замість енерговитратних обчислень, PoS базується на підтвердженні транзакцій учасниками, які мають значний обсяг активів у мережі. Це дозволяє скоротити час обробки та зменшити енергоспоживання.

Виклики реалізації PoS

Незважаючи на переваги, PoS також має свої недоліки. Найбільшою проблемою є надійність автентифікації вузлів. Якщо вузли з найбільшими ставками (stake) скомпрометовані, це може призвести до захоплення контролю над мережею. Тому розробляються нові протоколи, що комбінують PoS з іншими методами (наприклад, Delegated Proof of Stake, DPoS) для підвищення надійності.

Перспективи оптимізації

Одним з перспективних рішень є застосування шардингу (sharding) — технології, що розділяє базу даних на менші сегменти (шарди), кожен з яких обробляється окремою підмережею. Також використовуються рішення другого рівня (наприклад, Lightning Network), які дозволяють здійснювати транзакції поза основним ланцюгом, зберігаючи при цьому цілісність та безпеку.

Баланс між безпекою та продуктивністю

Забезпечення високої продуктивності не повинно знижувати рівень безпеки мережі. Розробка адаптивних консенсусних алгоритмів, що комбінують переваги PoW та PoS, дозволяє досяг-

ти оптимального співвідношення між надійністю та швидкістю обробки даних.

Таким чином, розвиток блокчейн-технологій у контексті кібербезпеки передбачає не лише вдосконалення захисних механізмів, але й активне вирішення проблем масштабованості для забезпечення стабільної роботи системи у великих мережах.

3.3.4. Ризики та обмеження впровадження блокчейну у технічних системах

1) Загрози, пов'язані з децентралізованими системами технічних систем

Децентралізовані системи технічних систем, попри численні переваги, стикаються з рядом специфічних загроз, що обумовлені їхньою структурою та принципами функціонування. Однією з головних проблем є ускладнене управління мережею, що призводить до труднощів у досягненні консенсусу між учасниками. Через відсутність єдиного централізованого контролера кожен вузол може мати власну версію істини, що створює ризики колізій під час прийняття спільних рішень. Це особливо небезпечно у випадках, коли технічна система має критичне значення для функціонування інфраструктури або забезпечення безпеки.

Особливої уваги потребують смарт-контракти, що виступають автоматизованими елементами управління та обробки даних у децентралізованих системах. Недостатній аудит та перевірка коду смарт-контрактів можуть призводити до серйозних уразливостей, що експлуатуються зловмисниками. Такі вразливості можуть використовуватись для маніпулювання транзакціями, порушення логіки виконання контракту або доступу до конфіденційних даних. Крім того, навіть добре спроектовані смарт-контракти можуть стати об'єктом експлуатації у разі використання старих або нестабільних версій бібліотек.

Крім того, через складну архітектуру та високий ступінь автономії окремих елементів, процес моніторингу та реагування на інциденти ускладнюється. Це потребує впровадження комплексних систем виявлення та усунення загроз із використанням методів машинного навчання та штучного інтелекту, що дозволяють своєчасно виявляти аномалії в децентралізованих струк-

турах. Також доцільно використовувати спеціалізовані інструменти моніторингу стану блокчейн-мереж, що забезпечують цілодобове відстеження змін та інцидентів.

2) Можливі вектори атак на блокчейн-системи технічних систем

Попри високий рівень стійкості до зовнішніх втручань, блокчейн-системи не позбавлені вразливостей, особливо коли йдеться про технічні системи з критичними функціями. Одним із найнебезпечніших векторів атак є так звані атаки типу «51%», коли зловмисники отримують контроль над більшістю обчислювальних потужностей, що дозволяє їм модифікувати блокчейн-дані, здійснювати повторні витрати або блокувати транзакції. Подібні атаки особливо небезпечні в системах, де критично важлива непорушність записів, наприклад, у фінансових або державних реєстрах.

Іншою значною загрозою є атаки через вразливості смарт-контрактів. Навіть незначні помилки в коді можуть дозволити зловмисникам використовувати контракти у власних інтересах. Для мінімізації таких ризиків необхідний комплексний підхід до перевірки коду, включаючи статичний та динамічний аналіз, а також аудит зовнішніми експертами. Окрім того, важливо дотримуватись принципу оновлюваності, адже зловмисники можуть скористатися відомими вразливостями у старих версіях смарт-контрактів.

Блокчейн також піддається атакам соціальної інженерії та DDoS-атакам на окремі вузли. Зважаючи на критичність технічних систем, необхідно передбачити багаторівневий захист із використанням розподілених систем моніторингу та реагування, а також впровадження криптографічних методів перевірки даних. Не менш важливо забезпечити надійність протоколів комунікації між вузлами та захист від спуфінгових атак, що можуть впливати на цілісність мережевих даних.

