НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

КЕРУВАННЯ ЕНЕРГЕТИЧНИМИ СИСТЕМАМИ ТА ПОВ'ЯЗАНИЙ З НИМ ІНФОРМАЦІЙНИЙ ОБМІН БЕЗПЕКА ДАНИХ ТА КОМУНІКАЦІЙ

Частина 1. Безпека зв'язку мережі та системи Загальні положення

(IEC/TS 62351-1:2007, IDT)

ДСТУ IEC/TS 62351-1:2014

Видання офіційне

БЗ № 12–2014/492

Київ
МІНЕКОНОМРОЗВИТКУ УКРАЇНИ
2015

ПЕРЕДМОВА

1 ВНЕСЕНО: Національний технічний університет України «Київський політехнічний інститут»

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **Д. Лавренова,** канд. техн. наук; **О. Яндульський,** д-р техн. наук (науковий керівник)

2 НАДАНО ЧИННОСТІ: наказ Мінекономрозвитку України від 2 грудня 2014 р. № 1432 з 2015–05–01

3 Національний стандарт відповідає IEC/TS 62351-1:2007 Power systems management and associated information exchange — Data and communications security — Part 1: Communication network and system security — Introduction to security issues (Керування енергетичними системами та пов'язаний з ним інформаційний обмін. Безпека даних та комунікацій. Частина 1. Безпека зв'язку мережі та системи. Загальні положення)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад IEC/TS 62351-1:2007 Power systems management and associated information exchange — Data and communications security — Part 1: Communication network and system security — Introduction to security issues (Керування енергосистемами та відповідний інформаційний обмін. Безпека даних та зв'язку. Частина 1. Безпека зв'язку мережі та системи. Загальні положення).

Технічний комітет, відповідальний за цей стандарт, — ТК 162 «Керування енергетичними системами та пов'язані з ним процеси інформаційної взаємодії».

Стандарт містить вимоги, які відповідають чинному законодавству України.

До стандарту внесено такі редакційні зміни:

— словосполуки «ця частина міжнародного стандарту IEC 62351» та «цей міжнародний стандарт» замінено на «цей стандарт»;

— структурні елементи стандарту: «Титульний аркуш», «Передмову», «Національний вступ», першу сторінку та «Бібліографію» — оформлено згідно з вимогами комплексу стандартів «Національна стандартизація України».

У розділі «Нормативні посилання» наведено «Національне пояснення», виділене в тексті рамкою.

Нормативні документи, на які є посилання в цьому стандарті, в Україні не прийнято як національні стандарти України і чинних нормативних документів замість них немає. Копії їх можна замовити в Головному фонді нормативних документів.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

КЕРУВАННЯ ЕНЕРГЕТИЧНИМИ СИСТЕМАМИ ТА ПОВ'ЯЗАНИЙ З НИМ ІНФОРМАЦІЙНИЙ ОБМІН БЕЗПЕКА ДАНИХ ТА КОМУНІКАЦІЙ

Частина 1. Безпека зв'язку мережі та системи Загальні положення

УПРАВЛЕНИЕ ЭНЕРГЕТИЧЕСКИМИ СИСТЕМАМИ И СВЯЗАННЫЙ С НИМ ИНФОРМАЦИОННЫЙ ОБМЕН БЕЗОПАСНОСТЬ ДАННЫХ И КОММУНИКАЦИЙ

Часть 1. Безопасность связи сети и системы
Общие положения

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE DATA AND COMMUNICATIONS SECURITY

Part 1. Communication network and system security
Introduction to security issues

Чинний від 2015–05–01

1 СФЕРА ЗАСТОСУВАННЯ І ЗАВДАННЯ

1.1 Сфера застосування

Сферою застосування серії стандартів IEC 62351 є інформаційна безпека керування енергосистемами. Основним завданням є тема «Розробляння стандартів щодо безпеки комунікаційних протоколів, визначених IEC TC 57, зокрема стандартів серії IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 та IEC 61968. Розробляння стандартів та/або технічних звітів щодо питання безпеки».

1.2 Об'єкт стандартизації

Об'єктом стандартизації стандартів серії IEC 62351 є:

— IEC 62351-1, який є вступом до інших частин стандарту, і, в першу чергу, подає різні аспекти інформаційної безпеки під час експлуатування енергосистем;

— IEC 62351-3 та IEC 62351-6, визначають стандарти щодо безпеки комунікаційних протоколів IEC TC 57. Їх може бути використано для забезпечування різних рівнів безпеки протоколу, залежно від протоколу і параметрів, відібраних для конкретної реалізації. Їх також було розроблено для зворотної сумісності та поетапних реалізацій;

— IEC 62351-7, визначає одну з багатьох можливих сфер інформаційної безпеки, а саме: поліпшування загального керування комунікаційними мережами, що забезпечує експлуатування енергосистем;

— інші частини, що описують інші сфери застосування інформаційної безпеки.

Обґрунтуванням для розробляння стандарту щодо інформаційної безпеки є те, що безпека, захист і надійність завжди були важливим питанням під час проектування та експлуатування

Видання офіційне

систем в енергетиці, а також інформаційна безпека стає все важливішою у цій сфері, тому що вона більшою мірою спирається на інформаційну інфраструктуру. Нерегульований ринок зумовив появу нових загроз, таких як знання конкурента про активи та роботи системи, які можуть бути корисними й отримання такої інформації є реальним. Крім того, ненавмисні дії (наприклад, недбалість і стихійні лиха) можуть бути настільки ж шкідливими, як і зумисні дії. Останнім часом з'явилася додаткова загроза — тероризм.

Хоча існує багато визначень «захисту тракту», тут наведено одне (багатозначне) з них «1. Зберігання інформації захищеної системи зв'язку криптографічним або захищеним розподілом системи відбувається від пункту відправлення до пункту призначення. 2. Зберігання інформації в інформаційній системі з пункту відправлення до пункту призначення»[1]. Використовуючи це визначення як основу, перші чотири стандарти визначають вдосконалювання системи безпеки для комунікаційних профілів IEC TC 57, тому що вони були визначені як перші очевидні кроки щодо забезпечування процесів експлуатування та керування енергосистемами. Однак ці вдосконалення системи безпеки можуть задовольнити тільки вимоги щодо безпеки між двома системами, але не задовольняють повний захист тракту, який охоплює внутрішні вимоги щодо безпеки, охоплюючи політику безпеки, забезпечування захисту, виявляння вторгнень у внутрішню системну та програмну цілісність, і все ширші потреби безпеки.

Таким чином, зазначене в розділі «Сфера застосування» має важливий зміст: воно пояснює, що використовування технологій фаєрволів, або лише просте використовування шифрування в протоколах, наприклад за допомогою долучання шифрувальних блоків апаратної реалізації безпеки, або навіть віртуальної приватної мережі (VPN — virtual private network) не може відповідати вимогам щодо безпеки у багатьох ситуаціях. Насправді безпека є потребою захисту тракту, що забезпечує доступ з ідентифікування до чутливого устаткування енергосистеми, несанкціонований доступ до конфіденційних даних ринку, достовірну та своєчасну інформації про функціювання устаткування і збої, поновлювання критично важливих систем, а також засоби контролювання, які дають змогу це виявити та відновити за умови появи руйнувальних подій.

2 НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче нормативні документи містять положення, які через посилання в цьому тексті становлять положення цього стандарту.

IEC 60870-5 (all parts) Telecontrol equipment and systems — Part 5: Transmission protocols

IEC 60870-6 (all parts) Telecontrol equipment and systems — Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations[2]

IEC 61850 (all parts) Communication networks and systems in substations[3].

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

IEC 60870-5 (усі частини) Пристрої та системи телекерування. Частина 5. Протоколи передавання

IEC 60870-6 (усі частини) Пристрої та системи телекерування. Частина 6. Протоколи телекерування, сумісні з ISO стандарти та рекомендації ITU-T

IEC 61850 (усі частини) Мережі зв'язку й системи в підстанціях.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито терміни і визначення позначених ними понять, наведені в IEC 62351-2.

---

[1] ATIS — розширення FS-1037C, яке є стандартним словником термінів федерального уряду США у сфері телекомунікацій.

[2] Також відомий як протокол зв'язку центру сумісного керування (ПЗЦСК), що дозволяє обмін даними крізь глобальну мережу (WAN) між центром керування енергокомпанії та іншим центром керування, іншими енергокомпаніями, об'єднаними енергосистемами, місцевими центрами керування та незалежними генераторами.

[3] IEC 61850, що є нормативною базою для релейного захисту, автоматики підстанції, автоматики розподільчих мереж, якості електроенергії, розподілення енергетичних ресурсів, зв'язку між підстанцією та центром керування і для інших керувальних функцій енергетичної галузі. Він містить профілі для надшвидкого часу відгуку релейного захисту та для вибірки виміряних значень, як і профілі для контролювання та керування устаткованням підстанції та промислової мережі.

4 ПІДҐРУНТЯ ДЛЯ СТАНДАРТІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Підстави для використовування інформаційної безпеки в процесі керування енергосистемами

Комунікаційні протоколи є однією з найважливіших частин керування енергосистеми, відповідальних за вилучання інформації з пам'яті устаткування і, навпаки, для надсилання керувальних команд. Незважаючи на їх ключові функції, на сьогодні ці комунікаційні протоколи рідко враховують будь-які заходи безпеки, разом із захистом від випадкових помилок, несправності устаткування енергосистеми, збою комунікаційного устаткування або навмисного саботажу. Оскільки ці протоколи є дуже спеціалізованими, основним підходом є «внесення невизначеності». Зрештою, лише оператори можуть контролювати вимикачі з високозахищених пунктів керування. Хто міг би подбати про мегавати на лінії, або знати про те, як зчитати специфічні біти і байти, відповідні одному із багатьох комунікаційних протоколів? І чому хтось хоче пошкодити енергосистему?

Однак внесення невизначеності більше не є чинною концепцією. Зокрема, ринок електрики чинить тиск на учасників ринку щодо отримання будь-якої можливої вигоди. Незначна кількість інформації може перетворити програшну ставку на переможну або утримання цієї інформації від ваших конкурентів може перетворити їх виграшні ставки на програшні.

На безпеку мають вплив не лише ринкові сили. Найбільші складності керування енергосистемами з'являються з роками, роблячи устаткування нетривким, а помилки керування вірогіднішими і значущими щодо обсягу і вартісності. Треба враховувати, що старі й «незрозумілі» протоколи замінюють стандартизованими, добре задокументованими, які прийнятніші для хакерів та промислових шпигунів.

З огляду на те, що енергопромисловість все більше залежить від інформації для керування енергосистемами, то зараз виникає потреба в керуванні двома інфраструктурами: не лише інфраструктурою енергосистеми, а й інфраструктурою інформації. Керування інфраструктурою енергосистеми стало надійнішим через інфраструктуру інформації, оскільки автоматика продовжує замінювати ручне керування, ринкові сили потребують точнішої та своєчасної інформації, а устаткування енергосистеми старішає. Тому надійність енергосистем зростає під впливом будь-яких проблем, які інформаційна інфраструктура може розв'язати.

4.2 Протоколи передавання даних ТС 57 IEC

Міжнародна електротехнічна комісія (IEC) технічного комітету ТС 57 «Керування енергосистемами та обмін інформації» відповідає за розробляння міжнародних стандартів для протоколів передавання даних в енергосистемах. Його ціль — «Підготовлення міжнародних стандартів для устаткування керування енергосистеми й систем разом із EMS, SCADA, поширення автоматизації, віддаленого захисту, а також пов'язаний з ними обмін інформацією в режимі реального часу чи в нереальному часі, що використовують під час планування, експлуатування та технічного обслуговування енергосистем. Керування енергосистемами охоплює контролювання з центрів керування, підстанцій, і окремих частин основного устаткування, разом із устаткуванням віддаленого керування та інтерфейсами для устаткування, систем і баз даних, які не належать до профілю сфери діяльності ТС 57. Потрібно враховувати особливі умови, наявні в середовищі високих напруг».

IEC ТС 57 розробив три стандарти для протоколів широкого застосовування і розробив свій четвертий протокол. Це такі три протоколи:

— IEC 60870-5, який широко використовують в Європі та інших неамериканських країнах для систем SCADA передавання даних до місця віддаленого керування (RTU). Його використовують як у послідовних каналах (див. IEC 60870-5-101) так і в мережах (див. IEC 60870-5-104). Формат DNP3 було отримано з IEC 60870-5 для використовування в США і на сьогодні широко використовують у багатьох інших країнах, а також, у першу чергу, для систем SCADA передавання даних до RTU;

— IEC 60870-6 (також відомий як TASE.2 або протокол зв'язку центру сумісного керування (ПЗЦСК)), використовуваний у всьому світі для зв'язку між центрами керування і часто для обміну даними між системами SCADA та іншими інженерними системами в центрах керування;

— IEC 61850, використовуваний для релейного захисту, автоматики підстанцій, автоматики розподілення електроенергії, керування якістю електроенергії, розподілення енергетичних ресурсів, підстанції в центрах керування та інших функцій керування в енергетиці. Він містить профілі з надшвидким часом відповіді захисних пристроїв релейного захисту та отримання вибірок значень вимірювання, а також профілі, спрямовані на контролювання та керування устаткуванням підстанції та промислової мережі.

Ці протоколи на сьогодні широко використовують в електроенергетиці. Однак їх було розроблено до того, як інформаційна безпека стала серйозним питанням для галузі, тому початкові стандарти не охоплювали жодних заходів безпеки.

4.3 Історія розроблення стандартів з безпеки

До 1997 року IEC TC 57 визначив, що безпека буде потрібна для комунікаційних протоколів. У зв'язку з цим вперше було створено тимчасову групу з вивчення питань безпеки. Ця група опублікувала IEC/TR 62210 із вимогами щодо безпеки. Одна з рекомендацій IEC/TR 62210 — це створення робочої групи для розробляння стандартів у частині протоколів безпеки IEC TC 57 та їх похідних.

Загальний критерій міжнародної організації стандартизації (ISO) спочатку було вибрано як метод визначання вимог щодо безпеки. У цьому підході використано концепцію цільової оцінки (КЦО) як осередок аналізування безпеки. Однак, визначивши, що характеристики КЦО для захисту стали дуже громіздкими, враховуючи різноманітність енергосистем та різні потреби у сфері безпеки, в кінцевому рахунку такий критерій не використовували. Замість нього було використано аналізування щодо послаблення загроз (визначення найпоширеніших загроз і вжиття заходів безпеки, спрямованих проти них).

Таким чином, у 1999 році було створено робочу групу IEC TC 57 WG 15, яка виконала цю роботу. WG 15 називається «Керування енергетичними системами та пов'язаний з ним інформаційний обмін. Безпека даних та комунікації», а її сфера діяльності та завдання — це «Розробляння стандартів безпеки комунікаційних протоколів IEC TC 57, зокрема стандартів серій IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 та IEC 61968. Розробляння стандартів та/або технічних звітів щодо питань безпеки».

