ETSI GS ISI 007 V1.1.1 (2018-12)

/лого/

Показники інформаційної безпеки (ISI);

Вказівки щодо побудови та експлуатації захищеного операційного центру безпеки (SOC)

Застереження

Цей документ був підготовлений і схвалений групою галузевих специфікацій (ISG) ETSI за показниками інформаційної безпеки (ISI) і представляє думки тих членів, які брали участь в цій групі ISG.

Це не обов'язково відображає погляди всіх членів ETSI.

Посилання

DGS/ISI-007

Ключові слова

кіберзахист, безпека

ETSI

650 Route des Lucioles
F-06921 Софія Антиполіс Седекс - ФРАНЦІЯ

Тел .: +33 4 92 94 42 00 Факс: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Prefecture de Grasse (06) N° 7803/88

Важливе повідомлення

Цей документ можна завантажити з:
http://www.etsi.org/standards-search

Цей документ може бути наданий в електронних версіях та/або в друкованому вигляді. Зміст будь-якого електронної та/або друкованої версії цього документа не можуть бути змінені без попереднього письмового дозволу ETSI. У разі будь-яких існуючих або передбачуваних відмінностей у змісті між такими версіями та/або у пресі, єдиним переважаючим документом є друкована версія Портативного формату документа (PDF), що зберігається на певному мережевому диску в Секретаріаті ETSI.

Користувачі цього документа повинні знати, що документ може піддаватися перегляду або зміні статусу.
Інформація про поточний стан цього та інших документів ETSI доступна за адресою
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

Якщо ви виявите помилки в цьому документі, надішліть свій коментар одній із таких служб:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Повідомлення про авторські права

Зміст

Право інтелектуальної власності

Основні патенти

Права інтелектуальної власності, необхідні або потенційно необхідні для нормативних результатів, могли бути оголошені ETSI. Інформація стосується цих основних прав інтелектуальної власності, якщо такі є, є загальнодоступним для **членів ETSI та не членів** , і їх можна знайти у ETSI SR 000 314: *"Права інтелектуальної власності (ПІВ); Основні або потенційно суттєві ПІВ, повідомлені ETSI у щодо стандартів ETSI "* , який можна отримати в Секретаріаті ETSI. Останні оновлення доступні на сервері ETSI (https://ipr.etsi.org/).

Відповідно до Політики щодо прав інтелектуальної власності ETSI, ETSI не проводила жодного розслідування, включаючи пошуки прав інтелектуальної власності.
Не може бути надано жодних гарантій щодо існування інших ПІВ, не згаданих в ETSI SR 000 314 (або оновленнях на веб- сервері ETSI), які є, або можуть бути, або можуть стати суттєвими для цього документа.

Торгові марки

Цей документ може включати торгові марки та/або торгові назви, які затверджуються та/або реєструються їх власниками.ETSI не вимагає права власності на них, за винятком тих, які вказані як власність ETSI, і не передає право на використання або відтворення будь-якої торгової марки та/або торгової назви. Згадування цих торгових марок у цьому документі
не є підтвердженням ETSI продуктів, послуг чи організацій, пов'язаних із цими торговими марками.

Передмова

Ця групова специфікація (GS) була підготовлена групою галузевих специфікацій ETSI (ISG)
За показниками інформаційної безпеки (ISI).

Цей документ входить до серії 9 специфікацій ISI 00x. Ці 9 специфікацій є наступними (див Рисунок 1 узагальнює різні концепції, що беруть участь у виявленні подій та взаємодії між усіма частинами):

- ETSI GS ISI 001-1 [1], що стосується (разом з відповідним керівництвом ETSI GS ISI 001-2 [2])показників інформаційної безпеки, призначених для вимірювання застосування та ефективності профілактичних заходів.
- ETSI GS ISI 002 [3], що стосується основної моделі класифікації подій та пов'язаної з нею таксономії.
- ETSI GS ISI 003 [i.1], що стосується ключового питання оцінки рівня зрілості організації щодо загального виявлення подій (технологія/процес/люди) для зважування результатів виявлення подій.
- ETSI GS ISI 004 [i.2], що стосується демонстрації на прикладах, як виробляти показники та як виявляти пов'язані події за допомогою різних засобів та методів (з класифікацією основних категорій випадків/симптомів використання).
- ETSI GS ISI 005 [i.3] , що стосується способів створення подій безпеки та перевірки ефективності існуючих засобів виявлення в організації (для основних типів подій), що є більш докладним і більш індивідуальним підходом, ніж ETSI GS ISI 003 [i.1], і тому може доповнювати його.
- ETSI GS ISI 006 [i.4], що стосується іншої інженерної частини серії, доповнюючи ETSI GS ISI 004 [i.2] і зосереджуючись на розробці мови кібербезпеки для моделювання інформації про загрози та забезпечення
сумісності засобів виявлення.
- **ETSI GS ISI 007 (цей документ), що стосується всеосяжних керівних принципів щодо створення та експлуатації
захищеного SOC, особливо щодо архітектурних аспектів, в контексті, коли SOC часто є реальними вишками управління в організаціях.**
- ETSI GS ISI 008 [i.5], що стосується і пояснює, як зробити SIEM цілісним підходом, який дійсно інтегрований в загальний загальноорганізаційний, а не тільки IT-орієнтований кіберзахист.