Отже, для забезпечення належного рівня безпеки децентралізованих систем технічних систем слід не лише враховувати архітектурні особливості блокчейну, а й застосовувати передові технології захисту на різних етапах розробки та експлуатації. Інтеграція методів кіберзахисту з технологіями штучного інтелекту дозволить швидше виявляти потенційні загрози та знижувати ризики експлуатації вразливостей.

3.4. Перспективи розвитку та стратегії інтеграції безпеки технічних систем на етапі проектування (Security by Design)

3.4.1. Концепція Security by Design.

У сучасних умовах інтенсивного розвитку цифрових технологій та глобальної цифровізації концепція Security by Design (SBD) стає стратегічно важливим підходом до забезпечення безпеки технічних систем [43, с. 5]. Зростаюча складність технічних рішень, що включають елементи штучного інтелекту, кіберфізичних систем та Інтернету речей (IoT), породжує нові ризики та вразливості, що вимагають принципово нового підходу до захисту на всіх етапах життєвого циклу системи.

Концепція SBD полягає у системному інтегруванні безпекових механізмів на початкових етапах проєктування, що дозволяє створювати стійкі до загроз системи ще до їхньої реалізації. На відміну від традиційних методів, що часто орієнтовані на реагування на вже існуючі загрози, SBD передбачає проактивний підхід, при якому безпека стає невід'ємною складовою архітектури системи. Завдяки цьому мінімізується вплив потенційних вразливостей ще на етапі проєктування, що підвищує загальну стійкість системи до атак.

Сучасні тенденції у сфері технічної безпеки свідчать про дедалі ширше впровадження SBD у різних галузях, включаючи промисловість, транспорт, енергетику та державне управління. Наприклад, у кіберфізичних системах, де інформаційні та фізичні компоненти тісно взаємодіють, інтеграція безпеки на етапі проєктування дозволяє забезпечити стійкість системи до кібератак з мінімізацією ризиків для фізичної інфраструктури.

У науково-технічному контексті SBD можна розглядати як складну міждисциплінарну концепцію, що поєднує методи системного аналізу, криптографічних технологій, кібергігієни та проєктування на основі ризиків. Враховуючи, що сучасні технічні системи часто базуються на інтелектуальних алгоритмах обробки великих даних, SBD набуває ще більшої актуальності. Зокрема, інтеграція методів машинного навчання для ідентифікації аномалій у роботі системи під час її проєктування забезпечує не тільки стійкість до відомих атак, але й адаптивність до нових видів загроз.

Зростаюче застосування концепції SBD обумовлене також розвитком нормативно-правового забезпечення у сфері безпеки технічних систем. Такі міжнародні стандарти, як ISO/IEC 27001 та NIST Cybersecurity Framework, включають принципи безпеки за замовчуванням та закликають до інтеграції безпекових заходів на всіх етапах розробки систем. Таким чином, SBD не тільки визначає нові методологічні основи проєктування, а й забезпечує відповідність регуляторним вимогам.

3.4.2. Основні принципи інтеграції безпеки на етапі проєктування Security by Design (SBD)

Розробка технічних систем з інтегрованими безпековими функціями ґрунтується на кількох ключових принципах, що дозволяють формувати надійні та адаптивні рішення:

1) Проактивність.

Включає раннє виявлення загроз та оцінку ризиків на початкових етапах проєктування. Замість реактивного усунення вразливостей після появи проблеми, SBD передбачає випереджувальний аналіз потенційних загроз, що знижує ймовірність атак.

2) Безперервність.

Безпека не обмежується лише початковими етапами розробки. SBD передбачає підтримку безпеки на всіх етапах життєвого циклу системи, від її розробки до виведення з експлуатації. Постійний моніторинг та оновлення дозволяють підтримувати актуальність захисних заходів у мінливому технологічному середовищі.

3) Модульність.

Розробка компонентів системи з вбудованими механізмами безпеки забезпечує їх незалежність та гнучкість. Такий підхід полегшує адаптацію та модернізацію безпеки окремих елементів без порушення цілісності системи.

4) Адаптивність.

Здатність системи до самонавчання та адаптації до нових загроз дозволяє швидко реагувати на зміни у кіберсередовищі. Впровадження штучного інтелекту та алгоритмів машинного навчання підвищує рівень автоматизації захисту та знижує ризики атак.

5) Прозорість.

Організація процесів безпеки з можливістю контролю та аудиту забезпечує відкритість та зрозумілість безпекових заходів. Це дозволяє залучити користувачів та операторів системи до активного контролю за станом безпеки.