Обґрунтування цього — безпека і надійність завжди були важливими питаннями проектування та експлуатування систем в енергетиці, а інформаційна безпека стає все важливішою у цій галузі через те, що енергосистеми більшою мірою залежать від інформаційної інфраструктури. Нерегульований ринок зумовив появу нових загроз, таких як знання конкурентами активів і роботи системи. Це корисна інформація та її придбання реально можливе. Останнім часом стала помітнішою додаткова загроза — тероризм.

Зазначене в розділі «Сфера застосування» має важливий зміст: воно пояснює, що використовування технологій фаєрволів або лише просте використовування шифрування в протоколах, наприклад, за допомогою долучання шифрувальних блоків апаратного реалізування безпеки, або навіть VPN не може відповідати вимогам безпеки у багатьох ситуаціях. Дійсно «захист тракту» потребує забезпечування доступу з перевірянням автентичності чутливого устаткування енергосистеми, достовірної та своєчасної інформації про функціювання устаткування і збої, резервне копіювання критично важливих даних, а також засоби керування, які дають змогу відновити найважливіші події.

5 ЗАГАЛЬНІ ПОЛОЖЕННЯ БЕЗПЕКИ ДЛЯ СТАНДАРТІВ СЕРІЇ IEC 62351

5.1 Загальна інформація про безпеку

Цей розділ містить додаткову інформацію про питання безпеки, не охоплену цим стандартом, але яка може бути корисною для розуміння змісту та сфери застосування цього стандарту.

5.2 Типи загроз безпеці

5.2.1 *Загальні положення*

Загрози безпеці зазвичай вважають потенціальною загрозою ресурсам. Ці ресурси можуть бути фізичним устаткованням, комп'ютерною технікою, будівлею і навіть людськими ресурсами. Однак у кіберсвіті до майна також належить інформація, бази даних та програмні застосування. Тому протидія загрозам безпеці повинна містити захист від фізичних атак та кібератак.

Загрози безпеці ресурсам можуть виникнути в результаті випадкової події, а також навмисного нападу. Насправді, часто більший збиток може завдати відмова системи безпеки, відмова устаткування, недбалість і стихійне лихо, ніж результати цілеспрямованих нападів. Проте вдалі навмисні напади можуть мати величезні правові, соціальні та фінансові наслідки, які можуть значно перевищити фізичні втрати.

Енергокомпанії зазвичай оберігають устаткування від відмов та необережності, пов'язаної з захистом. До уваги беруть стихійні лиха, зокрема енергокомпанії, які зазвичай перебувають у зоні ураганів, землетрусів, циклонів, снігових бур тощо, хоча останні не залежать від енергокомпаній. Така мінливість є важливою для захисту інформації, яка стає все важливішим аспектом безпечної, надійної та ефективної роботи енергосистеми.

Оцінювання ризиків для захисту має життєво важливе значення у визначанні саме того, що має бути захищено, від яких загроз і якою мірою. Ключовим є визначання витрат і корисності: «один розмір не підходить усім»[4] (підстанціям), декілька рівнів безпеки краще, ніж одне рішення, і в кінцевому рахунку жодний захист від атак не може бути абсолютним. Проте існує значна різниця між крайнощами: нічого не робити і робити все, для забезпечування рівня безпеки, потрібного для сучасного керування енергокомпаніями.

Переваги також можна розглядати з іншого боку. Якщо є додатковий захист від можливих навмисних нападів, то це контролювання може бути використано для поліпшування безпеки, мінімізації недбалості та підвищування ефективності технічного обслуговування устаткування.

Наведене нижче — це деякі з найзначущіших загроз для розуміння й для захисту. Більшість із них означено в стандартах серії IEC 62351, принаймні у частині контролювання.

5.2.2 ***Незумисні загрози***

5.2.2.1 *Захист від збоїв*

Безпека завжди була одним з основних завдань енергокомпаній, особливо для тих, що працюють з підстанціями, де наявні високі рівні напруги. Ретельні процедури розробляли та вдосконалювали знову і знову для покращування безпеки. Хоча ці процедури є найважливішим складником програми безпеки, контролювання стану основного устаткування та реєстрування/сигналізування відповідності процедури щодо забезпечування захисту за допомогою електронних засобів можуть підвищити безпеку значною мірою та задовольнити інші цілі.

Зокрема безпека доступу, за якої допускають лише вповноважений персонал до підстанції, що реалізується в першу чергу з міркувань безпеки, та електронне контролювання таких заходів безпеки може також допомогти унеможливити деякі навмисні напади, такі як вандалізм та крадіжки.

5.2.2.2 *Збої устаткування*

Збої устаткування є найпоширенішими й очікуваними загрозами надійної роботи енергосистеми. Значну роботу було зроблено за останні роки для контролювання стану устаткування підстанцій, таких як температура мастила, системи охолоджування, відхили частоти, рівня напруги та сили струму перевантаження. Цей стандарт не розглядає ці види контролювання за винятком випадків, коли додаткова інформація може забезпечувати додаткову фізичну безпеку.

Однак часто контролювання фізичного стану устаткування також може поліпшити ефективність обслуговування, можливості унеможливлення окремих видів відмов устаткування, виявляння в режимі реального часу відмов, які раніше не помічали, і послідовного аналізування процесів і впливу збоїв устаткування. Таким чином, загальні витрати на контролювання фізичної безпеки може бути зменшено, якщо брати до уваги ці додаткові наслідки.

5.2.2.3 *Недбалість*

Недбалість є однією із «загроз» для захисту активів підстанції, чи то можливість проникнення на підстанцію або незамкнені двері, чи випадковий дозвіл на несанкціонований доступ до паролів, ключів та інших заходів безпеки. Часто неуважність є виявом самовпевненості («ніхто ще не пошкодив будь-яке устаткування на підстанції») або через лінь («навіщо зачиняти двері, якщо я йду в інше місце на кілька хвилин»), або від емоцій («ці заходи безпеки впливають на мою здатність виконувати свою роботу»).

5.2.2.4 *Стихійні лиха*

Стихійні лиха, такі як шторми, урагани та землетруси, можуть призвести до масштабних збоїв енергосистеми, підвищити рівень небезпеки, а також можливості для крадіжок, вандалізму та тероризму. Контролювання фізичного та інформаційного стану промислової мережі та устаткування в реальному часі може надати енергокомпаніям «очі й вуха», щоб зрозуміти, що відбувається, і вжити пом'якшувальних заходів для мінімізації наслідків цих стихійних лих на діяльність енергосистеми.

[4] У сенсі того, що одне просте рішення не може бути використано для будь-яких ситуацій, тому дозволено багатовекторне рішення.

5.2.3 *Зумисні загрози*

5.2.3.1 *Загальні положення*

Зумисні загрози можуть призвести до цілеспрямованого пошкодження об'єктів та устаткування на підстанціях, на відміну від незумисних. Стимули для зумисних загроз зростають через те, що результати успішних атак можуть мати велику економічну та/або «соціальну/політичну» вигоду для атакувальників. Складне контролювання об'єктів і устаткування може допомогти уникнути деяких з цих загроз до того, як посилиться вплив успішних атак через повідомлення в режимі реального часу та атак через інші країни.

5.2.3.2 *Незадоволений працівник*

Незадоволені працівники є однією з основних загроз для майна енергосистеми. Незадоволені працівники, які знають як зашкодити, можуть заподіяти більшої шкоди, ніж сторонні люди, зокрема, в галузі енергетики, де багато дуже специфічних систем і устаткування.

5.2.3.3 *Промислове шпигунство*

Промислове шпигунство у сфері енергосистеми стає все загрозливішим, оскільки за умови обігу мільйонів доларів дерегулювання та конкуренція забезпечує зростання стимулів для несанкціонованого доступу до інформації та можливість навмисного пошкодження устаткування. Крім фінансових вигод, деякі зловмисники можуть отримати «соціальну/політичну» вигоду внаслідок «викривання» некомпетентності або ненадійності конкурентів.

5.2.3.4 *Вандалізм*

Вандали можуть пошкодити об'єкти та устаткування без конкретних намірів нападу, а заради самого акту і щоб довести всім, що це можливо. Часто вандали не знають або не піклуються про можливі наслідки своїх дій.

Контролювання доступу на закриті об'єкти та тривога за будь-якого ненормального доступу в режимі реального часу може допомогти уникнути більшості актів вандалізму. Однак деякі акти вандалізму, такі як розстрілювання устаткування у дворі поза межами підстанції, чи вимикання устаткування та програмного забезпечення, потребує додаткових видів контролювання.

5.2.3.5 *Кіберхакери*

Хакери — це люди, які шукають слабкі місця в комп'ютерній безпеці для отримання вигоди. Ця вигода може бути безпосередньо грошова, або інформаційно-промислова, політична, соціальна чи лише для того, щоб переконатися, чи може хакер отримати доступ. Більшість хакерів користуються Інтернетом як основним ходом для зламу і саме тому більшість об'єктів застосовують фаєрволи, технологію ізолювання та інші засоби протидії, щоб відокремити систему керування енергосистемами від Інтернету.

Громадськість інформаційну безпеку часто вважає лише захистом від хакерів та пов'язаних з нею проблем комп'ютерних вірусів і «черв'яків». Комп'ютерні системи, які забезпечують роботу енергооб'єктів, зазвичай ізольовані від Інтернету, багато співробітників об'єкта не бачать жодних причин для долучання заходів безпеки для цих систем. Однак зрозуміло, це уже не є правильним, тому що мережа розширюється і зростають додаткові вимоги щодо доступу до інформації (наприклад, надання віддаленого доступу, доступ для обслуговування, під'єднання через ноутбук, доступ інженера релейного захисту для отримання спеціальних даних тощо).

5.2.3.6 *Віруси та «черв'яки»*

Як і хакери, віруси та «черв'яки» зазвичай атакують через Інтернет. Проте деякі віруси та «черв'яки» можуть бути впроваджені в програмне забезпечення, що завантажується в систему, ізольовану від Інтернету, або могли передатися через захищені комунікації з небезпечного ноутбука або іншої системи. Вони можуть містити віруси, залежні від людських дій, програми-шпигуни для збирання даних про енергосистему, а також інші троянські програми.

5.2.3.7 *Крадіжки*

Ціль крадіжки проста — чимось заволодіти (устаткованням, даними або знанням), на що не мають права. Зазвичай ціль має фінансову вигоду як мотив, хоча можуть бути й інші мотиви.

Так само контролювання доступу на закриті об'єкти та відстежування фізичного стану й справності устаткування (наприклад, немає відповіді чи роз'єднання) є основними методами для сповіщення персоналу, що можливо відбувається крадіжка.

5.2.3.8 *Тероризм*

Тероризм є найменш вірогідною загрозою, але має великі наслідки, оскільки головна ціль тероризму — нанесення максимальних фізичних, фінансових та соціальних/політичних збитків.

Контролювання та відстежування доступу (зокрема фізичний доступ) до об'єктів підстанції є, можливо, найефективнішим засобом для оповіщення персоналу про потенційні терористичні акти, такі як фізично підірвано підстанцію або інший об'єкт. Проте терористи можуть стати вправнішими в своїх діях і прагнути до пошкодження спеціального устаткування чи виведення з ладу критично важливого устаткування так, що це потенційно може завдати більшої шкоди енергосистемі загалом, ніж просто вибух однієї підстанції. Таким чином, додаткові види контролювання мають вирішальне значення, зокрема для стану й справності устаткування.

5.3 Вимоги до захисту від загроз, вразливостей, атак та до контрзаходів

5.3.1 *Вимоги щодо безпеки*

Користувачі — люди або програмне забезпечення, потребують не менше чотирьох пунктів безпеки, що захищають їх від чотирьох основних загроз. У будь-якому випадку авторизація потребує ідентифікування користувачів як основної передумови для:

— конфіденційності — унеможливлення несанкціонованого доступу до інформації;

— цілісності — унеможливлення несанкціонованої зміни або крадіжки інформації;

— доступу — унеможливлення відмови під час обслуговування та забезпечення санкціонованого доступу до інформації;

— ретельне виконання обов'язків або простежуваність — уникнення відмови під час дії, що відбулася, або право на дію, що не відбулася.

5.3.2 *Загрози безпеці*

Загалом є чотири типи інформаційних загроз безпеці:

— несанкціонований доступ до інформації;

— несанкціонована зміна або крадіжка інформації;

— відмова обслуговувати;

— відмова від повідомлення/неможливість ідентифікування.

Однак є багато різних видів уразливості та способів нападу через цю уразливість, за допомогою яких атаки можуть бути успішними. Контрзаходи безпеки враховують різні види вразливості й способи атак.

5.3.3 *Уразливість безпеки*

Уразливість інформаційної безпеки належить до слабкостей або відкритості системи, які б дали змогу реалізувати навмисні чи випадкові несанкціоновані загрозливі дії. Уразливість може бути результатом помилки або конструктивних недоліків у системі, але може також виникнути в результаті відмови устаткування та фізичних дій. Уразливість може бути або тільки теоретично, або може бути цілком відомим засобом атаки.

5.3.4 *Атаки на безпеку*

Загрози може бути зреалізовано різними типами атак, деякі з них наведено на рисунку 1. Як показано, той самий тип атак часто може бути задіяно для різних загроз безпеці. З такої розгалуженості потенційних атак випливає, що не існує лише одного методу виконання конкретних вимог щодо безпеки: необхідно протидіяти кожному типу атаки, який представляє певну загрозу.

До того ж «ланцюг атак», в якому послідовність атак, спроможних залучати різні активи і тривати якнайдовше, може також зреалізувати наявну загрозу.

