ТЕМА 6. МІЖНАРОДНІ СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА /АБО КІБЕРБЕЗПЕКИ

6.1. Регламенти ЄС в галузі кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»

6.2. ДСТУ ISO 27001, ISO 27002, ISO 27003

6.3. ISO/IEC 15408- 2, ISO/IEC 15408-3

6.4. Стек протоколів ДСТУ ISO/IEC 27000

Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. За даними глобального огляду, проведеного об'єднанням ISACA тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта 83% відносять кібернапади до одною з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки.

Система кібербезпеки – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберсереди, ресурсів організацій і користувачів.

Основними завданнями кібербезпеки вважаються забезпечення: конфіденційності доступності, а також цілісності, що включає автентичність. Кібербезпека є необхідною умовою розвитку інформаційного суспільства.

6.1 Регламенти ЄС в галузі кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»

ENISA – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. Агентство Європейського Союзу з кібербезпеки, ENISA, є агентством Союзу, яке займається досягненням високого загального рівня кібербезпеки в Європі. Агентство Європейського Союзу з кібербезпеки, засноване в 2004 році та посилене Актом про кібербезпеку ЄС, сприяє кіберполітиці ЄС, підвищує надійність продуктів, послуг і процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС і допомагає Європі підготуватися для кібервикликів завтрашнього дня. Завдяки обміну знаннями, розбудові потенціалу та підвищенню обізнаності Агентство співпрацює зі своїми ключовими зацікавленими сторонами, щоб зміцнити довіру

до підключеної економіки, підвищити стійкість інфраструктури Союзу та, зрештою, зберегти європейське суспільство та громадян у цифровій безпеці.

РОЗДІЛ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Предмет та сфера застосування

1. З метою забезпечення належного функціонування внутрішнього ринку з одночасним прагненням досягнути високого рівня кібербезпеки, кіберстійкості та довіри в межах Союзу, цей Регламент встановлює:

(a) цілі, завдання та організаційні питання, що стосуються ENISA (Агентства Європейського Союзу з питань мережевої та інформаційної безпеки); та

рамки для створення європейських схем сертифікації кібербезпеки з метою забезпечення належного рівня кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ в Союзі, а також з метою уникнення фрагментації внутрішнього ринку стосовно схем сертифікації кібербезпеки в Союзі.

Рамки, зазначені в пункті (b) першого підпараграфа, застосовують без обмежень до спеціальних положень в інших правових актах Союзу, що стосуються добровільної або обов’язкової сертифікації.

Цей Регламент не обмежує компетенцій держав-членів щодо діяльності, пов’язаної з громадською безпекою, обороною, національної безпекою, та діяльності держави у сферах кримінального права.

Стаття 2. Терміни та означення

Для цілей цього Регламенту застосовують такі терміни та означення:

«**кібербезпека**» означає діяльність, необхідну для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які зазнають впливу кіберзагроз;

«**мережева та інформаційна система**» означає:

мережу електронного зв’язку у розумінні пункту (a) статті 2 Директиви 2002/21/ЄС;

будь-який пристрій або групу взаємоз’єднаних чи пов’язаних пристроїв, один або декілька з яких, відповідно до програми, здійснює автоматичне опрацювання цифрових даних; або

цифрові дані, які зберігають, опрацьовують, видобувають або передають за допомогою елементів, згаданих в пунктах (a) та (b), для цілей їхньої експлуатації, використання, захисту та технічного обслуговування;

«**національна стратегія безпеки мережевих та інформаційних систем**» означає рамки, що забезпечують стратегічні цілі та пріоритети безпеки мережевих та інформаційних систем на національному рівні;

«**оператор основних послуг**» означає оператора основних послуг, як означено в пункті (4) статті 4 Директиви (ЄС) 2016/1148;

«**надавач цифрових послуг**» означає будь-яку юридичну особу, що надає цифрову послугу;

(1) «**інцидент**» означає будь-яку подію, що має фактичний негативний вплив на безпеку мережевих та інформаційних систем;

(2) «**врегулювання інцидентів»** означає всі процедури на підтримку виявлення, аналізу інциденту, обмеження його наслідків і реагування на нього;

(3) «**кіберзагроза**» означає будь-яку потенційну обставину, подію або дію, яка може пошкодити, порушити або інакше негативно вплинути на мережеві та інформаційні системи, користувачів таких систем та інших осіб;

(4) «**європейська схема сертифікації кібербезпеки**» означає комплексний набір правил, технічні вимоги, стандарти та процедури, які встановлені на рівні Союзу та які застосовують до сертифікації або оцінювання відповідності конкретних продуктів ІКТ, послуг ІКТ або процесів ІКТ;

(5) «**національна схема сертифікації кібербезпеки**» означає комплексний набір правил, технічні вимоги, стандарти та процедури, які розроблені та ухвалені національним органом публічної влади та які застосовують до сертифікації або оцінювання відповідності продуктів ІКТ, послуг ІКТ або процесів ІКТ в рамках конкретної схеми;

(6) «**європейський сертифікат з кібербезпеки**» означає документ, виданий відповідним органом, який підтверджує, що було проведено оцінювання певного продукту ІКТ, послуги ІКТ або процесу ІКТ на відповідність конкретним вимогам, встановленим у європейській схемі сертифікації кібербезпеки;

(7) «**продукт ІКТ**» означає елемент або групу елементів мережі або інформаційної системи;

(8) «**послуга ІКТ**» означає послугу, що головним або переважним чином полягає в передачі, зберіганні, отриманні або опрацюванні інформації за допомогою мережевих та інформаційних систем;

(9) «**процес ІКТ**» означає комплекс заходів, спрямованих на проєктування, розробку, надання або технічне обслуговування продукту ІКТ або послуги ІКТ;

(10) «**акредитація**» означає засвідчення національним органом з акредитації дотримання органом з оцінювання відповідності вимог, установлених у гармонізованих стандартах, та, у відповідних випадках, у будь- яких інших додаткових вимогах, у тому числі тих, що викладено у відповідних секторальних схемах, для провадження конкретної діяльності з оцінювання відповідності;

(11) «**національний орган з акредитації**» означає єдиний орган у держави-члени, який проводить акредитацію на підставі повноважень, наданих державою;

(12) «**оцінювання відповідності**» означає процес підтвердження того, що встановлені вимоги до продукту, процесу, послуги, системи, особи або органу було виконано;

(13) «**орган з оцінювання відповідності**» означає орган, який провадить

діяльність з оцінювання відповідності, у тому числі такі її види як калібрування, випробування, сертифікацію та інспектування;

(14) «**стандарт**» означає стандарт, як означено в пункті (1) статті 2 Регламенту (ЄС) № 1025/2012;

(15) «**технічні специфікації**» означають документ, що встановлює технічні вимоги, яким повинні відповідати продукт ІКТ, послуга ІКТ або процес

ІКТ, або процедури оцінювання відповідності стосовно продукту ІКТ, послуги ІКТ або процесу ІКТ;

(16) «**рівень надійності**» означає основу впевненості в тому, що продукт ІКТ, послуга ІКТ або процес ІКТ відповідає вимогам безпеки конкретної європейської схеми сертифікації кібербезпеки, вказує, на якому рівні відбулося оцінювання продукту ІКТ, послуги ІКТ або процесу ІКТ, але як такий не визначає рівень безпеки відповідного продукту ІКТ, послуги ІКТ або процесу ІКТ;

(17) «**самооцінювання відповідності**» означає дію, виконувану виробником або надавачем продуктів ІКТ, послуг ІКТ або процесів ІКТ, яка надає оцінку стосовно того, чи такі продукти ІКТ, послуги ІКТ або процеси ІКТ відповідають вимогам конкретної європейської схеми сертифікації кібербезпеки.

У наступних розділах та статтях визначено наступне:

РОЗДІЛ II. (АГЕНТСТВО ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ)

ГЛАВА I. Мандат та цілі Стаття 3. Мандат.

Стаття 4. Цілі

1. ENISA є центром експертних знань з кібербезпеки завдяки своїй незалежності, науковій та технічній якості наданих консультацій, допомоги та інформації, прозорості своїх оперативних процедур, методів роботи та сумлінного виконання своїх завдань.

2. ENISA надає допомогу установам, органам, офісам та агентствам Союзу, а також державам-членам у розробленні та імплементації політики Союзу з питань кібербезпеки, у тому числі галузевої політики з кібербезпеки.

3. ENISA підтримує розбудову потенціалу та готовність на території Союзу шляхом надання допомоги установам, органам, офісам та агентствам Союзу, а також державам-членам та публічним і приватним стейкхолдерам для посилення захисту

їхніх мережевих та інформаційних систем, розробки та посилення кіберстійкості та можливості реагування, а також для розвитку вмінь і навичок у сфері кібербезпеки.

4. ENISA сприяє співпраці, у тому числі обміну інформацією та координації на рівні Союзу, серед держав-членів, установ, органів, офісів та агентств Союзу та відповідних приватних і публічних стейкхолдерів у питаннях кібербезпеки.

5. ENISA сприяє розширенню можливостей у сфері кібербезпеки на рівні Союзу, щоб підтримати заходи держав-членів для запобігання кіберзагрозам та реагування на них, зокрема у випадку транскордонних інцидентів.

6. ENISA сприяє використанню європейської схеми сертифікації кібербезпеки з метою уникнення фрагментації внутрішнього ринку. ENISA сприяє впровадженню та технічному обслуговуванню європейських рамок сертифікації кібербезпеки відповідно до розділу III цього Регламенту з метою посилення прозорості кібербезпеки продуктів ІКТ, послуг ІКТ, процесів ІКТ, внаслідок чого відбуватиметься посилення рівня впевненості в цифровому внутрішньому ринку та його конкурентоспроможності.

7. ENISA сприяє досягненню високого рівня обізнаності в питаннях кібербезпеки, у тому числі кібергігієни та кіберграмотності, серед громадян, організацій та підприємств.

РОЗДІЛ II. Завдання

Стаття 65. Санкції

РОЗДІЛ IV. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Стаття 66. Процедура комітету

Стаття 67. Оцінювання й перегляд

Стаття 68. Скасування та правонаступництво

Стаття 69. Набуття чинності

6.2. ДСТУ ISO 27001, ISO 27002, ISO 27003

Система кібербезпеки, яка базується на міжнародних стандартах надзвичайно важлива у сучасному цифровому світі. Розробкою зазначених стандартів займаються Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). На сьогодні фахівцями цих організацій розроблена серія стандартів ISO/IEC 27000, яка постійно доповнюється новими документами. В Україні на даний час діють стандарти серії ДСТУ ISO/IEC 27000, які відповідно гармонізовані з ISO/IEC 27000. До них відносяться наступні:

ДСТУ ISO/IEC 27000:2019

ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT) – ISO/IEC 27000:2018 дає змогу переглянути системи управління інформаційною безпекою (СУІБ). Це також забезпечує терміни і визначення, як правило, використовувані в СУІБ сімейства стандартів. Цей документ є застосованим до всіх типів і розмірів організації (наприклад, комерційні організації, державні агенції, не для сприяння охоплюють загальновживані терміни та визначення в сімействі стандартів СУІБ; не підтримують всі терміни і терміни, які застосовуються в сімействі стандартів СУІБ; не встановлює значення СУІБ у стандартах у визначенні нових термінів для використання.