Інтеграція принципів Security by Design дозволяє створювати високонадійні технічні системи, що адаптуються до мінливих умов кіберсередовища. Такий підхід забезпечує не лише високий рівень кіберзахисту, а й підвищує загальну довіру до технічних рішень, що інтегруються в складні соціотехнічні середовища.

3.4.3. Стратегії впровадження Security by Design у сучасних технічних системах

Реалізація підходу Security by Design (SBD) у сучасних технічних системах є надзвичайно актуальною задачею у сфері кібербезпеки. Такий підхід передбачає інтеграцію безпекових компонентів на всіх етапах розробки та експлуатації системи, починаючи з проєктування та завершуючи підтримкою й модернізацією. Основна ідея полягає у забезпеченні стійкості до потенційних загроз ще на початкових етапах створення системи.

Ключові шляхи стратегії впровадження SBD

1) Інженерна інтеграція.

На етапі проєктування технічних систем необхідно передбачити включення безпекових компонентів, таких як криптографічний захист даних, ідентифікація та автентифікація користувачів. Інженерна інтеграція також передбачає регулярне тестування та верифікацію системи для виявлення вразливостей. Додатково слід враховувати методи безперервного моніторингу системи на предмет виявлення нетипової поведінки компонентів, що може свідчити про наявність кіберзагроз.

2) Використання шаблонів безпеки.

Розробка стандартних шаблонів для проєктування безпечних систем дозволяє знизити ризики, пов’язані з повторенням типових помилок. Такі шаблони можуть включати типові схеми захисту мереж, обробки конфіденційних даних та механізмів реагування на інциденти. Уніфікація підходів до безпеки дозволяє спростити процеси тестування та верифікації систем.

3) Автоматизація процесів.

Застосування автоматизованих інструментів для аналізу загроз та оцінки ризиків дозволяє оперативно виявляти потенційні небезпеки та мінімізувати людський фактор у прийнятті рішень. Сучасні системи безпеки активно використовують машинне навчання для виявлення аномалій у роботі технічних компонентів. Зокрема, алгоритми глибокого навчання забезпечують високу точність у прогнозуванні потенційних *атак на основі великих обсягів даних.*

4) Використання стандартизованих протоколів.

Інтероперабельність та надійність сучасних технічних систем досягається шляхом впровадження стандартизованих протоколів обміну даними та шифрування. Це забезпечує захищений обмін інформацією між різними компонентами системи. Зокрема, застосування протоколів TLS 1.3 та IPsec дозволяє забезпечити криптостійкість і захист від перехоплення даних.

5) Залучення фахівців з безпеки на початкових етапах.

Формування багатофункціональних команд, що включають експертів з кібербезпеки на етапі архітектурного планування, дозволяє передбачити можливі вектори атак та відповідно адаптувати архітектуру системи. Впровадження методологій загрозоорієнтованого проєктування (Threat Modeling) дозволяє структуровано оцінити можливі ризики та запобігти їх реалізації на етапі проєктування.

Застосування перелічених стратегій дозволяє знизити ризики реалізації потенційних загроз та забезпечує надійність і стійкість технічних систем до кіберзагроз.

3.4.4. Перспективи розвитку Security by Design

З розвитком новітніх технологій, концепція Security by Design (SBD) отримує нові вектори впровадження, що дозволяють забезпечити ще вищий рівень безпеки технічних систем. Основні перспективні напрями включають [54, с. 3]:

1) Інтелектуальні системи безпеки.

Інтеграція штучного інтелекту для автоматизованого виявлення нових загроз та адаптивного реагування на них, що дозволяє підвищити ефективність захисту навіть у складних середовищах. Використання алгоритмів самообучення забезпечує динамічне оновлення моделей загроз у режимі реального часу.

2) Інтеграція блокчейн-технологій.

Використання децентралізованих платформ на основі блокчейну забезпечує додаткову стійкість до несанкціонованих змін даних та втручання в роботу систем. Блокчейн також дозволяє зберігати логи без можливості їх підробки, що є критично важливим для забезпечення цілісності даних.

3) Квантові алгоритми.

З огляду на розвиток квантових обчислень, з'являється потреба у використанні нових алгоритмів шифрування, що здатні витримати атаки з використанням квантових комп'ютерів. Розробка квантово-стійких алгоритмів є ключовим напрямом у забезпеченні довготривалої безпеки технічних систем.

4) Автоматизовані платформи управління ризиками.