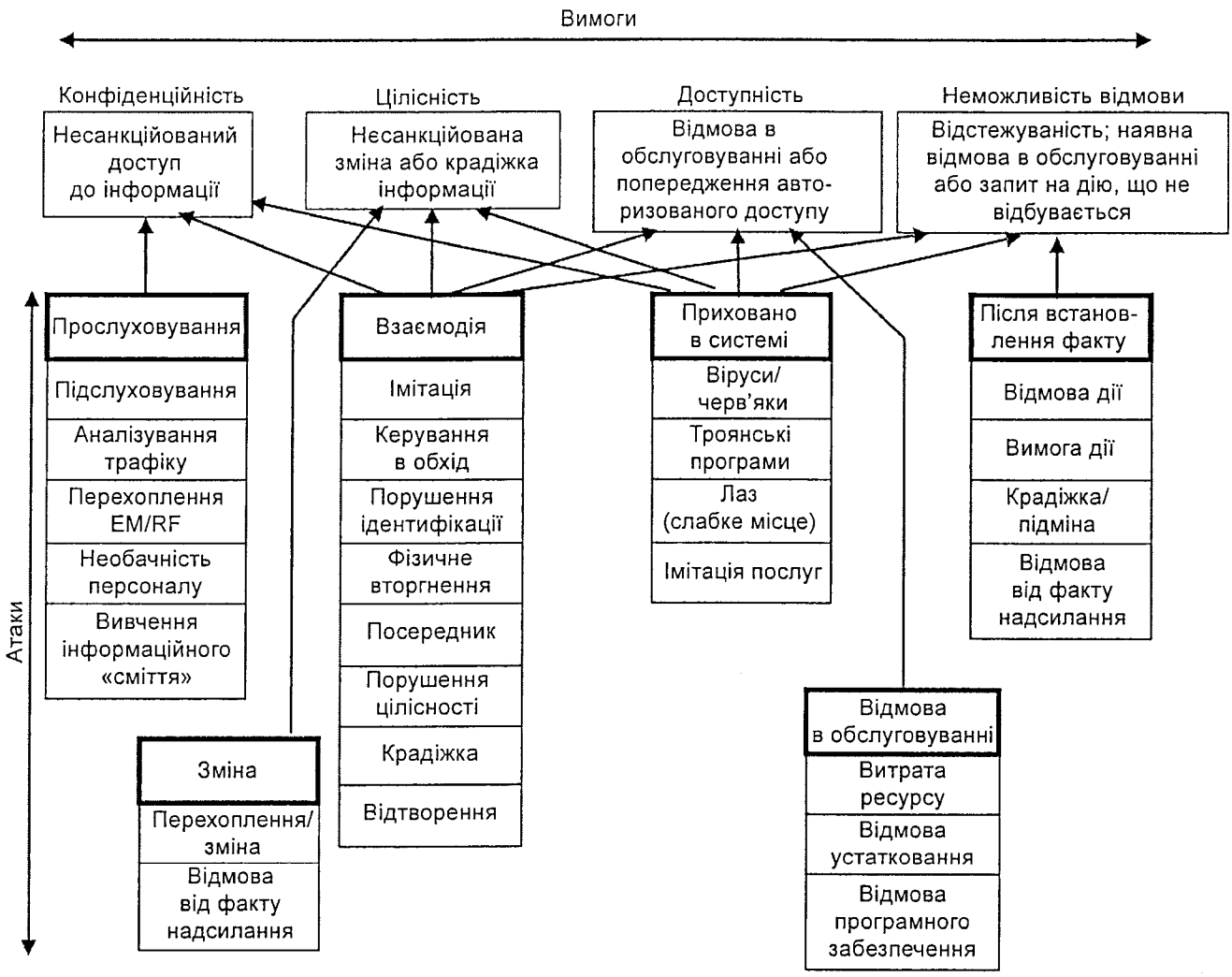

Рисунок 1 — Вимоги щодо безпеки, загрози і можливі атаки

5.3.5 *Категорії безпеки*

З одного боку, інформаційну безпеку можна поділити на чотири категорії (див. рисунок 2). Ці категорії наведено нижче.

Зазвичай усі чотири категорії повинні містити заходи безпеки, застосовні для досягнення захисту інформації під час передавання. Виконання лише однієї категорії зазвичай не ефективно. Наприклад, впроваджена VPN обробляє лише загрози транспортним протоколам зв'язку і не заважає особі маскуватися під іншу чи не захищає від проникнення шкідливого програмного забезпечення від головного комп'ютера через VPN до навколишніх пристроїв.

Ці заходи безпеки мають бути ретельно поєднані один з одним так, щоб не виникало непередбачених проблем.

5.3.6 *Заходи протидії загрозам безпеки*

Заходи протидії загрозам безпеки, як показано на рисунках 3—6, також впливають на взаємопов'язані технології та правила. Не всі заходи протидії загрозам безпеки потрібні або бажані весь час для всіх систем: це буде забагато і призведе до того, що вся система буде непридатною або дуже повільною. Тому цей перший крок має визначити, які заходи протидії корисніші для досягнення потрібної цілі. Огляд усіх заходів протидії наведено на рисунку 7.