ДСТУ ISO/IEC 27001:2015

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту

системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) – Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Вимоги, наведені в цьому стандарті, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи. Вилучення будь-якої з вимог, наведених в розділах 4- 10 неприпустимо в разі, якщо організація прагне відповідати цьому стандарту.

Входить в групу стандартів ISO 27000 – СУІБ та тісно пов'язаний із стандартом ISO/IEC 27002.

У стандарті ISO/IEC 27001 (ISO 27001) зібрані описи найкращих світових практик в області управління інформаційною безпекою. ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений в якості моделі для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення **СистемиУправління Інформаційної Безпеки (СУІБ)**.

Система управління інформаційною безпекою СУІБ (англ. *information security management system*, ISMS) – частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес- ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для **процесів СУІБ застосована модель ПВПД** (плануй-виконуй- перевіряй-дій; англ. ***Plan-Do-Check-Act, PDCA***):

– Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;

– Do (дія) – етап реалізації та впровадження відповідних заходів;

– Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;

– Act (поліпшення) – виконання превентивних і коригуючих дій

Складові політики інформаційної безпеки:

- визначення критичних бізнес-процесів/банківських продуктів;
- надання доступу до інформації;
- контроль доступу;
- парольний захист;
- антивірусний захист;
- захист мережі банку;
- віддалений доступ до ресурсів мережі;
- ідентифікація та автентифікація ресурсів СУІБ;
- криптографічний захист інформації;
- політика «чистого екрана» та «чистого стола»

Мета СУІБ – вибір відповідних заходів управління безпекою, призначених для захисту інформаційних активів і гарантують довіру зацікавлених сторін.

Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені і інші властивості, такі як справжність, неможливість відмови від авторства, достовірність.

Конфіденційність – забезпечення доступності інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі).

Доступність – забезпечення доступу до інформації авторизованим користувачам, коли це необхідно (на вимогу).

Цілісність – забезпечення точності і повноти інформації, а також методів її обробки.

Саме поняття «**Захист інформації**» трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Основа стандарту ICO 27001 – система управління ризиками, пов'язаними з інформацією. **Система управління ризиками** дозволяє отримувати відповіді на наступні питання:

- на якому напрямку інформаційної безпеки потрібно зосередити увагу;
- скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації.

Стандарт ISO 27001 гармонізований зі стандартами систем менеджменту якості ISO 9001:2015 та ISO 14001:2015 та базується на їх основних принципах і процесному

підході. Більш того, обов'язкові процедури стандарту ISO 9001 потрібні і стандартом ISO 27001. Структура документації за вимогами ISO 27001 аналогічна структурі за вимогами ISO 9001. Велика частина документації, необхідна по ISO 27001, вже могла бути розроблена, і могла використовуватися в рамках ISO 9001. Таким чином, якщо організація вже має систему менеджменту згідно, наприклад, з ISO 9001 або ISO 14001, то переважно забезпечувати виконання вимоги стандарту ISO 27001 в рамках вже існуючих систем.

Також **основними принципами стандарту ISO 27001** є:

– конфіденційність інформації
– доступність інформації
– цілісність інформації

Організація може бути **сертифікована акредитованими агентствами відповідно до цього стандарту. Процес сертифікації** складається з трьох стадій:

– стадія 1 – вивчення аудитором ключових документів системи менеджменту інформаційної безпеки – положення про можливість застосування (SoA), план обробки ризиків (RTP), і ін. Може виконуватися як на території організації так і шляхом висилки цих документів зовнішньому аудитору;

– стадія 2 – детальний, глибокий аудит включаючи тестування впроваджених заходів та оцінка їх ефективності. Включає повне вивчення документів, які вимагає стандарт;

– стадія 3 – виконання інспекційного аудиту для підтвердження, що сертифікована організація відповідає заявленим вимогам. Виконується на періодичній основі.

Процедура сертифікації системи менеджменту за допомогою одного з міжнародних стандартів або їх комбінації підрозділяється на 4 етапи:

– 1 етап. Підготовка до сертифікації;
– 2 етап. Аудит 1-го ступеня (перевірка готовності до сертифікації);
– 3 етап. Аудит 2-го ступеня (сертифікаційний аудит);
– 4-ий етап. Видача сертифіката і нагляд.

ДСТУ ISO/IEC 27002:2015

ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) – Цей стандарт встановлює настанови стосовно організаційних стандартів щодо інформаційної безпеки та загальні практики управління інформаційною безпекою, охоплюючи вибір, впровадження та управління заходами безпеки з урахуванням розгляду середовища ризиків інформаційної безпеки організації. Цей стандарт розроблено для використання організаціями, які намагаються: визначити заходи безпеки в межах процесу впровадження **системи управління інформаційною безпекою (СУІБ)** або як її ще називають **системи менеджменту інформаційною безпекою (СМІБ)** на основі ISO/IEC 27001; впровадити загальноприйняті заходи інформаційної безпеки; розробити власні настанови щодо управління інформаційною безпекою.

До 2007 року цей стандарт називався ISO/IEC 17799. Стандарт розроблений у 2005 році на основі версії **ISO 17799**, опублікованої в 2000, яка була повною копією Британського стандарту **BS 7799-1:1999**.

Стандарт надає найкращі практичні поради щодо менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. ***Інформаційна безпека*** визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна лише тим, хто уповноважений мати такий доступ), цілісності (гарантії точності та повноти інформації, а також методів її обробки) та доступності (гарантії того, що уповноважені користувачі мають доступ до інформації та пов'язаних з нею ресурсів)».

Поточна версія стандарту складається з таких основних розділів:

- Політика безпеки (*Security policy*).
- Організація інформаційної безпеки (*Organization of information security*).
- Управління ресурсами (*Asset management*).
- Безпека персоналу (*Human resources security*).
- Фізична безпека та безпека оточення (*Physical and environmental security*).
- Управління комунікаціями та операціями (*Communications and operations*

management).

- Управління доступом (*Access control*).
- Придбання, розробка та підтримка систем (*Information systems acquisition, development and maintenance*).
- Управління інцидентами інформаційної безпеки (*Information security incident management*).
- Управління безперебійною роботою організації (*Business continuity management*).
- Відповідність нормативним вимогам (*Compliance*).

Цей документ описує 127 механізмів контролю, які необхідні для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду (best practices) у цій галузі. Цей документ є практичним посібником зі створення СУІБ.

Британський стандарт BS 7799, на якому базується ISO/IEC 27002, рекомендує включати в документ, що характеризує політику безпеки організації, наступні розділи:

- вступний, підтверджуючий заклопотаність вищого керівництва проблемами інформаційної безпеки;
- організаційний, утримуючий опис підрозділів, комісій, груп і т.д., відповідальних за роботи в області інформаційної безпеки;
- класифікаційний, що описує наявні в організації матеріальні й інформаційні ресурси й необхідний рівень їхнього захисту;
- штатний, що характеризує міри безпеки, застосовувані до персоналу (опис посад з погляду інформаційної безпеки, організація навчання й перепідготовки персоналу, порядок реагування на порушення режиму безпеки й т.п.);
- розділ, що висвітлює питання *фізичного захисту*;
- керуючий розділ, що описує підхід до управління комп'ютерами й комп'ютерними мережами;
- розділ, що описує *правила розмежування* доступу до виробничої інформації;
- розділ, що характеризує *порядок розробки* й супроводу систем;
- розділ, що описує міри, спрямовані на забезпечення *безперервної роботи*

організації;

– юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

Існує 3 рівня:

– Верхній.

– Середній.

– Нижній.

Верхній рівень

Програму верхнього рівня очолює особа, відповідальна за інформаційну безпеку організації. У цієї програми наступні головні цілі:

– управління ризиками (*оцінка ризиків*, вибір ефективних засобів захисту);

– *координація* діяльності в області інформаційної безпеки, поповнення й розподіл ресурсів;

– *стратегічне планування*;

– *контроль* діяльності в області інформаційної безпеки.

У рамках програми верхнього рівня приймаються стратегічні рішення по забезпеченню безпеки, оцінюються технологічні новинки. Інформаційні технології розвиваються дуже швидко, і необхідно мати чітку політику відстеження й впровадження нових засобів.

Контроль діяльності в області безпеки має двосторонню спрямованість. По-перше, необхідно гарантувати, що дії організації не суперечать законам. При цьому варто підтримувати контакти із зовнішніми контролюючими організаціями. По-друге, потрібно постійно відслідковувати стан безпеки усередині організації, реагувати на випадки порушень і допрацьовувати захисні міри з урахуванням зміни обстановки.

Варто підкреслити, що програма верхнього рівня повинна займати строго певне місце в діяльності організації, вона повинна офіційно прийматися й підтримуватися керівництвом, а також мати певний штат і бюджет.

Середній рівень

До середнього рівня можна віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – відношення до передових (але, можливо, недостатньо

перевірених) технологій, доступ в Internet (як сполучити незалежність доступу до інформації із захистом від зовнішніх погроз?), використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення й т.д.

Політика середнього рівня повинна для кожного аспекту висвітлювати наступні теми:

– Опис аспекту. Наприклад, якщо розглянути застосування користувачами неофіційного програмного забезпечення, останнє можна визначити як ПЗ, що не було схвалено й/або закуплене на рівні організації.

– Область застосування. Варто визначити, де, коли, як, стосовно кого й чому застосовується дана *політика безпеки*.

– Позиція організації по даному аспекту. Продовжуючи приклад з неофіційним програмним забезпеченням, можна уявити собі позиції повної заборони, розробки процедури приймання подібного ПЗ й т.п. Позиція може бути сформульована й у набагато більше загальному виді, як набір цілей, які переслідує організація в даному аспекті. Взагалі стиль документів, що визначають політику безпеки (як і їхній перелік), у різних організаціях може сильно відрізнятися.

– Ролі й обов'язки. В «політичний» документ необхідно включити інформацію про посадові особи, відповідальні за реалізацію політики безпеки. Наприклад, якщо для використання неофіційного програмного забезпечення співробітникам потрібен дозвіл керівництва, повинне бути відомо, у кого і як його можна одержати. Якщо неофіційне програмне забезпечення використовувати не можна, варто знати, хто стежить за виконанням даного правила.