Впровадження платформ, що здатні у реальному часі аналізувати ризики та приймати рішення без втручання людини, дозволяє значно підвищити швидкість реагування на інциденти. Використання хмарних технологій забезпечує масштабованість та швидке впровадження нових засобів захисту.

Таким чином, інтеграція новітніх технологій у концепцію Security by Design дозволить забезпечити високу адаптивність технічних систем у відповідь на нові виклики кібербезпеки.

3.4.5. Виклики та ризики при впровадженні Security by Design

Впровадження принципу **Security by Design** на етапі проектування технічних систем не є простою задачею і включає низку суттєвих викликів, які можуть значно вплинути на ефективність та результативність забезпечення кібербезпеки в майбутньому. Ось детальніше про ключові проблеми, з якими стикаються організації при реалізації цього підходу.

1) Інженерна складність.

Одним з основних викликів є інженерна складність інтеграції безпекових функцій на етапі проектування. Впровадження безпеки в архітектуру технічних систем вимагає наявності глибоких знань і компетенцій не тільки в області інформаційної безпеки, але й в програмуванні, моделюванні, а також у системному аналізі. Проектувальники повинні вміти розробляти системи таким чином, щоб безпека стала невід'ємною частиною архітек-

тури з самого початку, без потреби в «виправленнях» та додаткових заходах після впровадження системи.

Таке глибоке розуміння безпеки потребує залучення спеціалістів з різних галузей, таких як інженери з безпеки, фахівці з криптографії, аналітики загроз і системні архітектори. Крім того, інженерна складність значною мірою залежить від специфіки технічної системи, що розробляється, а також від її майбутнього використання в реальних умовах, де можуть бути змінені зовнішні фактори.

2) Людський фактор.

Не менш важливою перешкодою є людський фактор. Досвід показує, що навіть найкраще спроєктовані безпекові рішення можуть бути вразливими через недостатню кваліфікацію або недбалість персоналу, який їх впроваджує або експлуатує. Відсутність знань з методології **Security by Design** у працівників, особливо тих, хто безпосередньо займається розробкою системи, може призвести до множинних помилок. Наприклад, невірно налаштовані параметри доступу, недостатнє тестування або ігнорування новітніх методів захисту можуть залишити систему вразливою до зовнішніх і внутрішніх загроз.

Захист від людських помилок вимагає постійної професійної підготовки та освіти фахівців на всіх етапах життєвого циклу системи, а також розробки чітких процедур перевірки та тестування безпекових компонентів.

3) Вартість впровадження.

Інтеграція безпекових заходів в архітектуру системи на етапі проектування вимагає значних фінансових та ресурсних витрат. Витрати на дослідження, розробку, тестування та навчання персоналу можуть бути значними, що робить цей процес дорогим у порівнянні з традиційними підходами, де безпека інтегрується на більш пізніх етапах, коли система вже працює.

Однак економія на етапі проектування може призвести до більш значних витрат на етапах тестування, виправлення вразливостей або навіть на етапах експлуатації, коли вразливості стають критичними для безпеки користувачів або організацій. Більш того, витрати на інтеграцію безпеки на ранніх етапах часто виправдовуються завдяки зниженню ризиків і можливих втрат в майбутньому.

4) Динамічність загроз.

Одним з найбільших викликів для підходу **Security by Design** є постійно змінювана природа загроз в кіберпросторі. Швидке зростання і зміни в технологіях, а також постійна еволюція методів атаки вимагають від розробників постійної адаптації та актуалізації систем безпеки.

Загрози, які можуть бути актуальними на момент проектування системи, можуть швидко втратити свою релевантність або, навпаки, з'являються нові типи атак, які не були передбачені під час проектування. Для цього необхідно регулярно переглядати та оновлювати заходи безпеки, застосовуючи новітні методи захисту та інструменти для запобігання зловмисним діям.

3.4.6. Кращі практики реалізації Security by Design у технічних системах

Для того щоб забезпечити ефективне впровадження принципу **Security by Design**, варто орієнтуватися на кращі практики, що дозволяють інтегрувати безпеку в архітектуру системи з урахуванням актуальних загроз та вимог.

1) Розробка політик безпеки на ранніх етапах проекту.

Розробка чітких політик безпеки на початкових етапах проектування є однією з основних складових успішного впровадження Security by Design. Зокрема, необхідно визначити критерії безпеки, вимоги до конфіденційності, цілісності та доступності даних, а також створити план захисту від потенційних атак. Врахування цих аспектів на самому початку проекту дозволяє вбудувати безпеку в усі етапи розвитку системи, що зменшує ризики в майбутньому.

2) Проведення аудитів безпеки на кожній стадії життєвого циклу.