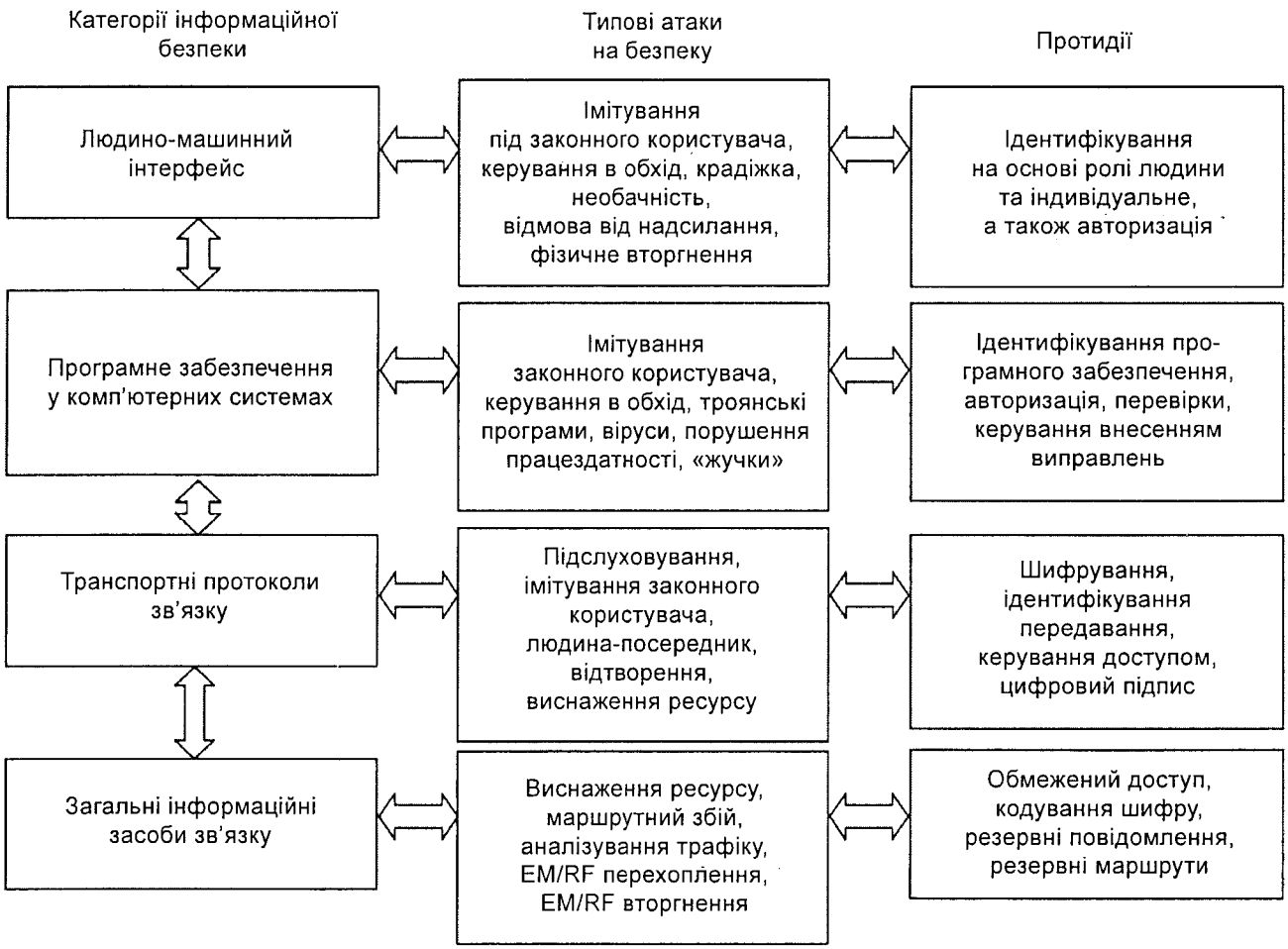

Рисунок 2 — Категорії безпеки, типові атаки та відповідні контрзаходи

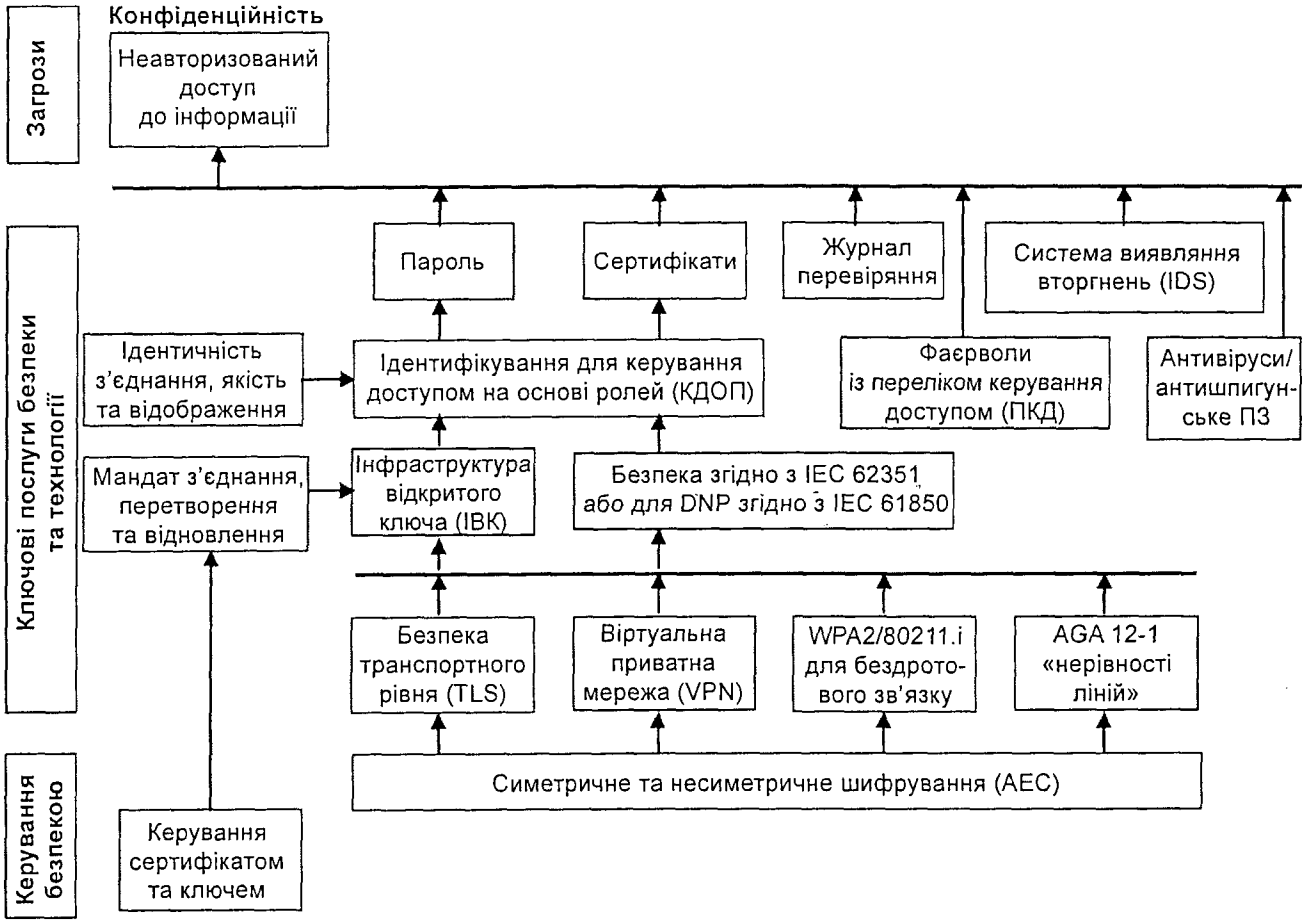

Рисунок 3 — Заходи протидії для конфіденційності безпеки

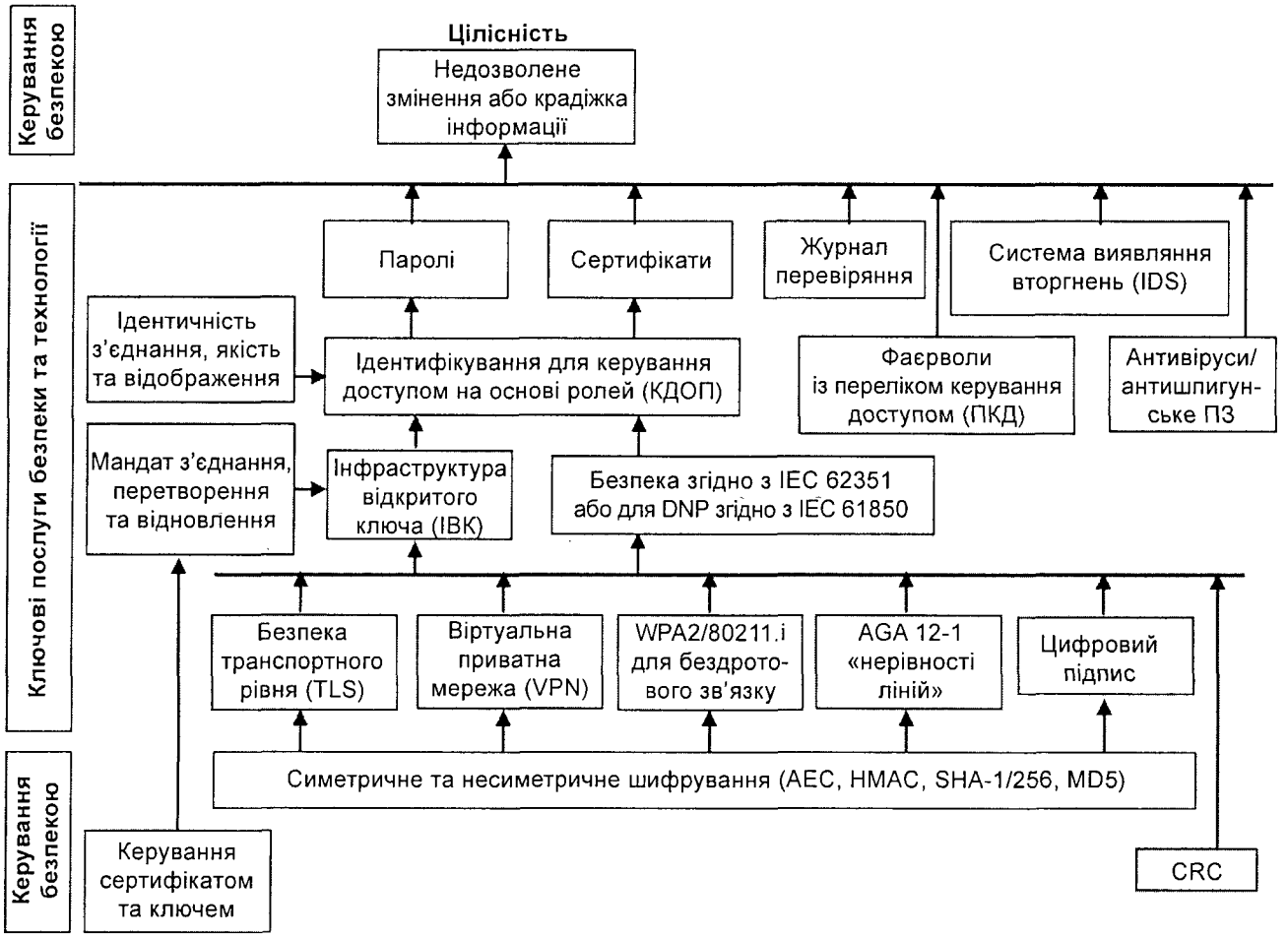

Рисунок 4 — Заходи протидії для цілісності безпеки

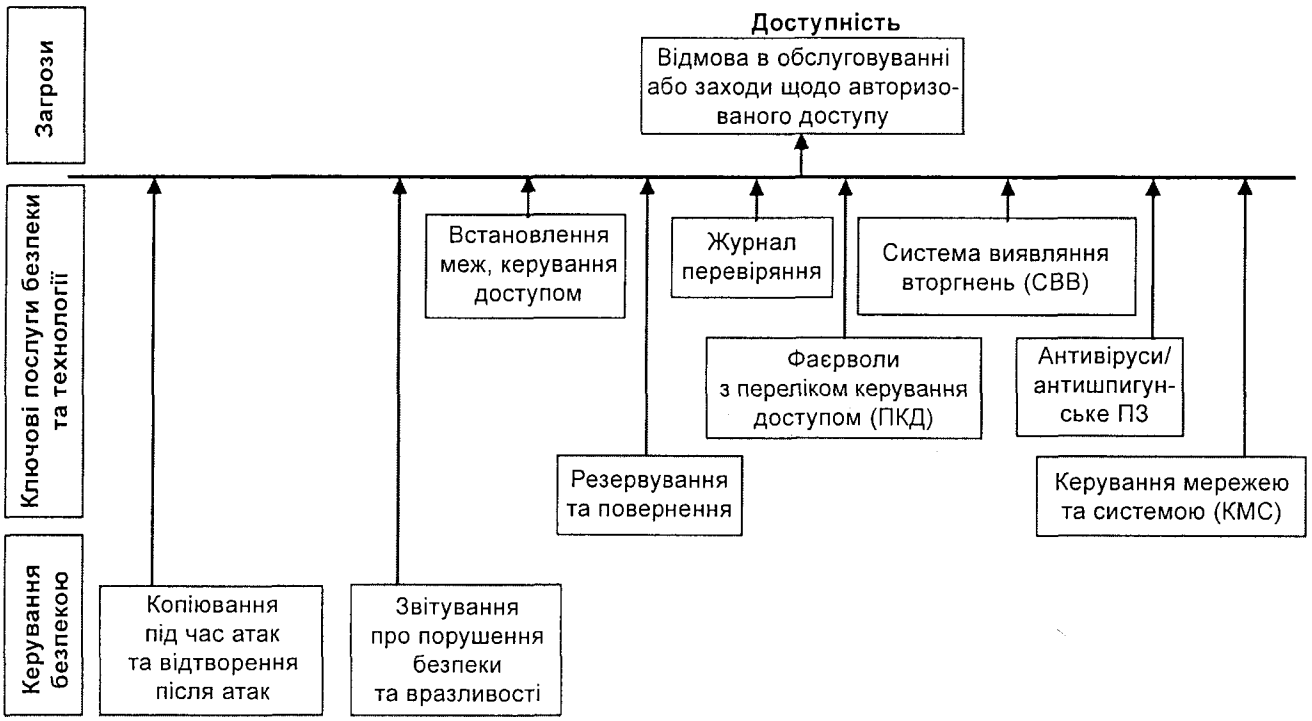

Рисунок 5 — Заходи протидії для доступу

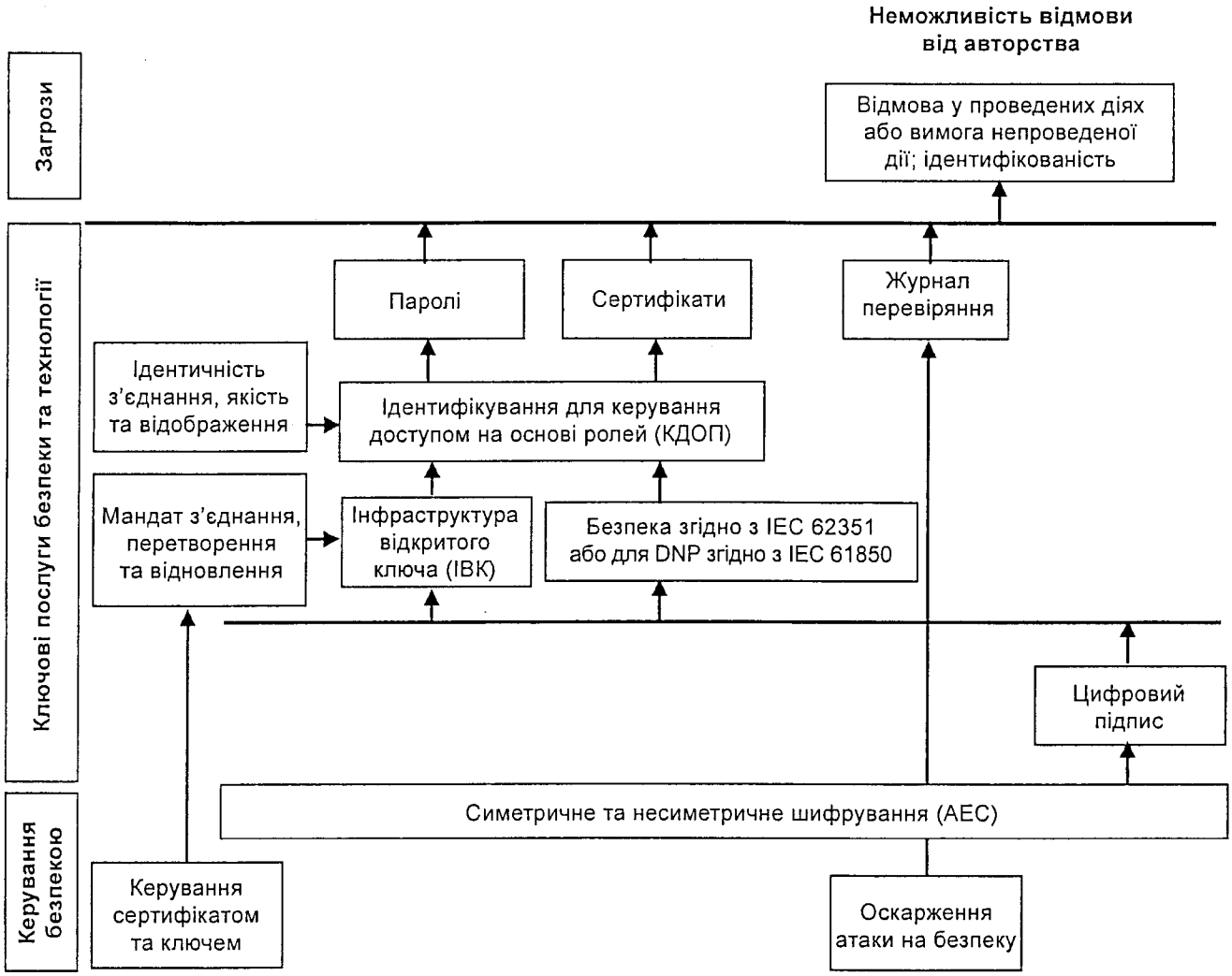

Рисунок 6 — Заходи протидії для визначання джерела надсилання

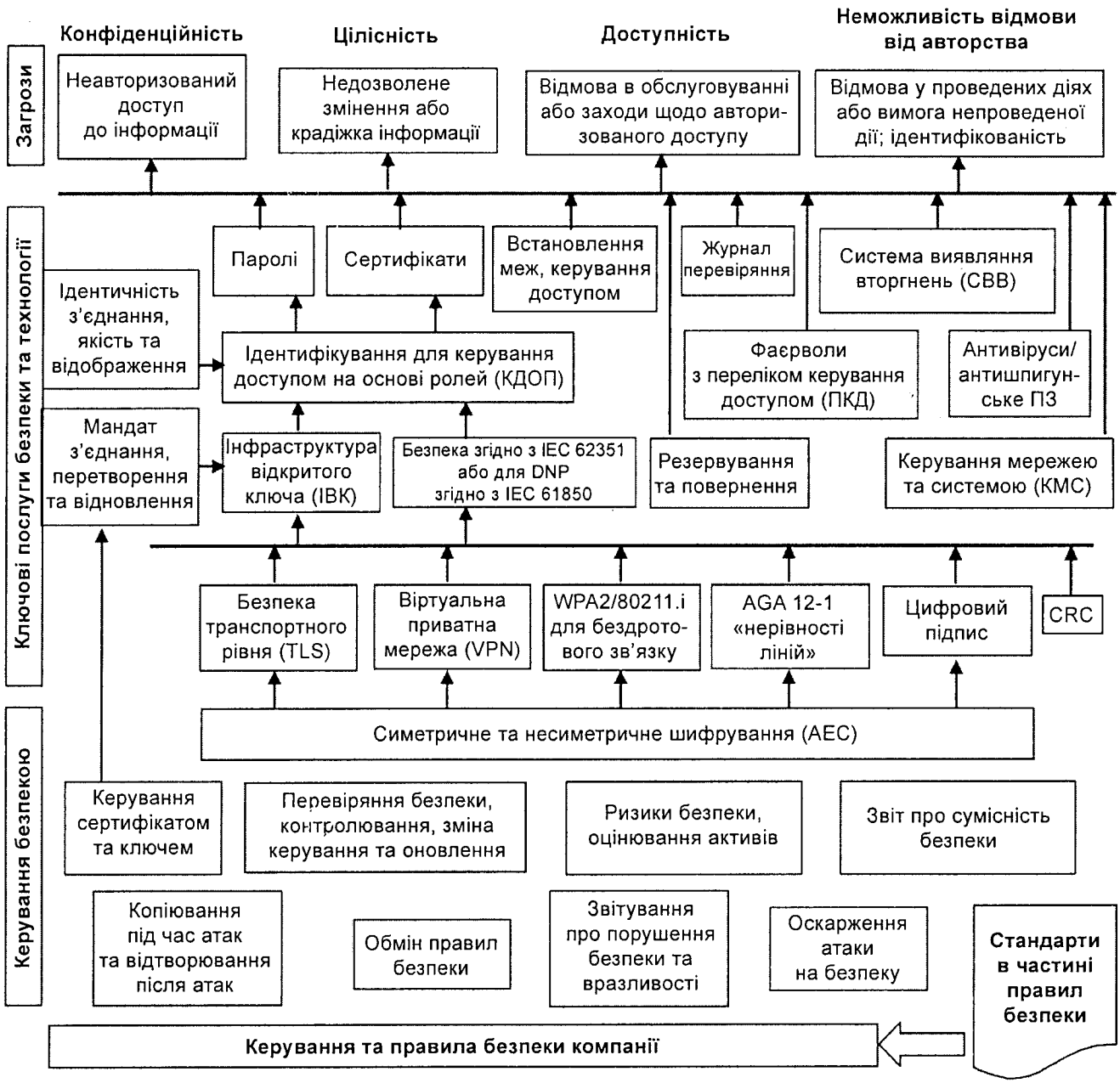

Рисунок 7 — Загальна безпека: вимоги безпеки, загрози, контрзаходи та керування

Ці рисунки мають лише інформативний характер, на них відображено не всі питання, що стосуються серії стандартів IEC 62351.

На рисунках 3—7 чотири вимоги безпеки (конфіденційності, цілісності, доступності та визначення джерела надсилання) відображено у верхній частині кожного рисунка. Основні загрози безпеці наведено нижче кожної вимоги. Ключові служби безпеки й технології, використовувані для боротьби з цими загрозами, наведено в блоках безпосередньо під загрозами. Це лише приклади найчастіше вживаних заходів безпеки, де стрілки означають, які технології та служби задіяні у підтримуванні їхніх заходів безпеки. Наприклад, шифрування використовують у багатьох заходах безпеки, охоплюючи TLS, VPN, захист бездротового зв'язку, і технологій апаратного реалізування безпеки. Це, в свою чергу, відповідає стандартам у частині безпеки IEC 62351 та ІВК, які загалом використовують для ідентифікування, тому їх паролі та сертифікати можуть бути взаємопов'язаними. У нижній частині кожного рисунка, нижче послуг безпеки і технологій, показано керування безпекою та правила безпеки, які забезпечують фундамент для всіх заходів безпеки.

5.3.7 *Аналізування загалу проблем безпеки*

Безпека охоплює надзвичайно складний і багатовимірний комплекс питань. Немає стандартизованих або чітко визначених механізмів для аналізування загалу проблем безпеки, і, отже, аналізування та впроваджування належних повних заходів безпеки в економічно-ефективному плані часто сприймають як нездійсненне завдання.

Наприклад, у минулому використовували два основних методи аналізування вимог щодо безпеки: аналізування на основі конкретного підприємства (один набір заходів безпеки, застосовний для всього підприємства) і аналізування на основі технологій/загроз (один набір технологій, таких як паролі та VPN, застосовний до всіх систем). Обидва підходи мають очевидні недоліки. Спроба розробити єдиний набір заходів безпеки для будь-якого підприємства може призвести до надлишковості або недостатньої безпеки для певних ділянок підприємства. Крім того, підприємство постійно розвивається і змінюється, і містить більше одного суб'єкта господарювання, тому не може бути застосовано один набір правил безпеки та технологій. Аналіз технологічний та оснований на загрозах допускає незмінність заходів безпеки, тому одне рішення є достатнім для всіх ситуацій. Проте це не відповідає дійсності, особливо в середовищі керування енергосистемами. Єдиного формату просто немає. Крім того, оскільки захист постійно розвивається, вибір типу безпеки, основаної на сучасних технологіях, може перешкодити впровадженню досконаліших технологій безпеки в майбутньому. Таким чином, будь-які рішення стосовно безпеки потребують значного координування і можуть призвести до того, що процес забезпечування безпеки буде оманливим, якщо не зовсім неможливим.

Однак проблеми безпеки можна розкласти на дрібніші ділянки аналізування/керування безпекою. Використовують три основні підходи, залежно від завдань. Це такі:

— фізичний периметр безпеки: шість стін фізичного кордону оточує комп'ютерні зали, телекомунікаційні кімнати, центри керування, а також інші місця, в яких розміщено критично важливе забезпечення, доступ до якого контролюють. Цей периметр може бути використано для фізичного захисту активів;

— електронна безпека периметра: логічні кордони оточувальної мережі, до якої під'єднано критично важливе забезпечення, доступ до якого контролюється. Цей периметр може бути використано для застосовування заходів комп'ютерної безпеки;

— безпека домену: ділянка, яка організаційно належить одній секції, відділу, компанії, або іншого підрозділу, де вимоги щодо безпеки можуть бути однаковими або, принаймні, під контролем тієї самої особи. Концепція безпеки домену, зокрема, відкриває набір ресурсів, які повинні бути керованими (в частині безпеки) самостійно, так як усе забезпечення разом із безпекою домену належить одній організації.