– Законослухняність. Політика повинна містити загальний опис заборонених дій і покарань за них.

– Точки контакту. Повинно бути відомо, куди варто звертатися за роз'ясненнями, допомогою й додатковою інформацією. Звичайно «точкою контакту» служать певні посадові особи, а не конкретна людина, що займає в цей момент даний пост.

Нижній рівень

Політика безпеки **нижнього рівня відноситься до конкретних інформаційних сервісів.** Вона містить у собі два аспекти – цілі й правила їхнього

досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута *політика* повинна бути визначена більш докладно. Є багато речей, специфічних для окремих видів послуг, які не можна єдиним образом регламентувати в рамках всієї організації. У той же час, ці речі настільки важливі для забезпечення режиму безпеки, що стосовні до них рішення повинні прийматися на управлінському, а не технічному рівні. Приведемо кілька прикладів питань, на які варто дати відповідь у політику безпеки нижнього рівня:

- хто має право доступу до об'єктів, підтримуваним сервісом?
- при яких умовах можна читати й модифікувати дані?
- як організований віддалений доступ до сервісу?

При формулюванні цілей політики нижнього рівня можна виходити з міркувань цілісності, доступності й конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути більше конкретними. Наприклад, якщо мова йде про систему розрахунку заробітної плати, можна поставити ціль, щоб тільки співробітникам відділу кадрів і бухгалтерії дозволялося вводити й модифікувати інформацію. У більш загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу й дії з ними.

Із цілей виводяться правила безпеки, що описують, хто, що й при яких умовах може робити. Чим докладніше правила, тим більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними засобами. З іншого боку, занадто тверді правила можуть заважати роботі користувачів, імовірно, їх прийдеться часто переглядати. Керівництву має бути знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не виявляться надмірно зв'язані. Звичайно найбільше формально задаються права доступу до об'єктів через особливу важливість даного питання.

Ціль програми нижнього рівня – забезпечити надійний і економічний захист конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які варто використовувати механізми захисту; закупаються й установлюються технічні засоби; виконується повсякденне адміністрування; відслідковується стан слабких місць і т.п. Звичайно за програму нижнього рівня відповідають адміністратори сервісів.

Програма безпеки

Після того, як сформульована *політика безпеки*, можна приступати до складання програми її реалізації й властиво до реалізації.

Щоб зрозуміти й реалізувати яку-небудь програму, її потрібно структурувати по рівнях, звичайно у відповідності зі структурою організації. У найпростішому й найпоширенішому випадку досить двох рівнів – верхнього, або центрального, котрий охоплює всю організацію, і нижнього, або службового, котрий відноситься до окремих послуг або груп однорідних сервісів.

Синхронізація програми безпеки з життєвим циклом систем

Якщо синхронізувати програму безпеки нижнього рівня з *життєвим циклом* сервісу, що захищається, можна домогтися більшого ефекту з меншими витратами. Програмісти знають, що додати нову можливість до вже готової системи на порядок складніше, ніж споконвічно спроектувати й реалізувати її. Те ж справедливо й для інформаційної **безпеки.**

У *життєвому циклі* інформаційного сервісу можна виділити наступні етапи:

Ініціація. На даному етапі виявляється необхідність у придбанні нового сервісу, документується його передбачуване призначення. З погляду безпеки найважливішою дією тут є оцінка критичності як самого сервісу, так і інформації, що з його допомогою буде оброблятися.

Закупівля. На даному етапі складаються специфікації, пробляються варіанти придбання, виконується властиво *закупівля*. Зрозуміло, особлива увага повинне приділятися питанням сумісності нового сервісу з існуючою конфігурацією. Підкреслимо також, що нерідко засобу безпеки є необов'язковими компонентами комерційних продуктів, і потрібно простежити, щоб відповідні пункти не випали зі специфікації.

Установка. Сервіс установлюється, конфігурується, тестується й вводиться в *експлуатацію*. Як правило, комерційні продукти поставляються з відключеними засобами безпеки; їх необхідно включити й належним чином налаштувати. Для великої організації, де багато користувачів і даних, початкове настроювання може

стати досить трудомісткою й відповідальною справою. По- друге, новий сервіс має потребу в процедурних регуляторах. Варто подбати про чистоту й охорону приміщення, про документи, що регламентують використання сервісу, про підготовку планів на випадок екстрених ситуацій, про організацію навчання користувачів і т.п.

Експлуатація. На даному етапі сервіс не тільки працює й адмініструється, але й піддається модифікаціям. Якщо безпека не підтримувати, вона слабшає. Користувачі не настільки ревно виконують посадові інструкції, адміністратори менш ретельно аналізують реєстраційну інформацію. То той, то інший користувач одержує додаткові привілеї. Здається, що в сутності нічого не змінилося; насправді ж від колишньої безпеки не залишилося й сліду. Для боротьби з ефектом повільних змін доводиться прибігати до періодичних перевірок безпеки сервісу.

Виведення з експлуатації. Відбувається перехід на новий сервіс. Тільки в специфічних випадках необхідно піклуватися про фізичне руйнування апаратних компонентів, що зберігають конфіденційну інформацію. При *виведенні даних з експлуатації* їх звичайно переносять на іншу систему, архівують, викидають або знищують.

ДСТУ ISO/IEC 27003:2018

ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT) – забезпечує висвітлення та управління на ISO/IEC 27001:2013.

ISO/IEC 27003 містить керівні вказівки щодо вимог до системи управління інформаційною безпекою (СУІБ), як зазначено у стандарті ISO/IEC 27001, і надає рекомендації, можливості та дозволи щодо них. Цей документ не передбачає надання загальних рекомендацій з усіх аспектів інформаційної безпеки. Статті 4-

10 цього документа відображають структуру ISO/IEC 27001:2013. Стандарт ISO/IEC 27003 не додає нових вимог до СУІБ та пов'язаних з ними термінів та визначень. Організації, що впроваджують СУІБ, не зобов'язані дотримуватися вказівок у цьому документі. СУІБ підкреслює важливість наступних етапів:

розуміння потреб організації та необхідності встановлення політики інформаційної безпеки та цілей інформаційної безпеки;

оцінка ризиків організації, пов'язаних з інформаційною безпекою;

впровадження та керування процесами інформаційної безпеки, контролю та іншими заходами щодо ліквідації ризиків;

моніторинг та перевірка продуктивності та ефективності СУІБ;

впровадження постійного вдосконалення СУІБ.

СУІБ, подібний до будь-якого іншого типу системи управління, включає такі **ключові компоненти**:

а) політика;

б) особи з визначеними обов'язками;

в) процеси управління, пов'язані з:

- встановлення політики;
- забезпечення обізнаності та компетентності;
- планування;
- реалізація;
- експлуатація;
- оцінка продуктивності;
- огляд управління;
- вдосконалення;

г) документально підтверджена інформація.

СУІБ має додаткові ключові компоненти, такі як: д) оцінка ризику інформаційної безпеки;

є) обробка ризиків інформаційної безпеки, включаючи детермінацію та здійснення контролю.

Цей документ є загальним і призначений для застосування до всіх організацій, незалежно від типу (державні чи комерційні) та розміру. Організація повинна визначити, яка частина цього стандарту поширюється на неї відповідно до її специфічного організаційного контексту (Стаття 4 ISO/IEC 27001:2013). Деякі інструкції можуть бути придатними для великих організацій, але для дуже маленьких організацій (наприклад, з менш ніж 10 співробітниками) можуть бути непотрібними або неприйнятними.

6.3. ISO/IEC 15408- 2, ISO/IEC 15408-3

Стек стандартів **ISO/IEC 15408 включає в себе наступні стандарти:**

ISO/IEC 15408-1/2/3:2017 Інформаційні технології. Методи захисту. Критерії оцінки:

Частина 1. Вступ та загальна модель (ISO/IEC 15408-1: 2022, IDT).

Частина 2. Функціональні вимоги (ISO/IEC 15408-2: 2022, IDT).

Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3: 2022, IDT).

Стандарт містить загальний набір вимог до функцій безпеки IT-продуктів і систем, а також до заходів гарантії, застосованих до них під час оцінки безпеки.

Якщо взяти європейські стандарти, відносно яких відбувається гармонізація, то їх вже 5:

ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 1. Вступ і загальна модель

Цей документ встановлює загальні концепції та принципи оцінювання безпеки IT і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки IT-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки IT-продуктів.

Цей документ представляє:

- ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;
- опис організації компонентів безпеки по всій моделі;
- різні операції, за допомогою яких функціональні компоненти та компоненти

гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

- загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;
- настанова щодо застосування ISO/IEC 15408-4 для розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;
- загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;
- інформація щодо обсягу схем оцінювання.

ISO/IEC 15408-2:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 2. Функціональні компоненти безпеки.

Цей документ визначає необхідну структуру та зміст функціональних компонентів безпеки з метою оцінки безпеки. Він містить каталог функціональних компонентів, який відповідає загальним вимогам безпеки багатьох IT-продуктів.

ISO/IEC 15408-3:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання IT-безпеки. Частина 3. Компоненти забезпечення безпеки.

Цей документ визначає вимоги серії стандартів ISO/IEC 15408. Він включає окремі компоненти гарантії, з яких складаються рівні гарантії оцінки та інші пакети, що містяться в ISO/IEC 15408-5, а також критерії для оцінки профілів захисту (PP), конфігурацій PP, модулів PP та цілей безпеки (STs).

ISO/IEC 15408-4:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 4. Структура для специфікації методів оцінювання та діяльності

Цей документ забезпечує стандартизовану структуру для визначення об’єктивних, повторюваних і відтворюваних методів оцінювання та діяльності з оцінювання. Цей документ не визначає, як оцінювати, приймати або підтримувати методи оцінювання та діяльність з оцінювання. Ці аспекти є справою для тих, хто розробляє методи оцінювання та діяльність з оцінювання в їхній конкретній сфері інтересів.

ISO/IEC 15408-5:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінювання ІТ-безпеки. Частина 5. Попередньо визначені пакети вимог до безпеки.

Цей документ надає пакети забезпечення безпеки та функціональні вимоги безпеки, які були визначені як корисні для підтримки загального використання зацікавленими сторонами.

Приклади наданих пакетів включають рівні гарантії оцінювання (EAL) і складені пакети гарантій (CAP).