Аудити безпеки повинні проводитися на кожній стадії життєвого циклу системи: від проектування до реалізації та підтримки. Вони дозволяють виявити потенційні вразливості, оцінити ефективність впроваджених заходів і коригувати проєкт у разі виявлення недоліків. Цей процес дозволяє своєчасно виявляти загрози та коригувати систему, мінімізуючи ризики її експлуатації.

3) Використання методів загрозомоделювання.

Загрозомоделювання є важливим інструментом для прогнозування можливих ризиків і створення ефективних заходів без-

пеки. Моделювання дозволяє виявити слабкі місця системи, оцінити ймовірність загрози та її наслідки для системи, що дає змогу розробити заходи щодо її мінімізації.

4) Навчання персоналу.

Навчання персоналу методології **Security by Design** є необхідним кроком для забезпечення ефективності розробки та експлуатації безпечних систем. Співробітники повинні бути обізнані з актуальними стандартами безпеки, а також із кращими практиками проектування та реалізації безпечних систем. Постійне підвищення кваліфікації персоналу дозволяє мінімізувати помилки, пов'язані з людським фактором.

5) Постійне вдосконалення архітектури системи.

Інтеграція безпеки повинна бути безперервним процесом, який триває на всіх етапах життєвого циклу системи. З цією метою важливо регулярно оновлювати архітектуру, застосовуючи нові методи і технології для захисту системи від нових загроз. Це дозволяє створювати адаптивні та стійкі системи, які ефективно реагують на зміни в кіберзагрозах.

Реалізація підходу **Security by Design** є складним і ресурсоємним процесом, який вимагає інтеграції безпеки на всіх етапах життєвого циклу системи. Врахування викликів, таких як інженерна складність, людський фактор, вартість впровадження та динамічність загроз, дозволяє створювати безпечні та надійні системи. Застосування кращих практик — від розробки політик безпеки до постійного вдосконалення архітектури — є ключовим фактором для зменшення ризиків і досягнення високого рівня захисту від потенційних кіберзагроз

Контрольні питання

1. Які основні безпекові виклики виникають при інтеграції IoT у технічні системи?
2. Які ризики для технічних систем створюють кіберфізичні системи?
3. Як забезпечити надійність обміну даними в середовищі IoT?
4. Які методи автентифікації використовуються для захисту IoT-пристроїв?
5. Які сучасні стандарти використовуються для забезпечення безпеки в IoT?

6. Як враховуються вимоги до кібербезпеки при проєктуванні кіберфізичних систем?

7. Які основні алгоритми машинного навчання використовуються для моніторингу технічних систем?

8. Як штучний інтелект сприяє ідентифікації нових типів атак?

9. Які виклики пов'язані із застосуванням штучного інтелекту для кібербезпеки?

10. Як нейронні мережі використовуються для аналізу аномалій у технічних системах?

11. Які етичні аспекти виникають при використанні ШІ для безпеки технічних систем?

12. Як поєднання штучного інтелекту та кіберфізичних систем впливає на безпеку?

13. Які основні переваги використання блокчейн-технологій для захисту технічних систем?

14. Як розподілені реєстри впливають на цілісність даних у технічних системах?

15. У чому полягає роль смарт-контрактів у забезпеченні кібербезпеки?

16. Які виклики постають при інтеграції блокчейн-рішень у технічні системи?

17. Як блокчейн забезпечує надійність ідентифікації користувачів?

18. Які перспективи розвитку блокчейну для забезпечення безпеки технічних систем?

19. У чому полягає концепція «Security by Design» у технічних системах?

20. Які принципи безпеки враховуються на етапі проєктування систем?

21. Як використання моделей загроз на етапі проектування впливає на надійність системи?

22. Які методи забезпечення безпеки доцільно застосовувати на різних етапах життєвого циклу системи?

23. Як аналіз ризиків впливає на проектування безпечних технічних систем?

24. Які основні підходи до інтеграції безпеки на рівні архітектури технічних систем?

25. Які інноваційні стратегії дозволяють оптимізувати процес впровадження безпеки в технічні системи?