Розділення загалу проблем безпеки на керовані частини може значно допомогти організації розробити належні та економічно ефективні заходи безпеки. Однак виникає питання, як забезпечити механізм убезпечування для міждоменних бірж або через периметри безпеки. Щоб вирішити цю проблему, спеціальним міждоменним службам безпеки потрібно перетинати ці межі.

5.4 Важливість правил безпеки

Документи щодо правил безпеки описують основні загрози для об'єктів компанії, пояснюють причини залучання працівників для підтримування безпеки інформації про компанію, а також визначають права й обов'язки працівників компанії, зокрема користувачів та IT-персоналу.

Як доповнення до документів щодо правил безпеки, ґрунтовні вимоги щодо безпеки мають бути розроблені для вирішення конкретних питань безпеки, пов'язаних із конкретними технологіями і програмним забезпеченням, зокрема рішеннями конфігурації IT-мережі, з питаннями продуктивності мережі, розташування і налаштування фаєрволів, класифікації безпеки даних, з вимогами протоколу безпеки, а також запитом пароля/сертифіката.

Одне з основних призначень цього документа — навчальний посібник. Співробітники будуть підтримувати заходи безпеки охочіше і ретельніше, якщо вони розуміють реальні загрози, ризики безпеки, пов'язані з повсякденними функціями і діями заходів безпеки, які вони будуть вповноважені підтримувати, щоб мінімізувати ці ризики. Політика безпеки має бути також зрозумілою в частині дисциплінарних заходів, які може бути впроваджено, коли не дотримано правил.

Документ щодо правил безпеки має бути чинним з урахуванням нових технологій і нових вимог щодо безпеки. Його треба переглядати і вносити зміни не менше ніж один раз на рік, або кожного разу, коли трапляються нові події в сфері безпеки або в ІТ-устаткованні.

5.5 Оцінювання ризику безпеки

Ще одне питання, як правило, найскладніше полягає у вирішенні того, що має бути захищене і якою мірою воно має бути захищене. Хтось може стверджувати, що всі об'єкти мають бути захищені стовідсотково, але зазвичай це недоцільно. Крім того, такий підхід робить використовування/адаптування безпеки надзвичайно дорогим і може завадити органам, які відповідають за безпеку, спробувати впровадити навіть мінімальну безпеку.

Єдиний варіант не підходить усім: усі активи не мають бути повністю та надмірно захищені, хоча всі вони можуть бути захищені. Проте всі активи мають оцінюватися з урахуванням потреби й ступеня безпеки.

Оцінювання ризиків для безпеки визначає ступінь пошкодження, до якого може призвести порушення правил безпеки, і забезпечує аналіз збитку (фінансового, соціального, а також збереження) щодо витрат на впроваджування і підтримування протидії з боку системи безпеки. Таким чином, оцінювання ризиків для безпеки є ключовою функцією безпеки, яку має бути подано до початку будь-якого впроваджування системи безпеки.

5.6 Розуміння вимог щодо безпеки та впливу заходів безпеки на керування енергосистемою

5.6.1 *Проблеми безпеки під час керування енергосистемою*

Керування енергосистемою ставить багато викликів безпеці, що відрізняються від більшості інших галузей промисловості. Наприклад, більшість заходів безпеки було розроблено для боротьби проти хакерів в Інтернеті. Середовище Інтернет сильно відрізняється від середовища керування енергосистемою. Тому в індустрії безпеки зазвичай є недостатнє розуміння вимог щодо безпеки і потенційного впливу заходів безпеки на потрібний обсяг інформаційного обміну під час керування енергосистемою.

Зокрема, послуги безпеки й технології було розроблено, насамперед, для галузей, які не потребують суворого виконання та надійності, потрібних для керування енергосистемою. Наприклад:

— ненадання доступу авторизованому диспетчеру до керування підстанцією може мати серйозніші наслідки, ніж ненадання доступу клієнтові до свого власного банківського рахунка. Таким чином, загроза відмови в обслуговуванні є набагато важливішою, ніж більшість типових операцій в Інтернеті;

— більшість каналів зв'язку, використовуваних в енергетиці, — вузькосмугові, кінцеві пристрої часто обмежені в пам'яті та обчислювальних потужностях, тим самим не допускаються певні додаткові інформаційні витрати, потрібні для певних заходів безпеки, таких як шифрування даних і обмін ключами;

— більшість систем і устаткування перебувають в ізольованих некерованих віддалених місцях, які не мають доступу до Інтернету. Це робить керування ключами, відкликання сертифікатів, а також певні заходи безпеки складними для реалізування;

— багато систем пов'язано багатоточковими каналами зв'язку, таким чином, типові для промисловості заходи безпеки мережі не можуть бути застосовані;

— хоча бездротові комунікації починають широко використовувати для багатьох застосувань, енергокомпанії мають дуже обережно поставитися до того, де і які функції виконують ці бездротові технології, частково через завади у середовищі електричних підстанцій (потенційний вплив на доступність), а частково через потребу деяких застосувань щодо швидкої та надзвичайно надійної відповіді (пропускна здатність). Хоча заходи безпеки доступні для багатьох бездротових систем, це може збільшити додаткові інформаційні витрати (подібно до дротових засобів передавання інформації).

5.6.2 *Керування ключами та анулювання сертифікатів*

Враховуючи значні території, вузькосмугові канали зв'язку, обмежені можливості деяких кінцевих пристроїв, а також віддаленість великої кількості устаткування для легкого доступу персоналу, керування шифруванням секретних ключів є завданням, з яким більшість інших галузей, зокрема обробна промисловість, не стикаються. Секретні ключі, такі як загальноіндивідуальна система ключів або симетрична система таємного ключа чи використання шифрувальних пристроїв як «буфер середовища», мають бути розміщені в кінцевих пристроях в безпечному режимі.

Однією з можливостей для техніків є виїзд до устаткування та завантаження кожного секретного ключа на кожну одиницю устаткування. Цей варіант підходить для початкових установок, але може стати значною проблемою, якщо ключ потрібно регулярно оновлювати. Ще однією альтернативою є «сервер ключів», який розміщують разом із кінцевими пристроями та взаємозалежним устаткуванням через локальну мережу. Сервер ключів може потім використовувати окремий широкосмуговий безпечний зв'язок для завантаження нових секретних ключів, які він може видавати різним одиницям устаткування.

Анулювання сертифіката має аналогічні проблеми для керування ключами, за винятком того, що обмеження не полягає у вузькій смузі пропускання каналу зв'язку, а в тому, що експлуатаційне устаткування фактично не може бути під'єднано до Інтернету. Зазвичай анулювання сертифіката обробляє довірений менеджер сертифікатів, який запитує анулювання через Інтернет у момент встановляння наявності проблеми з сертифікатом. В керуванні енергосистемами має бути передбачено певний спосіб надійного отримання оголошення про анулювання через Інтернет і далі надійного передавання в строк цього анулювання відповідному кінцевому пристрою.

5.6.3 ***Керування системою та мережею***

Інформаційну інфраструктуру в системі керування електроенергетики зазвичай не розглядають як єдину інфраструктуру, а розглядають як сукупність окремих каналів зв'язку, баз даних, кількох систем, а також різних протоколів. SCADA-системи часто виконують певне мінімальне контролювання зв'язку, наприклад, чи є доступними канали зв'язку для RTU, а потім, якщо зв'язок втрачено, вони помічають дані як «недоступні». Однак це завдання обслуговувального персоналу — знайти, в чому проблема, яке устаткування постраждало, де воно розташоване, і що потрібно зробити, щоб усунути проблему. Це тривалий і специфічний процес. У середньому енергосистема не контролюється нормально, а певні керувальні дії не можуть бути виконані. Як показав аналіз аварії 14 серпня 2003 р. — від'єднання північно-східного узбережжя Сполучених Штатів, основна причина від'єднання — не було доступу до критичної інформації у споживача в потрібний час.

Кожна енергокомпанія відрізняється тим, яка інформація доступна для її обслуговувального персоналу. Телекомунікаційні техніки, як правило, відповідають за відстежування будь-яких проблем короткохвильових чи оптико-волоконних кабелів; провайдери телекомунікаційних послуг повинні відстежувати свої мережі, адміністратори баз даних повинні визначати, чи правильно завантажуються дані з систем автоматизації підстанцій або з баз даних СГІ; інженери протоколів повинні виправляти помилки в протоколах; інженери-програмісти повинні визначати несправність роботи програми, незбіжність результатів, або зациклювання; оператори повинні фільтрувати великі обсяги даних, щоб визначити, по можливості, коли «проблема енергосистеми» є насправді «проблемою інформаційної системи».

У майбутньому проблема керування інформацією ставатиме все складнішою. Системи SCADA більше не будуть мати виняткове контролювання зв'язку в сферах, які можуть підтримуватися провайдерами телекомунікаційних послуг, або корпоративними мережами, чи іншими енергокомпаніями. Програмне забезпечення, критичне для надійності енергосистем, буде працювати на інтелектуальних електронних пристроях (IDE), які самі будуть відстежувати й унеможливлювати «падіння» програмного забезпечення і збої системи. Віддалені пристрої будуть взаємодіяти з іншими віддаленими пристроями, використовуючи канали, які не будуть перебувати під наглядом будь-якої системи SCADA. Інформаційні мережі на підстанціях будуть спиратися на локальні «самовідновлювані» процедури, за якими також не будуть явно наглядати або контролювати сьогоднішні системи SCADA.

5.7 П'ятиступінчаста послідовність забезпечення безпеки

Захист і убезпечення мережі, інтелектуального устаткування, а також даних та інформації, які є життєво важливими для керування майбутньою енергосистемою, — це одне з ключових питань після розроблення архітектури виробничого рівня. Інформаційна безпека стикається зі значними проблемами як організаційними, так і технічними в таких основних напрямках:

— потреба підвищування рівня інтегрування з різними суб'єктами господарювання;

— ширше використовування інфраструктур на основі відкритих систем, які буде охоплювати майбутня енергосистема;

— потреба відповідного інтегрування наявних або «застарілих» систем із майбутніми системами;

— зростає розвиненість та складність інтегрованих розподілених обчислювальних систем;

— зростає розвиненість і загрози з боку вороже налаштованих груп.

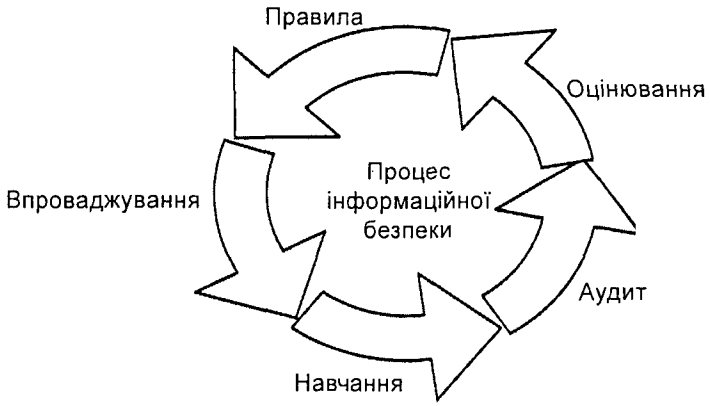

Рисунок 8 — Загальний процес забезпечення безпеки — безперервний цикл

Безпеку має бути сплановано й розроблено в системах до початку роботи. Функції безпеки є невід'ємною частиною розробляння систем. Планування безпеки ще до її реалізовування забезпечить повніше та економічно ефективніше рішення. Крім того, перспективне планування гарантує, що послуги безпеки можуть підтримуватися (може дорого коштувати модернізація) незапланованим оточувальним обладнанням. Це означає, що безпека має поширюватися на всі рівні архітектури.

Як наведено на рисунку 8, безпека не є статичним процесом, вона постійно розвивається. Вона потребує тривалої роботи й підготовляння, щоб підтримувати процеси безпеки згідно з вимогами до систем. Безпека продовжує бути змаганням на випередження між корпоративними правилами безпеки/інфраструктурою безпеки та вороже налаштованими групами. Процеси безпеки і системи розвиватимуться в майбутньому. Зазвичай немає 100-відсоткового захищеного зв'язку між пов'язаними системами. Завжди будуть дрібні ризики, які має бути враховано і скеровано. Таким чином, з ціллю підтримування безпеки потрібна постійна пильність та контролювання так само, як і адаптування до змін в усьому навколишньому устаткованні.

Весь процес відображено п'ятьма процесами високого рівня, які є складниками стратегії надійної безпеки. Незважаючи на циклічний характер, є певний порядок процесу.

Оцінювання безпеки — процес оцінювання активів у частині їх вимог щодо безпеки, ґрунтується на можливих ризиках нападу, відповідальності, пов'язаній з успішними атаками, і витратами на зменшення ризиків та зобов'язань. Рекомендації, що випливають з аналізування вимог щодо безпеки, стосуються розробляння правил безпеки, закупівлі, пов'язаних із безпекою продуктів і послуг, а також розроблення процедур безпеки.

Сенс циклічного процесу в тому, що оцінювання безпеки потребує періодичності. Для періодичного перегляду згідно з правилами має бути визначено строки переоцінювання.

Однак політика потребує постійного розвитку технологічних змін та зміни правил, що може потребувати негайного переоцінювання.

Правила безпеки — формування правил безпеки є процесом розроблення правил керування, реалізування та інсталяції безпеки в домені безпеки. Переглядають рекомендації, створені оцінкою безпеки, і розробляють та підтримують протягом тривалого часу правила, що забезпечують впровадження рекомендацій безпеки. Правила безпеки мають бути старанно опрацьовані в частині забезпечення безпеки, що визначає ґрунтовне реалізування заходів безпеки, графік реалізування цих заходів, а також процес переглядання для визначання результатів і поновлення плану.

Впровадження системи безпеки — сукупність закупівлі, встановляння та тестування продукції та послуг безпеки, а також реалізування розроблених правил і процедур безпеки. В рамках використання окремих правил безпеки має бути зреалізовано кілька процедур керування, які дають змогу виявляти вторгнення та дають можливість контрольних перевірянь.

Навчання заходів безпеки — необхідне безперервне навчання загрозам безпеці, технологіям убезпечення, а також корпоративним і правовим стратегіям, що впливають на безпеку. Загрози безпеці та технології постійно розвиваються і потребують поточного аналізування й підготовляння персоналу для впровадження і підтримування потрібної інфраструктури безпеки.

Аудит безпеки (моніторинг) — перевіряння систем та засобів безпеки є процесом, відповідальним за виявляння атак, прогалин у системі безпеки, а також оцінювання ефективності встановленої інфраструктури безпеки. Однак перевірення зазвичай застосовують після звершення події/вторгнення. Модель безпеки домену, як і активна інфраструктура безпеки, потребує постійного контролювання. Таким чином, процес аудиту має бути вдосконалено.