Цей документ представляє:

- сімейство пакетів *рівня гарантії оцінки (EAL),* які визначають попередньо визначені набори компонентів гарантії безпеки, на які можна посилатися в PP та ST, і які визначають відповідні гарантії безпеки, які необхідно надати під час оцінювання цілі оцінки (TOE);
- сімейство пакетів *гарантії композиції (CAP),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінювання складених ТО;
- пакет *складеного продукту (COMP),* який визначає набір компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінювання TOE складеного продукту;
- сімейство пакетів *гарантії профілю захисту (PPA),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають надаватися під час оцінювання профілю захисту;
- сімейство пакетів *гарантії цільової безпеки (STA),* які вказують набори компонентів гарантії безпеки, що використовуються для визначення відповідних гарантій безпеки, які мають бути надані під час оцінки цільової безпеки.

Серед користувачів цього документа можуть бути споживачі, розробники та оцінювачі безпечних ІТ-продуктів.

Опис стандарту 15408

У стандарті, що отримав назву «Загальні критерії оцінки безпеки інформаційних технологій » (The Common Criteria for Information Technology Security Evaluation), докладно розглянуто загальні підходи, методи та функції забезпечення захисту інформації в організаціях.

Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. **Всі функції представлені у вигляді чотирирівневої ієрархічної структури**: клас – сімейство – компонент – елемент.

За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ.

У стандарті виділені 11 класів функцій:

- аудит;
- ідентифікація та аутентифікація;
- криптографічний захист;
- конфіденційність;
- передача даних;
- захист даних користувача;
- управління безпекою;
- захист функцій безпеки системи;
- використання ресурсів;
- доступ до системи;
- надійність засобів.

Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих у стандарті функцій. У ISO 15408 міститься **ряд зумовлених моделей** (так званих **профілів),** що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих засобів. Простим прикладом профілів може служити модель міжмережевого екрану.

Сертифікований профіль являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об'єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об'єкта.

Стандарт ISO 15408 вигідно відрізняє **відкритість.** Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначена також послідовність дій для самостійного створення профілів.

Загальні критерії узагальнили зміст і досвід використання Помаранчевої книги, розвинули рівні впевненості Європейських критеріїв, втілили в реальні структури концепцію профілів захисту Федеральних критеріїв США.

Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) описує інфраструктуру (Framework) в якій користувачі комп'ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цій стпндарт дозволяє бути впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку.

У "Загальних критеріях" (ЗК) проведена класифікація широкого набору функціональних вимог і вимог довіри до безпеки, визначені структури їх групування і принципи цільового використання

Загальні критерії дозволяють підвищити довіру до засобів захисту і самої інформації, що захищається за рахунок трьох основних якостей:

1. Можливості гнучкого завдання вимог до засобів захисту інформації з урахуванням їх призначення і умов застосування.
2. Більш повного і обгрунтованого набору вимог безпеки.
3. Наявності методології оцінки, що забезпечує об'єктивність і порівнянність результатів.

Загальні критерії являють собою набір з п'яти окремих взаємопов'язаних частин. До них відносяться:

– Введення і загальна модель.

– Функціональні вимоги безпеки.

– Вимоги до надійності захисних механізмів.

– Попереднє визначення профілі захисту.

– Процедури реєстрації профілів захисту.

Основними відмітними рисами ЗК є наступні:

1. Перш за все, ЗК – це певна методологія та система формування вимог і оцінки безпеки ІТ. Системність простежується, починаючи від термінології та рівнів абстракції представлення вимог аж до їх застосування при оцінці безпеки на всіх етапах життєвого циклу продуктів і систем ІТ.

2. Загальні критерії характеризуються найбільш повною на сьогоднішній день сукупністю вимог безпеки ІТ.

3. У ЗК проведено чіткий поділ вимог безпеки на функціональні вимоги і вимоги довіри до безпеки. **Функціональні вимоги** (11 класів, 66 родин, 135 компонентів) відносяться до **функцій безпеки** (ідентифікації, аутентифікації, управління доступом, аудиту і т. д.), а **вимоги довіри** (8 класів,
44 сімейства, 93 компонента) – до досягнення **впевненості в коректності реалізації та ефективності функцій безпеки** шляхом оцінки технології розробки, тестування, аналізу вразливостей експлуатаційної документації, постачання і супроводу продуктів та систем ІТ.

4. Загальні критерії включають шкалу довіри до безпеки (оціночні рівні довіри – ОРД), яка може використовуватися для отримання різного ступеня впевненості у безпеці продуктів і систем ІТ

5. Систематизація і класифікація вимог щодо ієрархії «клас» – «сімейство» – «компонент» – «елемент» з унікальними ідентифікаторами вимог забезпечує зручність їх використання.

6. Компоненти вимог в родинах і класах ранжовані за ступенем повноти і строгості, а вимоги довіри згруповані в пакети вимог

7. Гнучкість у підході до формування вимог безпеки для різних типів продуктів і систем ІТ та умов їх застосування забезпечується можливістю цілеспрямованого формування необхідних наборів вимог у вигляді певних в ЗК стандартизованих структур (пакетів вимог, профілів захисту і завдань з безпеки).

8. Загальні критерії володіють відкритістю і розширюваністю, тобто дозволяють уточнювати існуючі і вводити додаткові вимоги.

Як показують оцінки фахівців у галузі інформаційної безпеки за рівнем систематизації, повноті і можливостям деталізації вимог, універсальності і гнучкості в застосуванні ЗК представляють найбільш досконалий з існуючих в даний час стандартів. Причому, що дуже важливо, в силу особливостей побудови він має практично необмежені можливості для розвитку і являє собою базовий стандарт, що містить методологію завдання вимог і оцінки безпеки ІТ, а також систематизований каталог вимог безпеки. Як функціональних стандартів, в яких

формулюються вимоги до безпеки певних типів продуктів і систем ІТ, передбачається використання профілів захисту (ПЗ), що створюються за методологією і на основі каталогу вимог ЗК. У ПЗ можуть бути включені і будь- які інші вимоги, які є необхідними для забезпечення безпеки конкретного типу продуктів або систем ІТ.

6.4. Стек протоколів ДСТУ ISO/IEC 27000

Крім вищеперерахованих протоколів ДСТУ ISO/IEC 27000, 27001, 27002, 27003, до даного стеку протоколів відносяться наступні:

– **ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT) –** ISO/IEC 27004:2016 містить настанови, спрямовані на допомогу організаціям в оцінюванні ефективності інформаційної безпеки та ефективності системи управління інформаційною безпекою з метою виконання вимог ISO/IEC 27001:2013, 9.1. Він встановлює: моніторинг та вимірювання ефективності інформаційної безпеки; моніторинг та вимірювання ефективності системи управління інформаційною безпекою (СУІБ), включаючи її процеси та засоби контролю; аналіз та оцінка результатів моніторингу та вимірювання. ISO/IEC 27004:2016 застосовний до організацій усіх типів і розмірів.

– **ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) –** Цей документ містить вказівки щодо управління ризиками інформаційної безпеки. Цей документ підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння задовільній реалізації інформаційної безпеки на основі підходу до управління ризиками. Знання концепцій, моделей, процесів і термінології, описаних у ISO/IEC 27001 та ISO/IEC 27002, є важливим для повного розуміння цього документа. Цей документ застосовується до всіх типів організацій (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які мають намір керувати ризиками, які можуть поставити під загрозу інформаційну безпеку організації.

– **ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT) –** Цей стандарт визначає вимоги та надає настанови для організацій, які надають послуги з аудиту та сертифікації систем управління інформаційною безпекою (СУІБ) додатково до вимог, що містяться в ISO/IEC 17021-1 та ISO/IEC 27001. Це, в першу чергу, спрямовано на підтримку акредитації організацій, які надають послуги із сертифікації СУІБ. Вимоги, які містить цей стандарт, необхідно продемонструвати в термінах компетентності та надійності всім організаціям, які здійснюють сертифікацію СУІБ, а настанови, долучені до цього стандарту, надають додаткову інтерпретацію цих вимог для будь-якої організації, яка виконує сертифікацію СУІБ. Цей стандарт може бути застосований як документ критеріїв для акредитації, експертного оцінювання або інших процесів аудиту.

– **ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем управління інформаційною безпекою (ISO/IEC 27007:2017, IDT) –** Цей документ містить вказівки щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ), щодо проведення аудитів та компетентності аудиторів СУІБ, на додаток до вказівок, що містяться в ISO 19011. Цей документ стосується тих, хто потребує розуміння чи проведення

внутрішніх чи зовнішніх аудитів СУІБ або управління програмою аудиту СУІБ.

– **ДСТУ ISO/IEC TS 27008:2019 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки (ISO/IEC TS 27008:2019, IDT) –** У цьому документі містяться вказівки щодо перегляду та оцінки впровадження та функціонування засобів контролю інформаційної безпеки, включаючи технічну оцінку засобів контролю інформаційної системи, відповідно до встановлених організацією вимог до інформаційної безпеки, включаючи технічну відповідність критеріям оцінки на основі вимог інформаційної безпеки, встановлених організації. У цьому документі пропонуються вказівки щодо того, як переглядати та оцінювати засоби контролю інформаційної безпеки, якими керують через систему управління інформаційною безпекою, визначену ISO/IEC 27001. Він застосовний до організацій усіх типів і розмірів, включаючи державні та приватні компанії, державні установи та некомерційні організації, які проводять огляди інформаційної безпеки та перевірки технічної відповідності.

– **ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT) –** Цей документ визначає вимоги до створення галузевих стандартів, які розширюють ISO/IEC 27001 і доповнюють або змінюють ISO/IEC 27002 для підтримки конкретного сектора (домену, області застосування або ринку). Цей документ пояснює, як: включати вимоги на додаток до вимог ISO/IEC 27001: уточнювати або інтерпретувати будь-які вимоги ISO/IEC 27001; включати засоби контролю на додаток до засобів ISO/IEC 27001:2013, Додаток А та ISO/IEC 27002; модифікувати будь-які засоби управління ISO/IEC 27001:2013, додаток А та ISO/IEC 27002; додати настанови до або змінити настанови ISO/IEC 27002. У цьому документі зазначено, що додаткові чи вдосконалені вимоги не роблять вимоги ISO/IEC 27001 недійсними. Цей документ застосовується до тих, хто бере участь у розробці галузевих стандартів.

– **ДСТУ ISO/IEC 27010:2018 Інформаційні технології. Методи захисту. Управління інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій (ISO/IEC 27010:2015, IDT) –** ISO/IEC 27010:2015

надає рекомендації на додаток до вказівок, наданих у сімействі стандартів ISO/IEC 27000, для впровадження управління інформаційною безпекою в спільнотах обміну інформацією. Цей міжнародний стандарт надає засоби контролю та вказівки, що стосуються, зокрема, ініціювання, впровадження, підтримки та покращення інформаційної безпеки в міжорганізаційних та міжгалузевих комунікаціях. Він містить вказівки та загальні принципи щодо того, як зазначені вимоги можуть бути виконані за допомогою встановлених повідомлень та інших технічних методів. Цей міжнародний стандарт застосовний до всіх форм обміну та спільного використання конфіденційної інформації, як загальнодоступної, так і приватної, на національному та міжнародному рівнях, у межах однієї галузі чи сектора ринку чи між секторами. Зокрема, це може бути застосовано до обміну інформацією та спільного використання, що стосується забезпечення, підтримки та захисту критичної інфраструктури організації або національної держави. Він призначений для підтримки створення довіри під час обміну конфіденційною інформацією та заохочення тим самим міжнародного зростання спільнот обміну інформацією.