СПИСОК ЛІТЕРАТУРИ

1. Конституція України: Закон України від 28.06.1996. № 254к/96. Дата оновлення: 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 14.06.2024).
2. Закон України "Про захист інформації в інформаційно-комунікаційних системах" (назва із змінами, внесеними згідно із Законом України від 16.12.2020 р. N 1089-IX). Дата оновлення 27.03.2025. *Ips.Ligazakon.Net.* Сайт. URL: https://ips.ligazakon.net/document/Z008000?an=4776 (дата звернення: 14.04.2025).
3. Закон України «Про державну таємницю» (Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93) Дата оновлення: 10.10.2024 N 4019-IX. URl: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 04.04.2025).
4. Закон України «Про енергетичну ефективність та енергетичну безпеку» (Відомості Верховної Ради України (ВВР), 2022, № 2, ст. 8). Дата оновлення 19.11.2024. URl: https://zakon.rada.gov.ua/laws/show/1818-20#Text (дата звернення: 10.04.2025).
5. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, № 48, ст. 650). Дата оновлення 10.10.2024. URl: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.04.2025).
6. Закон України «Про наукову і науково-технічну експертизу» (Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93). Дата оновлення: 10.10.2024. № 4017-IX. *Ips.Ligazakon.Net* Сайт. URL: https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80#Text (дата звернення: 04.04.2025).
7. Закон України «Про об'єкти підвищеної небезпеки» від 15 травня 2003 року N 762-IV, (який вводиться в дію з 1 січня 2024 року) (останні зміни: від 13 грудня 2022 року N 2849-IX) (дата звернення: 20.03.2025).
8. Закон України «Про охорону праці» (Відомості Верховної Ради України (ВВР), 1992, № 49, ст. 669). Дата оновлення 19.12.2024. URl: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення: 10.04.2025).

9. Закон України «Про стандартизацію» (Відомості Верховної Ради України (ВВР), 2013, № 31, ст. 1058). Дата оновлення 27.12.2025. URl: https://zakon.rada.gov.ua/laws/show/1315-18#Text (дата звернення: 10.04.2025).

10. Закон України «Про технічні регламенти та оцінку відповідності» (Відомості Верховної Ради України (ВВР), 2015, № 14, ст.96). Дата оновлення 27.03.2025. URl: https://zakon.rada.gov.ua /laws/show/124-19#Text (дата звернення: 10.04.2025).

11. Кодекс цивільного захисту України (Відомості Верховної Ради України (ВВР), 2013, № 34-35, ст. 458). Дата оновлення 19.12.2024. URl: https://zakon.rada.gov.ua/laws/show/5403#Text (дата звернення: 10.04.2025).

12. Постанова Кабінету Міністрів України «Про затвердження переліку об'єктів та окремих територій, які підлягають постійному та обов'язковому на договірній основі обслуговуванню державними аварійно-рятувальними службами» від 04.08.2000 № 1214.

13. Постанова Кабінету Міністрів України «Про затвердження порядку ідентифікації та обліку об'єктів підвищеної небезпеки» від 11.07.2002 № 956.

14. Закон України. Про Національну програму інформатизації: Документ 2807- IX, чинний, поточна редакція Прийняття від 01.12.2022. *Zakon.Rada.Gov.UA.* Сайт. URL: https://zakon.rada.gov.ua /laws/show/2807-20#Text (дата звернення: 25.05.2023).

15. ISO/IEC 27001:2022 – Система управління інформаційною безпекою (СУІБ) ДСТУ. URL : https://icr-cert.com.ua/iso-27001-2022-information-security-management-systems-isms/ (дата звернення: 20.03.2025).

16. ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (СУІБ). URL : https://icr-cert.com.ua/iso-27001-2022-information-security-management-systems-isms/ (дата звернення: 20.03.2025).

17. Балтовський О.А., Белека І.А., Ісмайлов К.Ю. Методика аналізу схем цифро-аналогових перетворювачів з використанням матриць гібридного типу. *Вісник Інженерної академії Укра-*

їни Кіровоградського національного технічного університету. 2019. № 3. С. 79-85.

18. Бонк М. Застосування машинного навчання для виявлення загроз в файрволах – переваги та можливості. *Mediacom.* 19 Січня, 2024. URL : https://mediacom.com.ua/zastosuvannya-mashinnogo-navchannya-dlya-viyavlennya-zagroz-v-fajrvolax-perevagi-i-mozhlivosti/ (дата звернення: 25.03.2025).

19. Бурячок В. Л. , Киричок Р. В. , Складанний П. М. Основи інформаційної та кібернетичної безпеки: Навчальний посібник. Київ 2019. р. 320 с.

20. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

21. Габрильчук А. В., Сусукайло В. А., Курій Є. О., Василишин С. І. Дослідження кібератак з використанням машинного навчання на системи управління інформаційною безпекою. *Computer Systems and Networks*. Vol. 7, No. 1, 2025. С. 68-78.

22. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах: Підручник. Ужгород : ПП «АУТДОР-ШАРК»,. 2021. 184 с.

23. Герасименко В.А., Малюк А.А. Основи захисту інформації. К.: Інкомбук, 2019. 540 с.