У разі спроби розвинути процес безпеки на базі підприємства неможливо врахувати всі суб'єкти підприємницької діяльності, політики й технологічних рішень, які можуть бути вибрані різними відділами, що функціюють на підприємстві. Тому обговорення питання безпеки на рівні підприємства часто є складним завданням, яке може ніколи не завершитися. Для того щоб спростити обговорення, дають змогу різним відділам керувати власними ресурсами і зосереджувати обговорення на важливих аспектах, систему безпеки потрібно розглядати в частині дії безпеки.

5.8 Застосування безпеки керування енергосистемою

Через велику різноманітність засобів зв'язку та експлуатаційних характеристик, а також через той факт, що жоден захід безпеки не може протистояти всім видам загроз, очікується, що буде зреалізовано декілька рівнів безпеки. Наприклад, VPN захищає лише протоколи транспортного рівня, але не забезпечує захист протоколів прикладного рівня, тому додаткові заходи безпеки, наведені в IEC 62351-4, надають безпеку на рівні застосування, та можуть працювати над VPN. Крім того, паролі особистого доступу, виявляння вторгнень, переліки керування доступом, закриті входи, а також інші заходи безпеки потрібні для забезпечення додаткового рівня безпеки.

З рисунків 3—7 зрозуміло, що ідентифікування відіграє велику роль у багатьох заходах безпеки. Насправді для більшості команд енергосистеми ідентифікування керувальних дій є набагато важливішим, ніж «приховання» даних шифруванням. Дуже важливо, щоб мали місце лише авторизовані керувальні дії.

Також через те, що під'єднання до Інтернету не має бути основним чинником, оскільки команди енергосистеми повинні бути добре захищені ізоляцією та/або фаєрволами, деякі із загальних загроз менш критичні, тоді як інші критичніші. Хоча важливість конкретних загроз може дуже варіюватися залежно від об'єктів, що охороняються, деякі з найсерйозніших загроз у керуванні енергосистемами це:

— з провини персоналу — працівники чіпляють свої паролі на монітори своїх комп'ютерів або залишають двері розблокованими;

— в обхід керування — працівники вимикають засоби безпеки, не змінюють паролі за промовчанням, або кожен використовує той самий пароль для доступу до всього устаткування підстанцій. Або програмне застосування вважає, що перебуває в безпечному середовищі, тому не перевіряє справжність своїх дій. Або запасний доступ виробника використовуваний не за призначенням;

— через невдоволених працівників — невдоволений працівник має знання щодо виконання дій, які можуть навмисно чи ненавмисно завдати шкоди діяльності енергосистеми (навіть спроба зіграти безневинний жарт з іншим працівником);

— через порушення авторизації — дехто виконує дії, на які він не має дозволу, іноді через порушення правила авторизації, або маскуванням під авторизованого користувача, крадіжки, або інших незаконних засобів;

— атака з використанням технології «незаконний посередник» — шлюз, сервер баз даних, канали зв'язку або інше некінцеве устаткування перебуває під загрозою, якщо дані, які проходять через це проміжне устаткування, читаються або змінюються перед відправленням за призначенням;

— через вичерпання ресурсів — устаткування випадково (чи навмисно) перевантажується і тому не може виконувати свої функції. Або закінчився строк чинності сертифіката і блокується доступ до устаткування. Ця відмова в обслуговуванні може серйозно вплинути на керування енергосистемою.

6 ОГЛЯД СТАНДАРТІВ СЕРІЇ IEC 62351

6.1 Сфера застосування стандартів серії IEC 62351

Стандарти, що поширюються на безпеку, було розроблено для різних профілів трьох протоколів зв'язку: стандарт IEC 60870-5 і його частини, стандарт IEC 60870-6 (TASE.2) та стандарти серії IEC 61850. Крім того, розглянуто безпеку мережі й системи керування. Ці стандарти, що поширюються на безпеку, мають відповідати різним цілям безпеки для різних протоколів, які різняться тим, як їх використовують. Деякі зі стандартів, що поширюються на безпеку, можна використовувати через певні протоколи, у той час як інші є дуже специфічними для певного профілю.

6.2 Ідентифікування як ключова вимога безпеки

Одним з основних напрямків стандартів серії IEC 62351 є ідентифікування, яке є рішенням для трьох із чотирьох основних загроз безпеці: конфіденційності, цілісності та безвідмовності. Стандарти серії IEC 62351 можуть стосуватися лише безпеки зв'язку, але вони намагаються забезпечити механізм, за допомогою якого може бути підтримано ролеву модель керування доступом (КДОП) у рамках впроваджування. КДОП може забезпечити захист від цих трьох загроз на рівні користувача та/або програмного забезпечення. Для того щоб забезпечити цю основу для КДОП, щонайменше потрібно ідентифікування зв'язку на рівні застосовувань.

6.3 Призначеність стандартів серії IEC 62351

Цілі безпеки охоплюють ідентифікування суб'єкта через цифровий підпис, що забезпечує лише санкціонований доступ, унеможливлення підслуховування, відтворювання та імітування зв'язку, і якоюсь мірою виявляння вторгнень. Для деяких конфігурацій важливі всі ці аспекти; для інших лише деякі з них, застосовані через обмеження обчислювальної потужності певних промислових пристроїв, через обмеження швидкості обміну інформації, через вимоги швидкої відповіді для релейного захисту, чи через потребу отримання дозволу на роботи в тій самій мережі як захищених, так і незахищених пристроїв.

Деякі вимоги щодо безпеки, описані в інших пунктах, не є предметом розгляду стандартів серії IEC 62351, оскільки вони пов'язані з правилами безпеки, навчанням персоналу, а також розробляннням і впроваджуванням системних рішень. Крім того, реєстрування та звіти про події й сигнали тривоги, які вже наявні в протоколах стандартів IEC, як очікується, будуть використовувати для ведення аудиту.

Таким чином, серію стандартів IEC 62351 було зосереджено на надання таких характерних заходів безпеки:

— Ідентифікування для мінімізації загрози атак відповідно до технології «незаконний посередник».

— Ідентифікування для мінімізації деяких видів обхідного керування.

— Ідентифікування для мінімізації безвідповідальності та дій незадоволеного працівника.

— Ідентифікування суб'єктів за допомогою цифрових підписів:

— забезпечування лише авторизованого доступу до інформації;

— керування доступом до зв'язку.

— Конфіденційність ключів ідентифікування шифруванням.

— Конфіденційність повідомлень через шифрування для зв'язку, який має ресурси, щоб впоратися з додатковим навантаженням.

— Цілісність: виявляння втручань.

— Унеможливлення відтворювання та імітування зв'язку.

— Як захищеним, так і незахищеним пристроям має бути надано можливість функціювати в одній мережі, навіть якщо це може відкрити додаткові джерела вразливості.

— Відстежування інфраструктури зв'язку, яке може забезпечити:

— ступінь виявляння вторгнень;

— відстежування ресурсів навантаження;

— доступність елементів у межах інформаційної системи.

— Потреба одного набору правил для керування ідентифікуванням (наприклад, однаковий механізм для всіх профілів).

— Бажання користуватися загальноприйнятими IT-методологіями.

6.4 Взаємозв'язок між стандартами серії IEC 62351 і протоколами IEC

У кожній частині стандартів серії IEC 62351 сформульовано відповідні вимоги щодо безпеки (наприклад ідентифікування, конфіденційність тощо). Крім того, міститься висновок про відповідність реалізації протоколу (Protocol Implementation Conformance Statement — PICS), який визначає обов'язкові та необов'язкові підтвердження на різних рівнях безпеки.

Цю серію стандартів видає IEC з познакою IEC 62351, частини 1—7, а саме:

1 IEC 62351-1: Загальні положення

2 IEC 62351-2: Терміни та визначення понять

3 IEC 62351-3: Профілі, що охоплюють TCP/IP (ця частина охоплює ті профілі, які використано в ПЗЦСК, IEC 608705-104, DNP 3.0 через TCP/IP, та IEC 61850 згідно з протоколом TCP/IP)

4 IEC 62351-4: Профілі, що охоплюють MMS (ця частина охоплює ті профілі, які використано ПЗЦСК і IEC 61850)

5 IEC 62351-5: Безпека згідно з IEC 60870-5 і його похідних (тобто DNP 3.0) (ця частина охоплює як послідовні, так і мережеві профілі, які використано в IEC 60870-5 і DNP)

6 IEC 62351-6: Безпека профілів IEC 61850 (ця частина охоплює ті профілі в стандарті IEC 61850, які не ґрунтуються на TCP/IP — GOOSE, GSSE і SMV)

7 IEC 62351-7: Вимоги інформаційної основи керування (MIB) до щільного керування мережею (ця частина стосується розвитку інформаційної основи керування для устаткування керування енергосистемою).

Взаємозв'язок між стандартами серії IEC 62351 та стандартами IEC TC 57 наведено на рисунку 9.

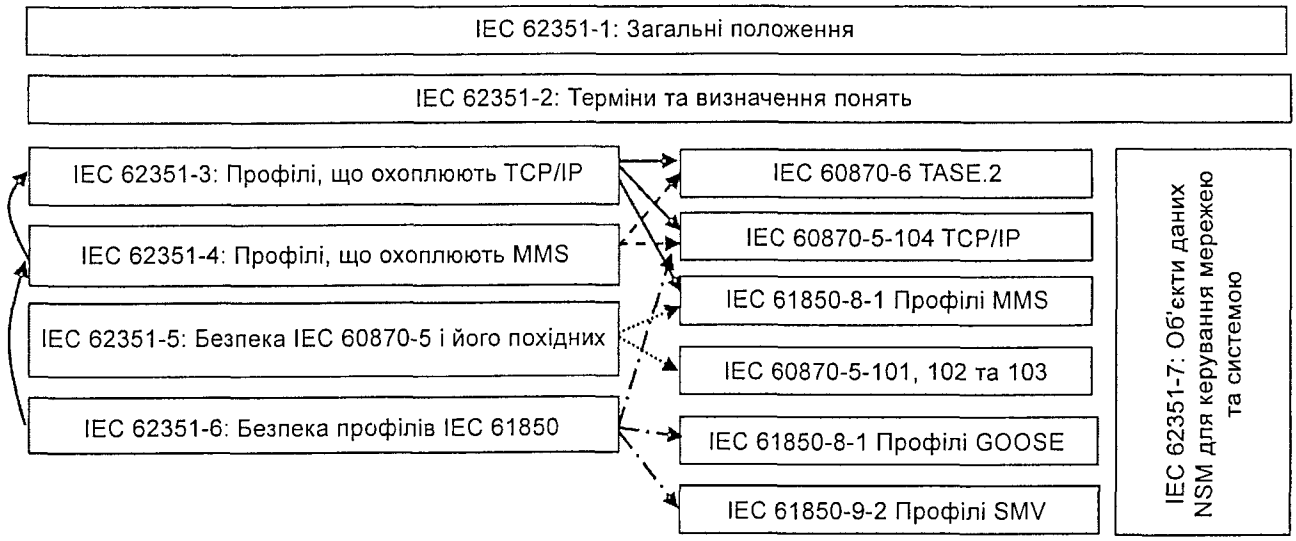

Рисунок 9 — Взаємозв'язок між профілями згідно зі стандартами серії IEC 62351 та стандартних профілів IEC TC 57

6.5 IEC 62351-1: Загальні положення

IEC 62351-1 (цей стандарт) є інформаційним вступом, який охоплює засади безпеки керування енергосистемою, а також забезпечує інформаційний огляд стандартів серії IEC 62351.

6.6 IEC 62351-2: Терміни та визначення понять

IEC 62351-2 містить визначення термінів і скорочень, які використано в стандартах серії IEC 62351. Ці визначення базуються на наявних визначеннях у галузевих стандартах, що поширюються на безпеку та зв'язок, максимально можливо, враховуючи, що терміни безпеки широко використовують в інших галузях, а також в енергосистемах. Коли використовують визначення галузевих стандартів, то подають посилання на джерело.

6.7 IEC 62351-3: Профілі, що охоплюють TCP/IP

6.7.1 *Протистояння загрозам і типам атак*

IEC 62351-3 забезпечує безпеку для будь-якого профілю, який містить TCP/IP. Замість того, щоб заново винаходити колесо, він визначає використання протоколу TLS, який зазвичай використовується в Інтернеті для безпечної взаємодії, разом з ідентифікуванням, конфіденційністю та цілісністю. В стандарті IEC 62351-3 описано обов'язкові та необов'язкові параметри й настроювання для TLS, які треба використовувати для керування об'єктами.

Призначеність IEC 62351-3 — це надання наскрізної транспортної безпеки зв'язку між програмними застосуваннями. Під час визначання найкращого підходу для досягнення цієї цілі було проаналізовано як безпеку IP, так і TLS. Безпеку IP зазвичай використовують, щоб захистити весь інформаційний потік, яким обмінюються два сегменти мережі, в той час як TLS забезпечує шифрування і захист від «незаконного посередника» на наскрізній основі. Для досягнення цієї цілі було вибрано TLS, а не безпека IP. Зрозуміло й прийнятно, що безпеку IP може бути використано для захисту іншого інформаційного потоку або навіть у поєднанні з TLS.

В IEC 62351-3 подано захист від:

— прослуховування через шифрування транспортного рівня безпеки (TLS);

— ризику для безпеки з боку «незаконного посередника» через проміжне ідентифікування повідомлень;

— обмани через сертифікати безпеки (ідентифікування вузла);

— повторів, знову ж за допомогою шифрування TLS.

Однак TLS не захищає від відмови в обслуговуванні. Цей тип атак на безпеку потрібно попереджувати через реалізування спеціальних заходів.

Безпека TLS для TCP/IP забезпечує безпеку транспортного рівня профілів зв'язку. TLS не забезпечує безпеки прикладного рівня, тому для цього має бути зреалізовано інші заходи безпеки.

6.7.2 *Вимоги щодо безпеки та заходи*

Для підтримання різних рівнів безпеки в IEC 62351-3 визначено, що продукти, які претендують на відповідність, мають підтримувати такі можливості:

— Взаємодія з іншими пристроями, які не забезпечено ні TLS, ні програмним ідентифікуванням. Це забезпечує потрібну зворотну сумісність із наявними реалізаціями, а також для поступового оновляння систем, що безпосередньо застосовують безпеку.

— Взаємодія з іншими пристроями, в яких не зазначено TLS, але підтримується програмне ідентифікування. Це може бути використано для реалізування через з'єднання VPN або всередині центрів керування.

— Взаємодія з іншими пристроями, які мають TLS, але не застосовують ідентифікування. Це дає можливість шифрування та ідентифікування тільки на рівні вузла.

— Взаємодія з іншими пристроями, в яких реалізуються як TLS, так і ідентифікування. Це забезпечує повну безпеку.