– **ДСТУ ISO/IEC 27011:2018 Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо управління інформаційною безпекою на основі ISO/IEC 27002 (ISO/IEC 27011:2016, IDT) –** Сфера застосування цієї Рекомендації | ISO/IEC 27011:2016 має визначити настанови, що підтримують впровадження засобів контролю інформаційної безпеки в телекомунікаційних організаціях. Прийняття цієї Рекомендації | ISO/IEC 27011:2016 дозволить телекомунікаційним організаціям відповідати базовим вимогам управління безпекою інформації щодо конфіденційності, цілісності, доступності та будь-яких інших відповідних властивостей безпеки.

– **ДСТУ ISO/IEC 27013:2017 Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 (ISO/IEC 27013:2015, IDT) –** ISO/IEC 27013:2021. Інформаційна безпека, кібербезпека та захист конфіденційності – Настанови щодо інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1 – Цей документ містить вказівки щодо інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-

1 для організацій, які мають намір: запровадити ISO/IEC27001, коли вже запроваджено ISO/IEC 20000-1, або навпаки; впроваджувати як ISO/IEC27001, так і ISO/IEC 20000-1 разом; інтегрувати існуючі системи менеджменту на основі ISO/IEC27001 та ISO/IEC 20000-1. Цей документ зосереджується виключно на інтегрованій реалізації системи управління інформаційною безпекою (ISMS), як зазначено в ISO/IEC 27001, і системи управління послугами (SMS), як зазначено в ISO/IEC 20000-1.

– **ISO/IEC 27014:2020. Інформаційна безпека, кібербезпека та захист конфіденційності – Управління інформаційною безпекою** – У цьому документі містяться вказівки щодо концепцій, цілей і процесів управління інформаційною безпекою, за допомогою яких організації можуть оцінювати, спрямовувати, контролювати та передавати пов'язані з інформаційною безпекою процеси всередині організації. Цільова аудиторія цього документа: орган управління та вище керівництво; тих, хто відповідає за оцінку, управління та моніторинг системи управління інформаційною безпекою (СУІБ) на основі ISO/IEC 27001; особи, відповідальні за управління інформаційною безпекою, яке відбувається поза сферою СУІБ на основі ISO/IEC 27001, але в межах сфери управління. Цей документ застосовується до організацій усіх типів і розмірів. Усі посилання на СУІБ у цьому документі стосуються СУІБ на основі ISO/IEC 27001. Цей документ зосереджується на трьох типах організацій СУІБ, наведених у Додатку B. Однак цей документ також може використовуватися іншими типами організацій.

– **ISO/IEC TR 27015:2012. Інформаційні технології – Методи безпеки – Настанови щодо управління інформаційною безпекою для фінансових послуг** – ISO/IEC TR 27015:2012 містить інструкції з інформаційної безпеки, які доповнюють засоби контролю інформаційної безпеки, визначені в ISO/IEC 27002:2005, для ініціювання, впровадження, підтримки та покращення інформаційної безпеки в організаціях, що надають фінансові послуги.

– **ISO/IEC TR 27016:2014. Інформаційні технології – Техніка безпеки – Управління інформаційною безпекою – Економіка організації** – ISO/IEC TR 27016:2014 надає вказівки щодо того, як організація може

приймати рішення щодо захисту інформації та розуміння економічних наслідків цих рішень у контексті конкуруючих вимог до ресурсів. ISO/IEC TR 27016:2014 застосовний до організацій усіх типів і розмірів і надає інформацію для прийняття економічних рішень щодо управління інформаційною безпекою вищим керівництвом, яке несе відповідальність за рішення щодо інформаційної безпеки.

– **ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT) –** Цей стандарт надає рекомендації щодо заходів інформаційної безпеки, які застосовують для надання та застосування хмарних послуг, за допомогою формування: додаткових рекомендацій щодо впровадження для відповідних заходів безпеки, визначених в ISO/IEC 27002; додаткових заходів безпеки з рекомендаціями щодо впровадження, що конкретно стосуються хмарних послуг. У цьому стандарті наведено заходи безпеки та рекомендації щодо впровадження як для провайдерів, так і для споживачів хмарних послуг.

– **ДСТУ ISO/IEC 27018:2019 Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII (ISO/IEC 27018:2019, IDT) –** У цьому документі встановлюються загальноприйняті цілі контролю, засоби контролю та вказівки щодо впровадження заходів із захисту особистої ідентифікаційної інформації (PII) відповідно до принципів конфіденційності в ISO/IEC 29100 для загальнодоступного середовища хмарних обчислень. Зокрема, цей документ містить інструкції на основі ISO/IEC 27002, беручи до уваги нормативні вимоги щодо захисту ідентифікаційної інформації, які можуть бути застосовані в контексті середовища(ів) ризику інформаційної безпеки постачальника публічних хмарних послуг. Цей документ стосується організацій усіх типів і розмірів, у тому числі державних і приватних компаній, державних установ і некомерційних організацій, які надають послуги з обробки інформації як процесори ідентифікаційної інформації через хмарні обчислення за контрактом з іншими організаціями. Рекомендації в цьому документі також можуть стосуватися організацій, які виконують функції контролерів ідентифікаційної інформації. Однак

на контролери ідентифікаційної інформації можуть поширюватися додаткові законодавчі акти, положення та зобов'язання щодо захисту ідентифікаційної інформації, які не стосуються обробників ідентифікаційної інформації. Цей документ не призначений для покриття таких додаткових зобов'язань.

– **ДСТУ ISO/IEC 27019:2019 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою для енергопостачальних організацій (ISO/IEC 27019:2017, IDT) –** ISO/IEC 27019:2017 надає вказівки на основі ISO/IEC 27002:2013, застосовані до систем управління процесами, що використовуються в енергетиці для контролю та моніторингу виробництва або виробництва, передачі, зберігання та розподілу електроенергії, газу, нафти та тепла, а також для контролю відповідних допоміжних процесів. Це включає, зокрема, таке: технологія централізованого та розподіленого управління процесами, моніторингу та автоматизації, а також інформаційні системи, що використовуються для їх роботи, такі як пристрої програмування та параметризації; цифрові контролери та компоненти автоматизації, такі як контрольні та польові пристрої або програмовані логічні контролери (PLC), включаючи цифрові датчики та виконавчі елементи; усі додаткові допоміжні інформаційні системи, що використовуються в області управління процесом, наприклад, для додаткових задач візуалізації даних і для контролю, моніторингу, архівування даних, реєстрації історії, звітності та документації; комунікаційна технологія, яка використовується в області управління процесом, наприклад, мережі, телеметрія, програми телеконтролю та технології дистанційного управління; Компоненти розширеної інфраструктури вимірювання (AMI), наприклад розумні лічильники; вимірювальні пристрої, наприклад, для значень викидів; цифрові системи захисту та безпеки, наприклад реле захисту, ПЛК безпеки, механізми аварійного регулювання; системи енергоменеджменту,

наприклад розподілених енергетичних ресурсів (DER), інфраструктури електричних зарядок у приватних домогосподарствах, житлових будинках або промислових установках споживачів; розподілені компоненти середовища інтелектуальної мережі, наприклад, в енергетичних мережах, у приватних домогосподарствах, житлових будинках або промислових установках споживачів; усе програмне забезпечення,

мікропрограми та програми, встановлені у вищезазначених системах, наприклад програми DMS (система управління розподілом) або OMS (система управління збоями); будь-які приміщення, в яких розміщено вищезазначене обладнання та системи; системи дистанційного обслуговування вищевказаних систем. ISO/IEC 27019:2017 не застосовується до області управління процесом ядерних установок. Цей домен охоплює стандарт IEC 62645. ISO/IEC 27019:2017 також містить вимогу щодо адаптації процесів оцінки та обробки ризиків, описаних у ISO/IEC 27001:2013, до вказівок, які наведені в цьому документі в секторі енергетики.

– **ДСТУ ISO/IEC 27021:2018 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги до компетенції професіоналів з управління інформацією (ISO/IEC 27021:2017, IDT**) – ISO/IEC 27021:2017 визначає вимоги до компетентності для фахівців із СУІБ, які керують або беруть участь у створенні, впровадженні, підтримці та постійному вдосконаленні одного або кількох процесів системи управління інформаційною безпекою, які відповідають ISO/IEC 27001.

– **ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT) –** ISO/IEC 27031:2011 описує концепції та принципи готовності інформаційно-комунікаційних технологій (ІКТ) до безперервності бізнесу та надає структуру методів і процесів для ідентифікації та визначення всіх аспектів (таких як критерії ефективності, проектування та впровадження) для підвищення готовності організації до ІКТ для забезпечення безперервності бізнесу. Це стосується будь-якої організації (приватної, урядової та неурядової, незалежно від розміру), яка розробляє свою програму готовності до ІКТ для забезпечення безперервності бізнесу (IRBC), і вимагає, щоб її послуги/інфраструктури ІКТ були готові підтримувати бізнес-операції у разі виникнення події та інциденти, а також пов’язані з ними збої, які можуть вплинути на безперервність (включаючи безпеку) критичних бізнес-функцій. Сфера застосування ISO/IEC 27031:2011 охоплює всі події та інциденти (включаючи

пов’язані з безпекою), які можуть вплинути на інфраструктуру та системи ІКТ. Він включає в себе та розширює практики обробки інцидентів інформаційної безпеки та управління ними, а також планування готовності до ІКТ та послуги.

– **ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT) –** Цей стандарт містить рекомендації щодо підвищення рівня кібербезпеки, розглядаючи різні

аспекти цього питання та їхній зв’язок з іншими видами безпеки, зокрема: інформаційною безпекою; мережевою безпекою; Інтернет-безпекою; захистом інформаційної інфраструктури. У стандарті розглянуто основні методи захисту зацікавлених сторін у кіберпросторі. Стандарт містить: огляд кібербезпеки; пояснення зв’язків між кібербезпекою та іншими видами безпеки; визначення зацікавлених сторін та їхньої ролі в кіберпросторі; настанова з вирішення основних питань кібербезпеки; способи взаємодії зацікавлених сторін для вирішення основних питань кібербезпеки. Цей стандарт стосується постачальників послуг у кіберпросторі. Але цільова аудиторія охоплює також споживачів, які користуються цими послугами. Якщо організації надають послуги в кіберпросторі іншим організаціям або людям для домашнього використання, то таким організаціям може знадобитися підготувати настанови на основі цього стандарту, які міститимуть додаткові пояснення або приклади, необхідні для повного розуміння читачами того, як треба діяти.