24. Герасимчук О.П. Теорія технічних систем: Навчальний посібник для здобувачів другого (магістерського) рівня вищої освіти денної та заочної форм навчання. Луцьк: ЛНТУ, 2023. 112 с.

25. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: НА СБ України, 2020. 256 с.

26. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки: Навчальний посібник. Вінниця. ВНТУ. 2018. 316 с.

27. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. КІВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

28. Ісмайлов К.Ю., Балтовський О.А., Сіфоров О.І. Основні підходи щодо вирішення завдання оптимального календарного планування з використанням спеціалізованих алгоритмів. *Електронне наукове видання «Порівняльно- аналітичне право».* 2019. №2. С. 98-101.

29. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун,. В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2009. 352 с. (Укр. мов.). 369 с.

30. Конспект лекцій з дисципліни "Безпека життєдіяльності та основи охорони праці" для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 051 "Економіка", 071 "Облік і оподаткування", 075 "Маркетинг" денної та заочної форми навчання / Уклад.: Бочковський А.П., Сапожнікова Н.Ю. Одеса: ОП, 2021. 100 с.

31. Крупа В.В. Теорія технічних систем: особливості побудови створення та розвитку: навчальний посібник / Володимир Крупа. Тернопіль : Осадца Ю.В., 2023. 308 с.

32. Купалова Г., Коренєва Н., Наталія Гончаренко Н. Теоретико-організаційні аспекти застосування технології блокчейн у підприємництві. *Modeling the Development of the Economic Systems*. 2022, №2 121-127.

33. Кутова М.А Основи інформаційної безпеки в системі електронного урядування. Науковий журнал «Economic Synergy», випуск 1 (11), 2024. С. 20-30.

34. Літнарович Р.М. Сучасні технології інформаційної безпеки. Частина 1. Навчальний посібник, МЕГУ, Рівне, 2011. 97 с.

35. Ловейкін В.С. Теорія технічних систем / В.С. Ловейкін, Ю.О. Ромасевич. К.: ЦП «КОМПРИНТ», 2017. 291 с.

36. Методичні вказівки до проведення практичних занять студентів з дисципліни «Надійність технічних систем і техногенний ризик» (для студентів 4 курсу денної та 5 курсу заочної форм навчання напряму підготовки 6.170202 Охорона праці) / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова; уклад.: В. Е. Абракітов, С. А. Грязнова. Харків : ХНУМГ ім. О. М. Бекетова, 2017. 83 с.

37. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. К.: Вид. Національної академії внутріш. справ, 2012. 104 с.

38. Севостьянов І. В. Теорія технічних систем : підручник / Севостьянов І. В. Вінниця : ВНТУ, 2014. 181 с.

39. Сторчак К.П., Тушич А.М., Срібна І.М., Яковенко Н.Д., Кравець Д.В. Технології Інтернет речей. Навч. посьбник підготов-

лено для студентів вищих навчальних закладів Київ: ДУТ, 2021. 68 с.

40. Сучасні підходи щодо адаптивного автоматизованого управління складними системами в умовах невизначеності: монографія / Кокошко В.С., Ісмайлов К.Ю., Балтовський А.О., Сіфоров О.І., Пядишев В.Г., Форос Г.В. та ін. Одеса: ОДУВС, 2019. 340 с.

41. Технічні ризики. Теорія та практикум: [Електронний ресурс]: навч. посібник для студ. спеціальностей: 141 «Електроенергетика, електротехніка та електромеханіка» спеціалізацій: «Інжиніринг електротехнічних комплексів», «Електромеханічні та мехатронні системи енергоємних виробництв» / О. М. Терентьєв, С. В. Зайченко, А. Й. Клещов, Н. А. Шевчук / КПІ ім. Ігоря Сікорського. Електронні тестові дані (1 файл: 5207 КБ). Київ: КПІ ім. Ігоря Сікорського, 2020. 168 с.

42. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

43. Чому вам потрібно розуміти концепцію кібербезпеки “Secure by Design”. *Klik Solutions*. 14 Листопада, 2023 Site. URL : https://www.kliksolutions.com.ua/great-info/chomu-vam-potribno-rozumity-konczepcziyu-kiberbezpeky-secure-by-design/ (дата звернення: 20.03.2025).

44. Щепотьєв О. І. Експлуатаційна надійність техніки / О.І. Щепотьєв, А.В. Жильцов, В.В. Васюк К.: ЦТІ «Аграр Медіа Груп» 2016. 507 с.

45. Щепотьєв О. І. Надійність технічних систем / О. І. Щепотьєв, А. В. Жильцов. К.: ЦТІ «Аграр Медіа Груп» 2012. 298 с.