Деякі з ключових елементів заходів безпеки для TCP/IP:

— нівелювання SSL 1.0 та 2.0 через відомі види вразливості;

— використання TLS 1.0 або вище (що еквівалентно SSL 3.1);

— нівелювання наборів шифрів, які не забезпечують потрібного шифрування;

— прозоре перевіряння ключа, базоване на часі надходження і кількості пакетів, дає змогу злегка перевантаженій мережі не втрачати сертифікації протягом тривалого часу, тому що більшість з'єднань є довгостроковими. Як час, так і кількість пакетів настроюється, але рекомендованими параметрами є час (10 хв) і кількість пакетів (5000);

— під'єднана реалізація відповідальна за узгодження ключа. Це дає змогу уникнути взаємоблокування протоколу;

— стандартизування для підтримування, принаймні, одного спільного набору шифрів AES;

— специфікація ідентифікації повідомлень TLS, щоб уникнути обману та відтворення;

— можливість запросити невеликі за обсягом сертифікати, щоб мінімізувати навантаження.

6.7.3 *Використання тунелів VPN і технології апаратного реалізування безпеки*

Використання рішень VPN-тунелів та/або апаратного реалізування безпеки (наприклад, AGA 12-2) не є предметом розгляду серії стандартів IEC 62351. Це не стосується їх використовування як частини комплексного рішення безпеки доти, доки буде визнано, що вони можуть захистити лише одну з категорій безпеки.

6.8 IEC 62351-4: Безпека профілів, що охоплюють MMS

6.8.1 *Загрози та типи атак, які враховують*

IEC 62351-4 забезпечує безпеку профілів, що охоплюють MMS, зокрема означені в TASE.2 (ПЗЦСК) та стандартах IEC 61850.

Безпека специфікації виробничих повідомлень (MMS) (стандарт ISO 9506) забезпечує безпеку прикладного рівня. Вона потребує TLS для настроювання і використовує заходи безпеки TLS, зокрема ідентифікування: два об'єкти взаємодіють один з одним і вони насправді саме ті об'єкти, якими вони назвалися.

Якщо шифрування не використовують, то конкретні загрози, враховані в IEC 62351-6, містять:

— несанкціонований доступ до інформації.

Якщо використовують IEC 62351-3, то конкретні загрози, враховані в IEC 62351-4, містять:

— несанкціонований доступ до інформації через рівень ідентифікації повідомлень і шифрування повідомлень;

— несанкціоновану зміну (підроблення) або крадіжку інформації через рівень ідентифікації повідомлень і шифрування повідомлень.

Наведені нижче методи атаки на безпеку враховано в IEC 62351-4. Наступний перелік не містить методів атак, що нейтралізуються засобами, означеними в IEC 62351-3. У разі, якщо IEC 62351-3 не використовують, враховані загрози обмежуються захистом під час створення зв'язку:

— «незаконний посередник»: цю загрозу буде нейтралізовано за допомогою використання механізму коду перевіряння справжності повідомлення, зазначеного в цьому стандарті;

— виявляння втручання/цілісності повідомлення: ці загрози буде нейтралізовано за допомогою алгоритму, використовуваного для створення механізму перевіряння справжності, як зазначено в цьому стандарті;

— повторення: цю загрозу буде нейтралізовано за допомогою використання приладів спеціалізованого обробляння стану, зазначених в IEC 62351-3 та IEC 62351-4.

6.8.2 ***Вимоги та заходи безпеки***

Таким чином, сумісне використовування IEC 62351-3 та IEC 62351-4 забезпечує наскрізну безпеку прикладного рівня зв'язку разом із такими видами безпеки:

— ідентифікація;

— конфіденційність;

— цілісність даних;

— безвідмовність.

IEC 62351-4 дає змогу використовувати як захищені, так і незахищені профілі одночасно, тому не всі системи потребують оновлення одночасно всіх заходів безпеки.

6.9 IEC 62351-5: Безпека згідно з IEC 60870-5 та його структурні елементи

6.9.1 ***Загрози та типи атак***

IEC 62351-5 забезпечує різні рішення для послідовного типу (в першу чергу IEC 60870-5-101, а також IEC 60870-5-102 та IEC 60870-5-103) і для мережевого типу (IEC 60870-5-104 та його структурні елементи щодо DNP3 за TCP).

Зокрема, IEC 62351-5 забезпечує ідентифікування рівня застосування, який захищає від імітування, відтворювання, зміни і деяких заперечень під час обслуговування. В стандарті не позначено шифрування, тому він не подає захист від перехоплення, аналізування трафіку або відмови.

Ідентифікування на рівні застосування потрібно тому, що двобічна безпека і, в деяких випадках, безпека транспортного рівня, не стосується:

— безпеки в кожному локальному вузлі;

— безпеки послідовних протоколів (наприклад, IEC 60870-5) із незашифрованими радіосигналами;

— безпеки послідовних протоколів, які передаються по мережі IP через термінал серверів;

— захисту від «шкідливих застосувань» або атак із хостів, які можуть бути заражені шкідливими програмами;

— КДОП для віддаленого вузла. На сьогодні ланки безпеки для ідентифікування на основі ролей користувачів зазвичай керуються хостом. Ідентифікування на рівні застосування дає впевненість, що лише ті користувачі, які уповноважені бачити певний набір даних, мають до них доступ, і немає передавання з віддаленого вузла доти, доки користувач не пройшов перевіряння на автентичність.

6.9.2 ***Вимоги та заходи безпеки***

Структурні елементи IEC 60870-5-104, які стосуються протоколу TCP/IP, можуть означувати заходи безпеки, описані в IEC 62351-3, який містить конфіденційність і цілісність, забезпечені шифруванням TLS. Таким чином, єдиною додатковою вимогою є ідентифікування послуг, що підтримуються IEC 62351-5.

Послідовний тип зазвичай використовують у комунікаційних засобах інформації, які можуть підтримувати лише малі швидкості передавання даних, або з промисловим устаткованням, обчислювальна здатність якого обмежена. TLS потребує занадто інтенсивних обчислень та/або інтенсивного зв'язку, щоб використовуватись у таких середовищах. Тому лише заходи безпеки, передбачені для послідовного типу, містять прості механізми ідентифікування.

6.9.3 *Можливі додаткові заходи безпеки згідно з IEC 62351-5*

Якщо потрібно шифрування, то може бути долучено інші криптографічні заходи безпеки, такі як VPN, або технології апаратного реалізування безпеки залежно від можливостей зв'язку та устаткування. Ці заходи виконують шифрування на транспортному рівні.

6.10 IEC 62351-6: Безпека профілів згідно з IEC 61850

6.10.1 *Загрози та типи атак*

IEC 62351-6 забезпечує профіль IEC 61850 за допомогою MMS над TCP/IP, використовуючи IEC 62351-3 та IEC 62351-4. Загрози безпеці, яким протистоять, містять «користувач-посередник», несанкціоновану модифікацію даних, несанкціоновану модифікацію повідомлень, виявляння вторгнень і відтворення. Для тих функцій, для яких вимоги продуктивності є не настільки жорсткими, і де потрібна конфіденційність, шифрування може бути забезпечено іншими заходами безпеки, такими як апаратне реалізування безпеки або VPN.

6.10.2 *Вимоги та заходи безпеки*

Профіль, означений в IEC 61850, з використанням MMS через TCP/IP відповідає вимогам стандартів IEC 62351-3 та IEC 62351-4. Додаткові профілі, означені в IEC 61850, які працюють через TCP/IP (послуги мережі або інші майбутні профілі), мають відповідати IEC 623513 та додатковим заходам безпеки, розробленим промисловістю зв'язку для безпеки рівня застосувань. Можна використовувати ці галузеві заходи безпеки додатково до стандартів серії IEC 62351.

Стандарт IEC 61850 також містить три протоколи (GOOSE, GSE та SMV), які є направленими датаграмами і не маршрутизуються, вони призначені для роботи в локальній мережі підстанції або в іншій немаршрутизованій мережі. У цьому середовищі повідомлення повинні передаватися протягом 4 мс, тому не допустимо використання більшості методів шифрування або інших заходів безпеки, які впливають на швидкість передавання даних. Перевіряння достовірності за допомогою цифрового підпису є єдиною мірою безпеки.

Характеристики цих трьох протоколів наведено в таблиці 1.

Таблиця 1 — Характеристики трьох направлених протоколів згідно з IEC 61850

	SMV	GOOSE	MMS
Розмір PDU	Приблизно 1500	Приблизно 1500	Від 30 000
Представлення	Потоком	4 мс	Без вимог
Тип	Групове передавання	Групове передавання	Зорієнтовано на зв'язок

Виходячи з цих характеристик, були визначені заходи безпеки, наведені в таблиці 2.

Таблиця 2 — Заходи безпеки для трьох направлених протоколів згідно з IEC 61850

	SMV	GOOSE	MMS
Сертифікат X.509 (ідентичний)	Ні	Ні	Так
Шифрування (конфеденційність)	Немає потреби	Лише тоді, коли перевищує 4 мс	Так
Визначання підроблення (визначання вторгнення)	Так	Так	Так

Деякі ключові елементи заходів безпеки для GOOSE та SMV, а саме:

— ідентифікування — це головний захід безпеки;

— шифрування не підтримується, тому що це долучає занадто багато байтів до повідомлення, а також вважається, що це неважливо. (У майбутньому може бути долучено деякі методи апаратного шифрування);

— перевіряння ключа «всередині діапазону» не підтримується, оскільки це може порушити висококритичний, високошвидкісний потік інформації;

— оскільки безпека може реалізовуватися протягом довгого часу, та через те, що вона може бути чи не бути потрібною для різних пристроїв, незахищений GOOSE-клієнт може ігнорувати повідомлення безпеки GOOSE;

— для зворотної сумісності зарезервоване поле зараз використовне для довжини, тому розширення може бути долучено до кінця повідомлення GOOSE/SMV. Це розширення містить значення ідентифікації (цифровий підпис — HMAC). Незахищені клієнти будуть просто ігнорувати це розширення. Воно долучає приблизно 20 байт;

— мова конфігурування, означена в стандарті IEC 61850 підстанції (SCL), розширена для підтримування обміну сертифікатами.

На діаграмі (рисунок 10) наведено заходи безпеки ідентифікування в GOOSE/SMV.

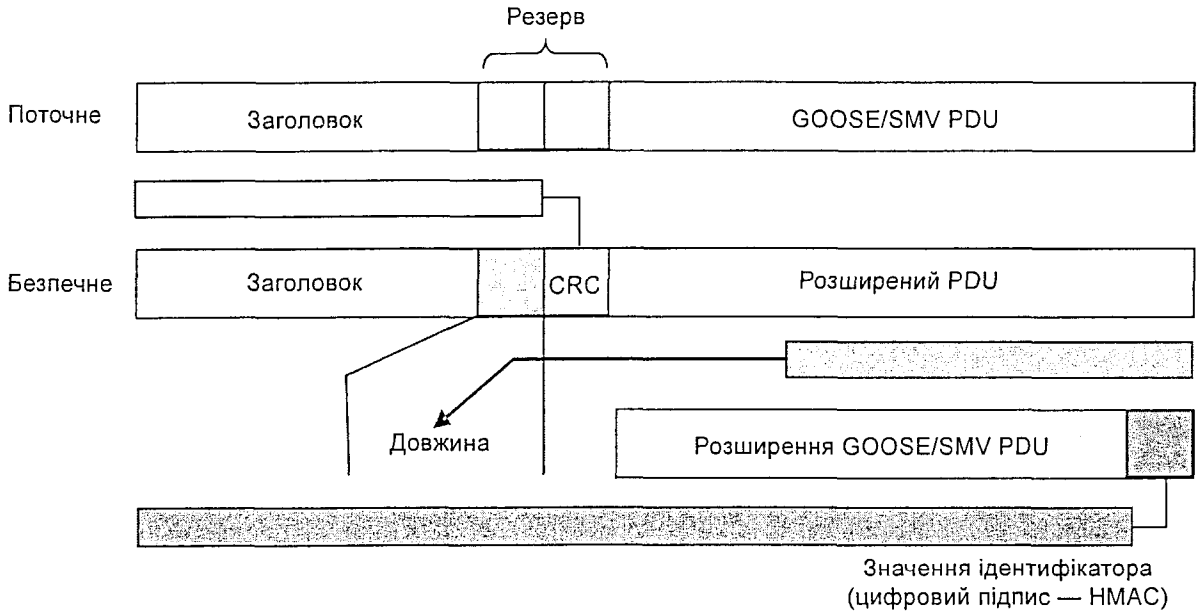

Рисунок 10 — Ідентифікаційні заходи безпеки в GOOSE/SMV

6.11 IEC 62351-7: Безпека керування системами і мережами

6.11.1 *Ціль та сфера застосування IEC 62351-7*

IEC 62351-7 стосується безпеки керування мережами і системами інформаційної інфраструктури.

Керування енергосистемами все частіше покладається на інформаційні інфраструктури разом із мережами зв'язку, ІЕП та протоколами зв'язку із самовизначенням. Тому керування інформаційною інфраструктурою має вирішальне значення для забезпечення потрібного високого рівня безпеки та надійності в діяльності енергосистеми. Ось чому IEC 62351-7 поширюється на об'єкти даних керування мережами та системами (NSM) для середовища керування енергосистемами. Ці об'єкти NSM-даних відображають, яка інформація потрібна для керування інформаційною інфраструктурою для надійного керування інфраструктурою енергосистеми (див. рисунок 11).

Стандарти керування мережами ISO CMIP та IETF SNMP можуть частково забезпечити таке керування. У SNMP бази MIB використовуються для відстежування стану мереж і систем, але кожен виробник повинен розробити свій власний набір баз MIB для свого устаткування. Під час керування енергосистеми SNMP бази MIB доступні лише для звичайних мережевих пристроїв, таких як маршрутизатори. Немає стандартних MIB, які було розроблено для ІЕП, тому виробники використовують спеціальні або власні методи відстежування певних видів неполадок. Зазначений стандарт забезпечує, таким чином, об'єкти даних MIB (визначені об'єкти даних NSM) для енергетичної галузі.

Об'єкти даних NSM подають набір інформації, який вважають обов'язковим, рекомендованим або додатковим для підтримування мережі й системи керування та виявляння проблем безпеки. Ці об'єкти даних NSM використовують правила йменування, розроблені в IEC 61850 і доповнені для вирішення питань з NSM.

Абстрактні моделі SNMP клієнт/посередник допустимі в межах стандарту, але SNMP не допустимий як протокол вибору. На противагу, абстрактні об'єкти NSM-даних, які визначено в IEC 62351-7, можуть бути відображені у будь-який відповідний протокол, зокрема згідно з IEC 61850, IEC 60870-5, IEC 60870-6, SNMP, послуг мережі, або будь-який інший відповідний протокол.