– **ДСТУ ISO/IEC 27033:2017. Інформаційні технології. Методи захисту. Безпека мережі. – складається з 6 частин:**

– ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT) – ISO/IEC 27033-1:2015 містить огляд мережевої безпеки та відповідних визначень. Він визначає й описує концепції, пов’язані з мережевою безпекою, і надає вказівки щодо управління нею. (Мережева безпека стосується безпеки пристроїв, безпеки управлінських дій, пов’язаних із пристроями, програмами/службами та кінцевими користувачами, на додаток до безпеки інформації, що передається через канали зв’язку.) Це актуально для всіх, хто бере участь у володінні, експлуатації або

використанні мережі. Це включає керівників вищої ланки та інших нетехнічних менеджерів або користувачів, на додаток до керівників і адміністраторів, які мають конкретні обов'язки за інформаційну безпеку та/або безпеку мережі, роботу мережі або які відповідають за загальну програму безпеки організації та розробку політики безпеки. Це також актуально для всіх, хто бере участь у плануванні, проектуванні та реалізації архітектурних аспектів безпеки мережі. ISO/IEC 27033-1:2015 також включає наступне: надає вказівки щодо того, як ідентифікувати та аналізувати ризики безпеки мережі та визначення вимог безпеки мережі на основі цього аналізу; надає огляд елементів управління, які підтримують архітектури технічної безпеки мережі та відповідні технічні засоби контролю, а також тих нетехнічних засобів контролю та технічних засобів контролю, які застосовуються не лише до мереж; знайомить із тим, як досягти високоякісної архітектури технічної безпеки мережі, а також аспекти ризику, дизайну та контролю, пов'язані з типовими мережевими сценаріями та областями мережевих «технологій» (які детально розглядаються в наступних частинах ISO/IEC 27033), і коротко розглядає питання, пов'язані з впровадженням і експлуатацією засобів контролю безпеки мережі, а також постійний моніторинг і перегляд їх впровадження. Загалом він містить огляд цього міжнародного стандарту та «дорожню карту» для всіх інших частин.

– ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT) – ISO/IEC 27033-2:2012 містить вказівки для організацій щодо планування, проектування, впровадження та документування безпеки мережі.

– ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 3. Еталонні мережеві сценарії.

– Загрози, методи проектування та проблеми управління (ISO/IEC 27033-3:2010, IDT) – ISO/IEC 27033-3:2010 описує загрози, методи проектування та проблеми управління, пов'язані зі сценаріями еталонної мережі. Для кожного сценарію в ньому надаються детальні вказівки щодо загроз безпеці, а також методи розробки безпеки та засоби контролю, необхідні для пом'якшення пов'язаних ризиків. У відповідних випадках він містить посилання на ISO/IEC 27033- 4 –

ISO/IEC 27033-6, щоб уникнути дублювання змісту цих документів. Інформація в ISO/IEC 27033-3:2010 призначена для використання під час перегляду архітектури/проекту технічної безпеки та під час вибору та документування бажаної архітектури/проекту технічної безпеки та пов'язаних засобів контролю безпеки відповідно до ISO/IEC 27033-2. Вибрана конкретна інформація (разом з інформацією, вибраною з ISO/IEC 27033-4 до ISO/IEC 27033-6) залежатиме від характеристик мережевого середовища, що перевіряється, тобто конкретного мережевого сценарію(ів) і теми «технології». Загалом, ISO/IEC 27033-3:2010 суттєво допоможе в комплексному визначенні та реалізації безпеки для мережевого середовища будь-якої організації.

– ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT) – ISO/IEC 27033- 4:2014 містить настанови щодо захисту зв'язку між мережами за допомогою шлюзів безпеки (брандмауер, брандмауер програм, система захисту від вторгнень тощо) відповідно до задокументованої політики інформаційної безпеки шлюзів безпеки, включаючи: виявлення та аналіз загроз мережевій безпеці, пов'язаних зі шлюзами безпеки; визначення вимог безпеки мережі для шлюзів безпеки на основі аналізу загроз; використання методів для проектування та впровадження для вирішення загроз та аспектів контролю, пов'язаних із типовими мережевими сценаріями; вирішення проблем, пов'язаних із впровадженням, експлуатацією, моніторингом та переглядом елементів управління шлюзом безпеки мережі.

– ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT) – ISO/IEC 27033-5:2013 містить вказівки щодо вибору, впровадження та моніторингу технічних засобів контролю, необхідних для забезпечення безпеки мережі за допомогою з'єднань віртуальної приватної мережі (VPN) для з'єднання мереж і підключення віддалених користувачів до мереж.

– ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі

(ISO/IEC 27033-6:2016, IDT) – ISO/IEC 27033-6:2016 описує загрози, вимоги безпеки, контроль безпеки та методи проектування, пов'язані з безпроводовими мережами. Він містить вказівки щодо вибору, впровадження та моніторингу технічних засобів контролю, необхідних для забезпечення безпечного зв'язку за допомогою безпроводових мереж. Інформація в цій частині ISO/IEC 27033 призначена для використання під час перегляду або вибору архітектури/проекту технічної безпеки, які передбачають використання безпроводової мережі відповідно до ISO/IEC 27033-2. Загалом, ISO/IEC 27033-6 значно допоможе у всебічному визначенні та реалізації безпеки для безпроводового мережевого середовища будь-якої організації. Він призначений для користувачів і розробників, які відповідають за впровадження та підтримку технічного контролю, необхідного для забезпечення безпечних безпроводових мереж.

ISO/IEC CD 27033-7. Інформаційна технологія. Безпека мережі. Частина 7. Настанови щодо безпеки віртуалізації мережі – В стадії розробки

ДСТУ ISO/IEC 27034:2017 Інформаційні технології. Методи захисту. Безпека програм. – складається з 7 частин:

– ДСТУ ISO/IEC 27034-1:2017 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 1. Огляд і загальні поняття (ISO/IEC 27034-1:2011; Cor 1:2014, IDT) – ISO/IEC 27034 надає організаціям інструкції, які допомагають інтегрувати безпеку в процеси, які організації використовують для управління своїми додатками. У цьому стандарті наведено загальний огляд безпеки додатків. Вона представляє визначення, принципи та процеси, які стосуються безпеки додатків. ISO/IEC 27034 можна застосовувати для додатків, розроблених в організації чи придбаних у третьої сторони, а також у разі аутсорсингу розроблення чи експлуатації додатків.

– ДСТУ ISO/IEC 27034-2:2016 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 2. Основні нормативні положення організації (ISO/IEC 27034-2:2015, IDT) – ISO/IEC 27034-2:2015 містить детальний опис нормативної бази організації та надає керівництво для організацій щодо її впровадження.

– ДСТУ ISO/IEC 27034-3:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 3. Процес управління безпекою прикладних програм (ISO/IEC 27034-3:2018, IDT) – У цьому документі міститься детальний опис і інструкції щодо впровадження процесу управління безпекою додатків.

– ДСТУ ISO/IEC TS 27034-5-1:2019 Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних управління протоколами та захистом застосунків. Схеми XML (ISO/IEC TS 27034-5-1:2018, IDT) – ISO/IEC 27034-5 описує та пояснює мінімальний набір основних атрибутів контролю безпеки додатків (ASC), а також докладно описує дії та ролі еталонної моделі життєвого циклу безпеки додатків (ASLCRM).

– ДСТУ ISO/IEC 27034-6:2018 Інформаційні технології. Методи захисту. Безпека прикладних програм. Частина 6. Вивчення випадків (ISO/IEC 27034- 6:2016, IDT) – ISO/IEC 27034-6:2016 надає приклади використання ASC для конкретних застосувань. Зазначені тут ASC надаються лише з метою пояснення, і аудиторії рекомендується створити власні ASC для забезпечення безпеки програми.

– ISO/IEC 27034-7:2018. Інформаційні технології. Безпека додатків. Частина 7. Структура прогнозування впевненості – Цей документ описує мінімальні вимоги, коли необхідні дії, визначені контролем безпеки додатків (ASC), замінюються обґрунтуванням безпеки додатків прогнозування (PASR). ASC, зіставлений із PASR, визначає очікуваний рівень довіри для наступної програми. У контексті очікуваного рівня довіри завжди існує оригінальна заявка, у якій команда проекту виконувала дії зазначеного ASC для досягнення фактичного рівня довіри. Використання обґрунтувань безпеки додатків прогнозування (PASR), визначених у цьому документі, застосовується до проектних груп, які мають визначену нормативну структуру додатків (ANF) і оригінальну програму з фактичним рівнем довіри. Прогнози щодо агрегування кількох компонентів або історії розробника щодо інших програм виходять за рамки цього документа.

– **ДСТУ ISO/IEC 27035:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. – складається з 4 частин:**

– ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту.

Управління інцидентами інформаційної безпеки. Частина 1. Принципи управління інцидентами (ISO/IEC 27035-1:2016, IDT) – ISO/IEC 27035-1:2016 є основою цього багатокомпонентного міжнародного стандарту. Він представляє основні концепції та етапи управління інцидентами інформаційної безпеки та поєднує ці концепції з принципами в структурованому підході до виявлення, звітування, оцінювання та реагування на інциденти, а також застосування отриманих уроків. Принципи, наведені в ISO/IEC 27035-1:2016, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати вказівки, наведені в ISO/IEC 27035- 1:2016, відповідно до свого типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Це також стосується зовнішніх організацій, які надають послуги з управління інцидентами інформаційної безпеки.

– ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT) – ISO/IEC 27035-2:2016 надає рекомендації щодо планування та підготовки до реагування на інциденти. Рекомендації базуються на етапі «Планування та підготовка» та етапі «Здобуті уроки» моделі «Фази управління інцидентами інформаційної безпеки», представленої в ISO/IEC 27035-1. Основні моменти на етапі «Планування та підготовка» включають наступне: політика управління інцидентами інформаційної безпеки та зобов'язання вищого керівництва політики інформаційної безпеки, включаючи ті, що стосуються управління ризиками, оновлені як на корпоративному рівні, так і на рівні системи, сервісу та мережі план управління інцидентами інформаційної безпеки створення групи реагування на інциденти (IRT) встановлювати стосунки та зв'язки з внутрішніми та зовнішніми організаціями технічне та інше забезпечення (включаючи організаційне та операційне) інструктажі та тренінги з управління інцидентами інформаційної безпеки тестування плану управління інцидентами інформаційної безпеки. Принципи, наведені в цій частині ISO/IEC 27035, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати вказівки, надані в цій частині ISO/IEC 27035, відповідно до їх типу, розміру та характеру

бізнесу щодо ситуації ризику інформаційної безпеки. Ця частина ISO/IEC 27035 також застосовується до зовнішніх організацій, що надають послуги з управління інцидентами інформаційної безпеки.