46. 10 Security Design Principles for Application Security. *LegitSecurity.Com*. Site. URL: https://www.legitsecurity.com/aspm-knowledge-base/security-design-principles (дата звернення: 20.03.2025).

47. Bearfield, G. Safety of technical systems: the next 30 years. *Rail Technology Magazine*. Feb/March 2019. Site. URL: https://www.railtechnologymagazine.com/Comment/safety-of-technical-systems-the-next-30-years (дата звернення: 04.04.2025).

48. Datta, S., Michal Aibin, A. Differences Between Network-level and Application-level Information Security. *Baeldung*. March 18, 2024. Site. URL: https://www.baeldung.com/cs/network-level-vs-application-level-information-security#:~:text=Network%2Dlevel%20information%20security%20refers,data%20transmitted%20over%20the%20network. (дата звернення: 20.03.2025).

49. El-Kady A.H., Halim S., El-Halwagi M.M., Khan F. Analysis of safety and security challenges and opportunities related to cyber-physical systems. *Process Safety and Environmental Protection.* Volume 173, May 2023. P. 384-413. Site. URL: https://www.sciencedirect.com/science/article/abs/pii/S0957582023002045 (дата звернення: 04.04.2025).

50. Hardware Security. *Tektelic.Com*. Site. URL : https://tektelic.com/what-it-is/hardw (дата звернення: 20.03.2025).

51. Hosnedl, S., Vanek, V., Stadler, C. Properties and Qualities of Technical Systems. International Design Conference - Design 2004, Dubrovnik, May 18-21, 2004. URL : file:///C:/Users/User/Downloads/ds32_190.pdf (дата звернення: 20.03.2025).

52. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Published (Edition 3, 2022). URL : https://www.iso.org/standard/27001 (дата звернення: 20.03.2025).

53. Jurvanen, L. What does technical information security mean? *Savelan.Fi*. 29.12.2023. URL : https://www.savelan.fi/en/what-technical-security-means/#:~:text=Technical%20security%20refers%20to%20the,and%20availability%20of%20sensitive%20information. (дата звернення: 25.03.2025).

54. KirvanIvy, P., Wigmore, I. What is security by design? techtarget.com. 2025. Site. URL : https://www.techtarget.com/whatis/definition/security-by-design (дата звернення: 20.03.2025).

55. Law, M.Top 10: Technology Risks. *TechnologyMagazine.Com*. September 11, 2024. Site. URL : https://technologymagazine.com/top10/top-10-technology-risks (дата звернення: 20.03.2025).

56. Security technology: Trends & Advancements. *City Security Magazine*. 2018. Site. URL : https://citysecuritymagazine. com/security-technology/security-technology-trends-advancements/ (дата звернення: 20.03.2025).

57. Technical Vulnerability. *ScienceDirect.Com*. Site. URL: https://www.sciencedirect.com/topics/computer-science/technical-vulnerability#:~:text=Technical%20vulnerabilities%20relate%20to%20a,designed%2C%20configured%2C%20or%20maintained. (дата звернення: 20.03.2025).

58. Technology Risks *Leanix.Net.* Site. URL : https://www. leanix. net/en/wiki/trm/what-is-technology-risk#form (дата звернення: 20.03.2025).

59. The Fast Way to a Secure Future: INTERSECT. Network Security Meets AI Innovation: Virtual Event. *Palo Alto Networks. 2025*. Site. URL : https://intersect.paloaltonetworks.com/ (дата звернення: 20.03.2025).

60. Threat Detection and Response. *RAPID7*. 2025. Site. URL : https://www.rapid7.com/fundamentals/threat-detection/ (дата звернення: 20.03.2025).

61. What is Blockchain Security? *IBM.Com*. 2025. Site. URL : https://www.ibm.com/think/topics/blockchain-security (дата звернення: 20.03.2025).

62. What is the Internet of Things (IoT)? *IBM.Com*.12 May 2023. Site. URL: https://www.ibm.com/think/topics/internet-of-things (дата звернення: 20.03.2025).

63. What Is the Role of AI in Threat Detection? *Palo Alto Networks*. 2025. P. 10. Site. URL : https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection (дата звернення: 20.03.2025).

Навчальне видання

БАЛТОВСЬКИЙ О. О., ФОРОС Г. В., ПЯДИШЕВ В. Г.

«БЕЗПЕКА ТЕХНІЧНИХ СИСТЕМ»

Навчальний посібник

Підписано до друку 19.06.2025. .Формат 60x84/16 Папір офсетний.
Гарн. «Times New Roman». Друк цифровий. Ум. друк .арк. 8,02.
Надруковано з готового оригінал-макета.
Наклад 30 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.