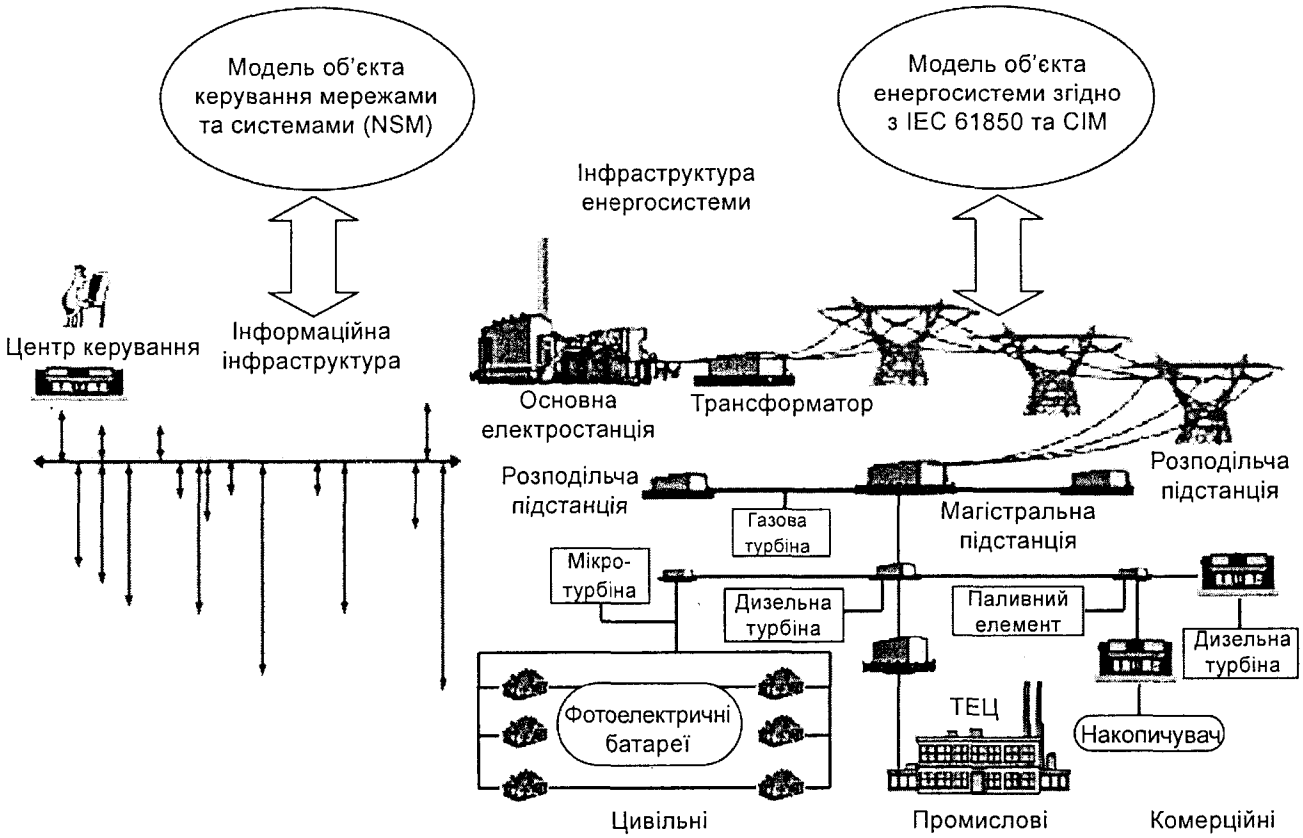

Рисунок 11 — Моделі об'єкта NSM — еквіваленти інформаційної інфраструктури для моделей об'єкта інфраструктури енергосистеми згідно з CIM та IEC 61850

6.11.2 *Вимоги до NSM*

Потрібно визначити вимоги щодо безпеки та надійності об'єкта даних NSM, які є специфічними для енергетики. Ці об'єкти даних NSM будуть підтримувати цілісність мережі зв'язку, справність системи та застосувань, системи виявляння вторгнень (IDS), фаєрволи та інші важливі для керування енергосистемами вимоги щодо безпеки/мережі. Основні елементи системи керування енергосистемою з долученням архітектури відстеження безпеки наведено на рисунку 12.

6.11.3 *Приклади об'єктів даних NSM*

Приклади вимог до керування мережею та системою, які виконують об'єкти даних NSM, охоплюють:

а) Керування мережею зв'язку: відстежування мереж і протоколів
   1) Визначання постійних збоїв мережевого устаткування
   2) Визначання тимчасових збоїв та/або перезапускання мережевого устаткування
   3) Визначання тривкості до відмов мережевого устаткування для резервування устаткування або каналів зв'язку
   4) Визначання статусу резервування або запасного устаткування
   5) Визначання версії та стану протоколу зв'язку
   6) Визначання несумісності різних версій протоколів
   7) Визначання підробляння/відтворення повідомлень протоколу
   8) Визначання недостатньої синхронізації таймерів у мережах
   9) Визначання вичерпності ресурсу захисту від атак відмови під час обслуговування (DOS-атаки)
   10) Визначання переповнення буфера DOS-атак

11) Визначання руйнування фізичного доступу
12) Визначання недійсного доступу до мережі
13) Визначання недійсного доступу/керування об'єктом застосування
14) Здатність визначити скоординовані атаки в різних системах
15) Збирання статистичної інформації від мережевого устаткування:
    — визначання середнього часу доставляння повідомлень — уповільнений, пришвидшений тощо;
    — підрахунок кількості повідомлень, розмір повідомлень
16) Забезпечування аудиту журналів безпеки та записів

b) Керування зв'язками мережі: керування мережами
1) Ручне подавання команд вмикання/вимикання устаткованню мережі
2) Ручне подавання команд щодо перемикання для мережевого устаткування
3) Настроювання параметрів і послідовності автоматичних дій у мережі
4) Автоматичні дії у відповідь на такі події, як переконфігурування мережі зв'язку за відмови устаткування

c) Керування системою: ІЕП відстеження
1) Кількість і час усіх зупинень і запускань системи, контролерів та застосувань
2) Стан кожного застосовання та/або програмного модуля: зупинено, припинено, працює, не відповідає, неправильний або суперечливо введено, помилки виведення, стан помилки тощо
3) Стан усіх мережевих під'єднань до ІЕП, разом із кількістю та періодами тимчасових і постійних збоїв
4) Стан будь-яких тактів «підтримання життя», зокрема пропущених тактів
5) Характеристика стану резервних або відмовотривких пристроїв, такі як кількість і час, коли ці пристрої були недоступні
6) Стан даних звітування: нормальний, не може підтримати запит, немає даних тощо
7) Стан доступу: кількість, час і типи спроб несанкціонованого доступу до даних або можливості керування
8) Аномалії доступу до даних (наприклад, поодинокий запит, тоді як зазвичай повідомляється періодично)

d) Система керування: керувальні дії для ІЕП
1) Запускання і припинення звітності
2) Перезапускання ІЕП
3) Припинення процесу та/або перезапускання програмного забезпечення
4) Відновляння зв'язку з іншими ІЕП
5) Від'єднання іншого ІЕП
6) Забезпечування журналу інформаційних подій
7) Зміна пароля
8) Зміна резервних чи аварійних настроювань
9) Забезпечування контрольного журналу та записів

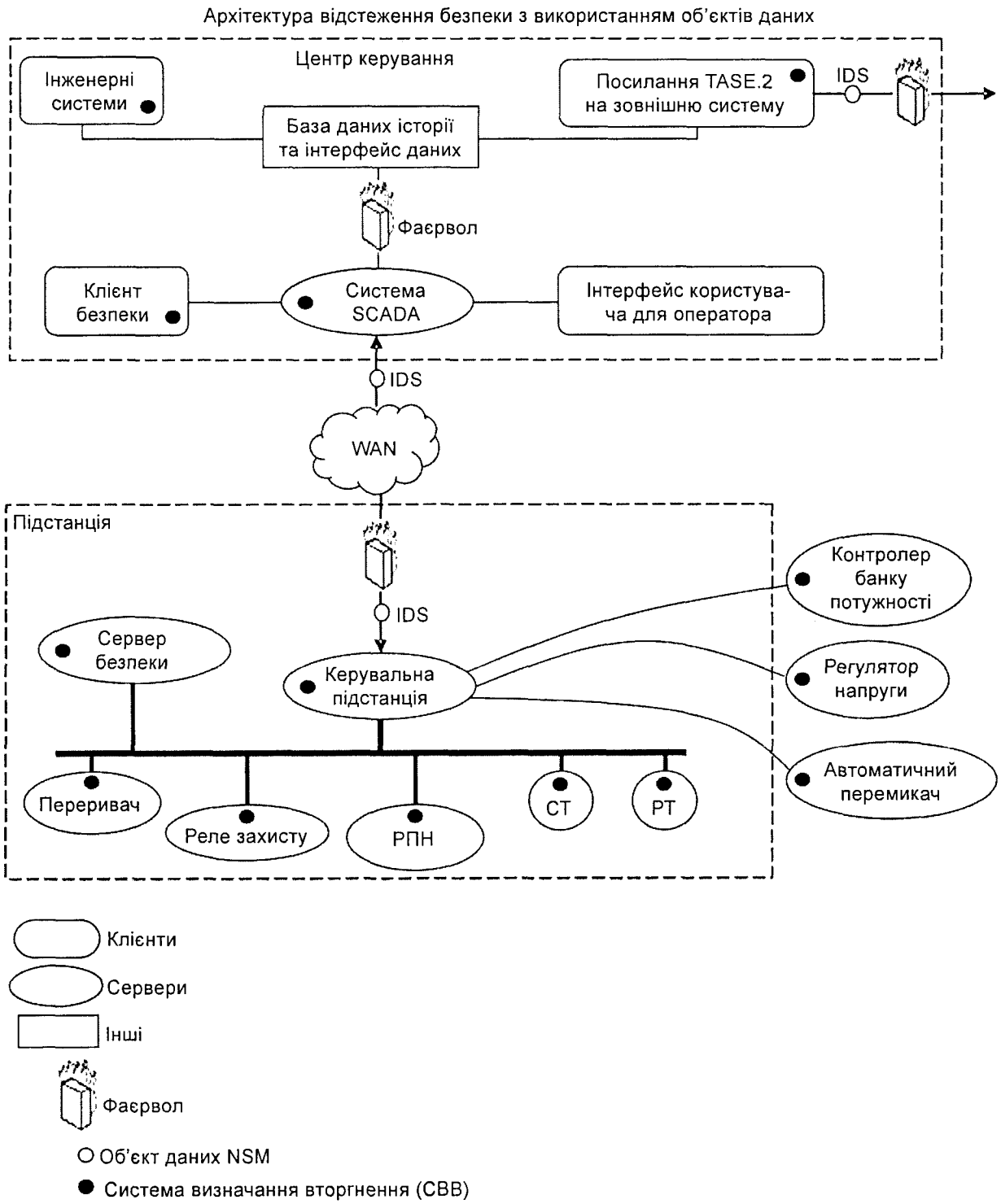

Рисунок 12 — Системи керування енергосистемою, що відображає архітектуру відстеження безпеки

7 ВИСНОВКИ

Заходи безпеки мають бути передбачені в будь-якій системі під час її проектування. Безпека містить не лише фаєрволи або «шифрування», які більшість людей вважає єдиними потрібними заходами безпеки, але також ідентифікування, керування доступом на основі ролей, унеможливлювання DOS-атакам, функції відстеження та контролювання для інформаційних інфраструктур, і нарешті, не менш важливі — правила безпеки, які забезпечують виконання та підтримання заходів безпеки.

БІБЛІОГРАФІЯ

North American Electric Reliability Council (NERC) Cyber Security Standard, CIP 002-009, 2006.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

Північноамериканська національна рада електричної надійності (NERC). Стандарт інформаційної безпеки, CIP 002-009, 2006.

ДОДАТОК НА
(довідковий)

ПОЗНАКИ ТА СКОРОЧЕННЯ

ПКД (ACL — Access Control Lists) — перелік керування доступом

AEC (Asymmetric Encryption) — несиметричне шифрування

AES (Symmetric Encryption) — симетричне шифрування

CMIP (Common Management Information Protocol) — протокол загальної керувальної інформації

CRC (Cyclic Redundancy Code) — контролювання циклічним надлишковим кодом

DNP (Distributed Network Protocol) — протокол розподіленої мережі

EMS (Energy Management System) — система керування споживанням

EMS-API (Energy Management System Application Program Interface) — інтерфейс прикладних програм керування енергосистемами

ПЗЦСК (ICCP) — Inter-Control Center Communications Protocol) — протокол зв'язку центру сумісного керування

СГІ (GIS — Geophysical Information System) — система геофізичної інформації

GOOSE (GNU Object-Oriented Statistics Environment) — об'єктно-зорієнтоване статистичне середовище проекту GNU

GSSE (Generic Substation Status Event) — статус подій генерувальної підстанції

HMAC (Hash-based Message Authentication Code) — ідентифікаційний код повідомлення на основі хешування — цифровий підпис

ІЕП (IDE — Intelligent Electronic Devices) — інтелектуальний електронний пристрій

IDS (Intrusion Detection Systems) — системи виявляння вторгнень

IEC (International Electrotechnical Commission) — міжнародна електротехнічна комісія

IETF (Internet Engineering Task Force) — група інженерного розробляння мережі

ISO (International Standardization Organization) — міжнародна організація стандартизації

IT (Information Technology) — інформаційна технологія

MIB (Management Information Base) — база інформації про керування

MMS (Manufacturing Message Specification) — специфікація виробничих повідомлень

NSM (Network And System Management) — керування мережами та системами

PICS (Protocol Implementation Conformance Statement) — висновок про відповідність реалізації протоколу

ІВК (PKI — Public Key Infrastructure) — інфраструктура відкритого ключа

КДОП (RBAC — Authentication for Role-Based Access Control) — ідентифікація для керування доступом на основі ролей

RTU (Remote Terminal Unit) — місце віддаленого керування

SCADA (Supervisory Control And Data Acquisition) — система диспетчерського контролювання та збирання даних

SCL (Substation Configuration Language) — мова конфігурації підстанції

SMV (Symbolic Model Verifier) — визначання символічної моделі

SNMP (Simple Network Management Protocol) — простий протокол керування мережами

SSL (Secure Sockets Layer) — рівень захищених сокетів

TLS (Transport Level Security) — безпека транспортного рівня

TCP/IP (Transmission Control Protocol/Internet Protocol) — протокол керування передаванням/міжмережевий протокол

КЦО (TOE — Target of Evaluation) — концепція цільової оцінки

VPN (Virtual Private Network) — віртуальна приватна мережа

WG (Work Group) — робоча група.

Код УКНД 33.200

Ключові слова: безпечність мережі, загальний огляд, керування енергосистемами, типи загроз безпеці.

Редактор **В. Кириленко**
Технічний редактор **О. Марченко**
Коректор **О. Опанасенко**
Верстальник **Т. Неділько**

Підписано до друку 22.06.2015. Формат 60 × 84 1/8.
Ум. друк. арк. 3,72. Зам. 1097 Ціна договірна.

Виконавець
Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)
вул. Святошинська, 2, м. Київ, 03115

Свідоцтво про внесення видавця видавничої продукції до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції від 14.01.2006 серія ДК № 1647