– ISO/IEC 27035-3:2020. Інформаційна технологія. Управління інцидентами інформаційної безпеки. Частина 3. Настанови щодо операцій реагування на інциденти ІКТ – У цьому документі містяться вказівки щодо реагування на інциденти інформаційної безпеки в операціях безпеки ІКТ. Цей документ робить це, по-перше, охоплюючи операційні аспекти операцій безпеки ІКТ з точки зору людей, процесів і технологій. Далі він зосереджується на реагуванні на інциденти інформаційної безпеки в операціях безпеки ІКТ, включаючи виявлення інцидентів інформаційної безпеки, звітування, сортування, аналіз, реагування, стримування, викорінення, відновлення та завершення. Цей документ не стосується операцій реагування на інциденти, не пов'язані з ІКТ, як-от втрата паперових документів. Цей документ базується на фазі «Виявлення та звітування», фазі «Оцінка та прийняття рішення» та фазі
«Відповіді» моделі «Фази управління інцидентами інформаційної безпеки», представленої в ISO/IEC 27035-1:2016. Принципи, наведені в цьому документі, є загальними та призначені для застосування в усіх організаціях, незалежно від типу, розміру чи природи. Організації можуть коригувати положення, наведені в цьому документі, відповідно до свого типу, розміру та характеру бізнесу щодо ситуації ризику інформаційної безпеки. Цей документ також стосується зовнішніх організацій, які надають послуги з управління інцидентами інформаційної безпеки.

– ISO/IEC CD 27035-4. Інформаційні технології. Управління інцидентами інформаційної безпеки. Частина 4. Координація – В стадії розробки

– **ДСТУ ISO/IEC 27036:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. – складається з 4 частин:**

– ДСТУ ISO/IEC 27036-1:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах із постачальниками. Частина 1. Огляд та поняття (ISO/IEC 27036-1:2014, IDT) – Цей документ є вступною частиною ISO/IEC 27036.

Він містить огляд настанов, спрямованих на допомогу організаціям у захисті їх інформації та інформаційних систем у контексті відносин з постачальниками. Він також представляє концепції, які детально

описані в інших частинах ISO/IEC 27036. Цей документ розглядає точки зору як покупців, так і постачальників.

– ДСТУ ISO/IEC 27036-2:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 2. Вимоги (ISO/IEC 27036-2:2014, IDT) – Цей документ визначає фундаментальні вимоги інформаційної безпеки для визначення, впровадження, експлуатації, моніторингу, перегляду, підтримки та покращення відносин постачальника та покупця. Ці вимоги охоплюють будь-яку закупівлю та постачання продуктів і послуг, таких як виробництво або складання, закупівля бізнес-процесів, програмних і апаратних компонентів, закупівля процесу знань, створення- експлуатація-передача та послуги хмарних обчислень. Цей документ застосовується до всіх організацій, незалежно від типу, розміру та характеру. Щоб відповідати вимогам, очікується, що організація запровадила всередині ряд базових процесів або активно планує це зробити. Ці процеси включають, але не обмежуються: управління бізнесом, управління ризиками, управління операційними й людськими ресурсами та інформаційна безпека.

– ДСТУ ISO/IEC 27036-3:2017 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 3. Настанови щодо безпеки ланцюга постачання інформаційних та комунікаційних технологій (ISO/IEC 27036-3:2013, IDT) – ISO/IEC 27036-3:2013 надає покупцям продуктів і послуг і постачальникам у ланцюзі постачання інформаційно-комунікаційних технологій (ІКТ) настанови щодо: отримання видимості та управління ризиками інформаційної безпеки, спричиненими фізично розосередженими та багаторівневими ланцюгами постачання ІКТ; реагування на ризики, пов’язані з глобальним ланцюгом постачання ІКТ-продуктів і послуг, які можуть мати вплив на інформаційну безпеку організацій, які використовують ці продукти та послуги. Ці ризики можуть бути пов’язані як з організаційними, так і з технічними аспектами (наприклад, введення шкідливого коду або наявність підроблених продуктів інформаційних технологій (IT); інтеграція процесів і практик інформаційної безпеки в процеси життєвого циклу системи та

програмного забезпечення, описані в ISO/IEC 15288 та ISO/IEC 12207, одночасно підтримуючи засоби контролю інформаційної безпеки, описані в ISO/IEC 27002. ISO/IEC 27036-3:2013 не включає питання управління безперервністю бізнесу/відмовостійкості, пов'язані з ланцюгом постачання ІКТ. ISO/IEC 27031 стосується безперервності бізнесу.

– ДСТУ ISO/IEC 27036-4:2018 Інформаційні технології. Методи захисту. Інформаційна безпека у відносинах з постачальниками. Частина 4. Настанова щодо безпеки хмарних послуг (ISO/IEC 27036-4:2016, IDT) – ISO/IEC 27036- 4:2016 надає клієнтам хмарних послуг і постачальникам хмарних послуг рекомендації щодо отримання інформації про ризики інформаційної безпеки, пов'язані з використанням хмарних служб, і ефективне управління цими ризиками, а також реагування на ризики, характерні для придбання або надання хмарних послуг, які можуть мати вплив на інформаційну безпеку організацій, які використовують ці служби. ISO/IEC 27036-4:2016 не включає питання управління безперервністю бізнесу/відмовостійкості, пов'язані з хмарною службою. ISO/IEC 27031 стосується безперервності бізнесу. ISO/IEC 27036- 4:2016 не надає вказівок щодо того, як постачальник хмарних послуг повинен запроваджувати, керувати та керувати інформаційною безпекою. Інструкції щодо них можна знайти в ISO/IEC 27002 та ISO/IEC 27017. Сфера застосування ISO/IEC 27036-4:2016 полягає у визначенні настанов, що підтримують впровадження управління безпекою інформації для використання хмарних служб.

– **ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT) –** Цей стандарт надає настанови для специфічної діяльності з оброблення потенційних цифрових доказів, такими процесами є: ідентифікація, збирання, здобуття та збереження потенційних цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів – прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть буті корисними на стадії аналізування потенційних

цифрових доказів. Цей стандарт також спрямовано на інформування осіб, які приймають рішення, та тих, кому потрібно визначати надійність потенційних цифрових доказів, що були їм надані. Він прийнятний для організацій, яким необхідно захищати, аналізувати та презентувати потенційні цифрові докази. Він важливий для поліцейських підрозділів, які формують та запроваджують процедури щодо цифрових доказів, часто як частину доказів більшого об'єму. Потенційні цифрові докази, розглянуті в цьому стандарті, можуть мати походження з різних типів цифрових пристроїв, мереж, баз даних тощо. Вони стосуються даних, які вже є в цифровому форматі. Цей стандарт не намагається охопити перетворення аналогових даних у цифровий формат. Завдяки недовговічності цифрових доказів потрібно мати прийнятну методологію для гарантування цілісності та автентичності потенційних цифрових доказів. Цей стандарт не вимагає обов'язкового використання винятковых інструментів або методів. Ключовим компонентом, який забезпечує довіру в розслідуваннях, є методологія, яку застосовують протягом цього процесу, та особи, що мають кваліфікацію для виконання завдань, визначених цією методологією. Цей стандарт не стосується методології для законодавчих та дисциплінарних судових процесів, а також інших пов'язаних діяльностей під час оброблення потенційних цифрових доказів, які знаходяться поза межами сфери ідентифікації, збирання, здобуття та збереження. Запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Він не повинен заміняти специфічні законодавчі вимоги будь-якої юрисдикції. Фактично, він може слугувати практичною настановою для DEFR або DES у дослідженнях, які охоплюють потенційні цифрові докази. Він не впливає на аналізування цифрових доказів та не замінює специфічних юридичних вимог, що стосуються таких питань, як визнання доказів, доказова вага, значущість та інші юридично контрольовані обмеження використання потенційних цифрових доказів у судах. Цей стандарт може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями. Для підтримання цілісності цифрових доказів користувачам цього стандарту потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних законодавчих вимог юрисдикції для доказів. Хоча цей стандарт не охоплює судової готовності, відповідна судова готовність може бути значною мірою

підтримана процесами ідентифікації, збирання, здобуття та збереження цифрових доказів. Судова готовність – це досягнення відповідного рівня здатності організації для спроможності ідентифікації, збирання, здобуття, збереження, захисту та аналізування цифрових доказів. Незважаючи на те, що процеси та діяльності, описані в цьому стандарті, є в основному реактивними заходами, використовуваними в розслідуваннях інциденту після того, як він вже трапився, судова готовність є проективним процесом спроби планування процесу дослідження інциденту. Цей стандарт відповідає ISO/IEC 27001 та ISO/IEC 27002, зокрема вимогам заходів щодо безпеки стосовно потенційних цифрових доказів за допомогою надання додаткової настанови щодо запровадження. Крім того, цей стандарт має застосування в контексті, незалежному від ISO/IEC 27001 та ISO/IEC 27002. Цей стандарт потрібно розглядати разом з іншими стандартами, пов'язаними з цифровими доказами та розслідуваннями інцидентів інформаційної безпеки. Цей стандарт надає настанови для специфічної діяльності з оброблення цифрових доказів, а саме: ідентифікації, збирання, здобуття та збереження цифрових доказів, що можуть мати доказове значення. Цей стандарт надає настанови для фахівців стосовно звичайних випадків, які трапляються в процесі оброблення цифрових доказів,та допомагає організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями. Цей стандарт надає настанови для таких пристроїв та/або функцій, використовуваних за різних обставин: Носій для зберігання цифрових даних, використовуваний у стандартних комп'ютерах, подібний жорстким дискам, гнучким дискам, оптичним і магнітооптичним дискам, цифровим пристроям з подібними функцпми; Мобільні телефони, Персональні цифрові помічники (PDAs), Персональні електронні прилади (PEDs), карти пам'яті; Мобільні навігаційні системи; Цифрові фото- та відеокамери (зокрема CCTV); Стандартний комп'ютер з мережевими з'єднаннями; Мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах; Прилади з функціями, подібними наведеним вище.

– **ДСТУ ISO/IEC 27038:2018 Інформаційні технології. Методи захисту. Специфікація цифрового редагування (ISO/IEC 27038:2014, IDT) –** ISO/IEC 27038:2014 визначає характеристики методів виконання цифрового

редагування цифрових документів. Він також визначає вимоги до засобів редагування програмного забезпечення та методів перевірки надійності цифрового редагування. ISO/IEC 27038:2014 не включає редагування інформації з баз даних.

– **ДСТУ ISO/IEC 27039:2017 Інформаційні технології. Методи захисту. Вибирання, розгортання та експлуатування систем виявлення та запобігання вторгненням (IDPS) (ISO/IEC 27039:2015, IDT) –** ISO/IEC 27039:2015 надає рекомендації для допомоги організаціям у підготовці до розгортання систем виявлення та запобігання вторгненням (IDPS). Зокрема, йдеться про вибір, розгортання та роботу IDPS. Він також містить довідкову інформацію, на основі якої походять ці рекомендації.

– **ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040:2015, IDT) –** ISO/IEC 27040:2015 надає детальні технічні вказівки щодо того, як організації можуть визначити відповідний рівень зниження ризику за допомогою перевіреного та послідовного підходу до планування, проектування, документування та реалізації безпеки зберігання даних. Безпека зберігання стосується захисту (безпеки) інформації, де вона зберігається, і безпеки інформації, що передається через канали зв'язку, пов'язані зі зберіганням. Безпека зберігання включає безпеку пристроїв і носіїв, безпеку дій з управління, пов'язаних із пристроями та носіями, безпеку програм і служб, а також безпеку, актуальну для кінцевих користувачів протягом усього терміну служби пристроїв і носіїв і після завершення використання. Безпека зберігання актуальна для всіх, хто бере участь у володінні, експлуатації або використанні пристроїв зберігання даних, засобів масової інформації та мереж. Це включає керівників вищої ланки, покупців продуктів і послуг зберігання та інших нетехнічних менеджерів або користувачів, на додаток до менеджерів і адміністраторів, які мають конкретні обов'язки за інформаційну безпеку чи безпеку зберігання, роботу сховища або які відповідають за загальну безпеку організації розробка програми та політики безпеки. Це також актуально для всіх, хто бере участь у плануванні, проектуванні та реалізації архітектурних аспектів безпеки мережі зберігання. ISO/IEC 27040:2015 містить огляд концепцій безпеки зберігання та відповідних визначень. Він містить вказівки щодо загроз, дизайну та аспектів

контролю, пов’язаних із типовими сценаріями зберігання та областями технологій зберігання. Крім того, він надає посилання на інші міжнародні стандарти та технічні звіти, які стосуються існуючих практик і методів, які можуть бути застосовані для безпеки зберігання.

– ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Посібник із забезпечення прийнятності та адекватності методів розслідування (ISO/IEC 27041:2015, IDT) – ISO/IEC 27041:2015 надає вказівки щодо механізмів забезпечення того, що методи та процеси, які використовуються під час розслідування інцидентів інформаційної безпеки, «відповідають меті». Він інкапсулює найкращі практики щодо визначення вимог, опису методів і надання доказів того, що реалізації методів можна показати, що задовольняють вимоги. Він включає в себе розгляд того, як тестування постачальників і третіх сторін можна використовувати для сприяння цьому процесу гарантії. Цей документ має на меті: надавати вказівки щодо збору й аналізу функціональних і нефункціональних вимог, пов’язаних із розслідуванням інцидентів

інформаційної безпеки (IS); давати вказівки щодо використання валідації як засобу забезпечення придатності процесів, залучених до розслідування; надати вказівки щодо оцінювання необхідних рівнів валідації та доказів, необхідних для перевірки; надати вказівки щодо того, як зовнішнє тестування та документацію можна включити в процес валідації.

– ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT) – ISO/IEC 27042:2015 містить настанови щодо аналізу та інтерпретації цифрових доказів у спосіб, який розглядає питання безперервності, валідності, відтворюваності та повторюваності. Він інкапсулює найкращі практики для вибору, проектування та реалізації аналітичних процесів і запису достатньої інформації, щоб такі процеси могли бути піддані незалежному контролю, коли це необхідно. У ньому містяться вказівки щодо належних механізмів демонстрації кваліфікації та компетентності слідчої групи. Аналіз та інтерпретація цифрових доказів може бути складним процесом. За деяких обставин може бути застосовано кілька методів, і члени слідчої групи повинні будуть обґрунтувати свій вибір

певного процесу та показати, наскільки він еквівалентний іншому процесу, який використовують інші дослідники. За інших обставин дослідникам, можливо, доведеться розробити нові методи дослідження цифрових доказів, які раніше не розглядалися, і вони повинні мати можливість показати, що отриманий метод «відповідає меті». Застосування певного методу може вплинути на інтерпретацію цифрових доказів, оброблених цим методом. Наявні цифрові докази можуть впливати на вибір методів для подальшого аналізу цифрових доказів, які вже були отримані. ISO/IEC 27042:2015 забезпечує загальну структуру для аналітичних та інтерпретаційних елементів обробки інцидентів безпеки інформаційних систем, які можуть бути використані для допомоги у впровадженні нових методів і забезпечують мінімальний загальний стандарт для цифрових доказів, отриманих у результаті такої діяльності.

– **ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (ISO/IEC 27043:2015, IDT) –** ISO/IEC 27043:2015 надає вказівки на основі ідеалізованих моделей для загальних процесів розслідування інцидентів у різних сценаріях розслідування інцидентів із використанням цифрових доказів. Це включає процеси від підготовки до інциденту до закриття розслідування, а також будь-які загальні поради та застереження щодо таких процесів. Інструкції описують процеси та принципи, застосовні до різних типів розслідувань, включаючи, але не обмежуючись, несанкціонований доступ, пошкодження даних, збої системи або корпоративні порушення інформаційної безпеки, а також будь-які інші цифрові розслідування. Підсумовуючи, цей міжнародний стандарт надає загальний огляд усіх принципів і процесів розслідування інцидентів, не вказуючи конкретних деталей у рамках кожного з принципів і процесів розслідування, охоплених цим міжнародним стандартом. Багато інших відповідних міжнародних стандартів, де

є посилання в цьому міжнародному стандарті, надають більш детальний зміст конкретних принципів і процесів розслідування.

– **ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. – складається з 4 частин:**

– ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття (ISO/IEC 27050-1:2016, IDT) – Електронне відкриття – це процес виявлення відповідної інформації, що зберігається в електронному вигляді (ESI) або даних, однією чи декількома сторонами, залученими до розслідування, судового розгляду чи подібного процесу. Цей документ містить огляд електронного відкриття. Крім того, у ньому даються визначення пов'язаних термінів і описуються концепції, включаючи, але не обмежуючись цим, ідентифікацію, збереження, збір, обробку, перегляд, аналіз і виробництво ESI. Цей документ також визначає інші відповідні стандарти (наприклад, ISO/IEC 27037) і те, як вони стосуються та взаємодіють із діяльністю з електронних відкриттів. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.

– ISO/IEC 27050-2:2018. Інформаційна технологія. Електронне відкриття. Частина 2. Керівництво з управління електронним відкриттям – У цьому документі містяться вказівки для технічного та нетехнічного персоналу на вищому рівні керівництва в організації, включно з тими, хто відповідає за дотримання законодавчих і нормативних вимог, а також галузевих стандартів. Він описує, як такий персонал може ідентифікувати ризики, пов'язані з електронним відкриттям, і взяти на себе відповідальність за них, встановити політику та досягти відповідності відповідним зовнішнім і внутрішнім вимогам. Він також пропонує, як виробити такі політики у формі, яка може інформувати процес управління. Крім того, він містить вказівки щодо того, як запроваджувати та контролювати електронні відкриття відповідно до політики.

– ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення (ISO/IEC 27050-3:2017, IDT) – У цьому документі містяться вимоги та рекомендації щодо діяльності з електронного відкриття, включаючи, але не обмежуючись, ідентифікацію, збереження, збір, обробку, перегляд, аналіз і створення електронно збереженої інформації (ESI). Крім того, цей документ визначає відповідні заходи, які

охоплюють життєвий цикл ESI від його початкового створення до остаточної ліквідації. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки. Важливо зазначити, що користувач повинен знати про будь-які застосовні вимоги юрисдикції.

– ISO/IEC 27050-4:2021. Інформаційні технології – Електронне відкриття – Частина 4: Технічна готовність – У цьому документі містяться вказівки щодо того, як організація може планувати, готуватися до та впроваджувати електронне відкриття з точки зору як технологій, так і процесів. Цей документ містить вказівки щодо профілактичних заходів, які можуть

допомогти забезпечити ефективне та відповідне електронне відкриття та процеси. Цей документ стосується як нетехнічного, так і технічного персоналу, який бере участь у деяких або всіх видах електронної техніки.

– ISO/IEC 27099:2022. Інформаційні технології – Інфраструктура відкритих ключів – Практика та рамки політики – У цьому документі встановлюється система вимог до управління інформаційною безпекою для постачальників довірчих послуг інфраструктури відкритих ключів (PKI) через політику сертифікації, положення про практику сертифікації та, де це можливо, їх внутрішню підтримку системою управління інформаційною безпекою (СУІБ) (ISMS). Структура вимог включає оцінку та обробку ризиків інформаційної безпеки, адаптованих для задоволення узгоджених вимог користувачів до послуг, як зазначено в політиці сертифікатів. Цей документ також призначений для того, щоб допомогти постачальникам послуг довіри підтримувати кілька політик сертифікатів. У цьому документі розглядається життєвий цикл сертифікатів відкритих ключів, які використовуються для цифрових підписів, автентифікації або встановлення ключа для шифрування даних. У ньому не йдеться про методи автентифікації, вимоги щодо неспростування або протоколи управління ключами, засновані на використанні сертифікатів відкритих ключів. Для цілей цього документа термін «сертифікат» стосується сертифікатів відкритих ключів. Цей документ не застосовується до сертифікатів атрибутів. У цьому документі використовуються концепції та вимоги СУІБ, як визначено в сімействі стандартів ISO/IEC 27000. Він використовує кодекс

практики для контролю інформаційної безпеки, як визначено в ISO/IEC 27002. Конкретні вимоги до PKI (наприклад, вміст сертифіката, перевірка ідентичності, обробка відкликання сертифіката) не розглядаються безпосередньо СУІБ, як визначено в ISO/IEC 27001. Використання ISMS або еквівалента адаптовано до застосування вимог до служби PKI, зазначених у політиці сертифікатів, як описано в цьому документі. Постачальник довірчих послуг PKI – це спеціальний клас довірчих послуг для використання сертифікатів відкритих ключів. Цей документ розрізняє системи PKI, які використовуються в закритому, відкритому та договірному середовищах. Цей документ призначений для полегшення впровадження операційного, базового контролю та практики в договірному середовищі. Хоча цей документ зосереджений на договірному середовищі, застосування цього документа до відкритих чи закритих середовищ не виключається.