Рисунок 1 узагальнює різні концепції, пов'язані з виявленням подій та взаємодією між специфікаціями.

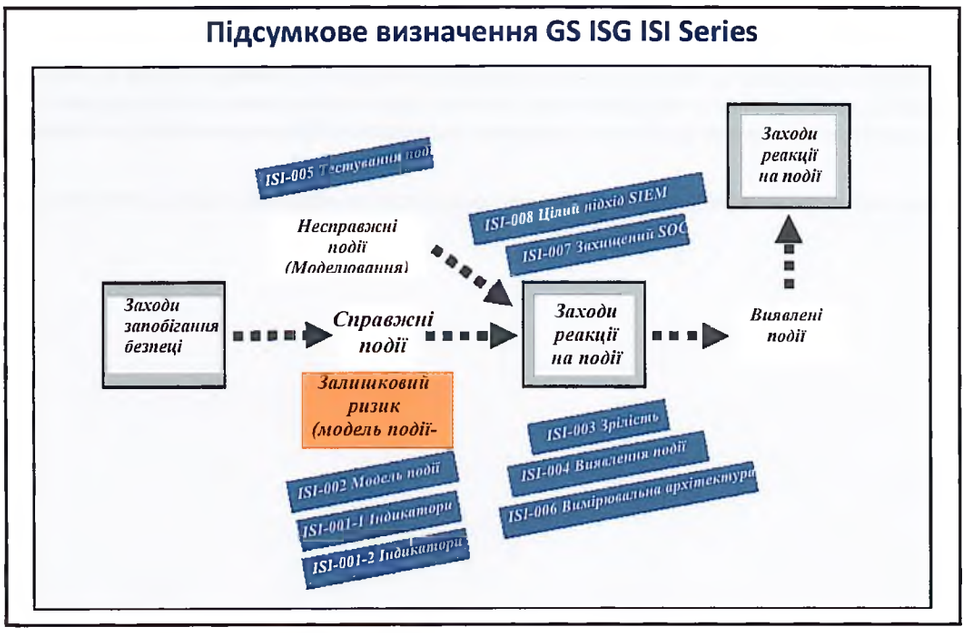

Рисунок 1: Позиціонування 9 GS ISI проти 3 основних заходів безпеки

Термінологія модальних дієслів

У цьому документі " **повинен**", " **не повинен**", " **повинен**", "**не повинен**", "**слід**", " **не слід**", "**буде**", "**не буде**", "**може**" і "**не можна**" потрібно тлумачити, як описано у пункті 3.2 Правил складання ETSI (словесні форми для вираження положення).

" **бути зобов'язаним**" і "**не бути зобов'язаним**" **НЕ** дозволяються в результатах ETSI, крім випадків, коли вони використовуються у прямому цитуванні.

Вступ

Зростаючий взаємозв'язок мереж та вимоги до дематеріалізації залишають інформаційні системи вразливими до кібератак. Точки з'єднання з зовнішніми мережами і, зокрема, з Інтернетом -це всі точки доступу, які зовнішній зловмисник може спробувати використовувати для входу і перебування в інформаційній системі з метою крадіжки, зміни або знищення її інформаційних активів. І боротьба з часто дуже небезпечними внутрішніми загрозами також необхідна.

Крім того, нові нормативні акти та закони роблять дедалі більш обов'язковим виявлення та звітування органів безпеки інцидентів. Це, зокрема, стосується **Директиви про мережеву та інформаційну безпеку (NIS) [** i.10 **]** , для якої цей документ може стати міцною основою для реалізації Статей 14 та 16. З цією метою в ньому розглядається захищений спосіб використання інформації про кіберзагрози для виявлення інцидентів безпеки, що є важливим питанням, яке має бути розглянуто в Директиві NIS.

Використання систем виявлення інцидентів безпеки сприяє захисту інформаційних систем від загроз кібератаки. Людські, технічні та організаційні ресурси можуть бути зосереджені в оперативному центрі кібербезпеки (CyberSOC або SOC), як правило, який є призначеним для виявлення інцидентів безпеки та реагування на них. В залежності від завдань, потреб і ресурсів об'єкта введення в експлуатацію цей центр може бути внутрішнім, виділеним на аутсорсинг або навіть поділитися. В останньому випадку об'єднання ресурсів може мати позитивні наслідки, наприклад, обмін інформацією про правила загрози та виявлення.

Коли надання послуги виявлення відповідає найсучаснішим технологіям та точно адаптується до потреб суб'єкта введення в експлуатацію, це допомагає запобігти серйозним інцидентам безпеки (шляхом виявлення вразливостей або відповідність - див. ETSI GS ISI 001-1 [1] або ETSI GS ISI 002 [3]) або, якщо такі випадки трапляються, обмежити наслідки, даючи можливість вжити швидких санаційних заходів, які можуть бути здійснені введенням в експлуатацію групи реагування на інциденти безпеки (розташовані або в CERT, або в самій SOC).

Однак концентрація та об'єднання можливостей виявлення роблять центр операцій з кібербезпеки головним мішень для зловмисників. Тому особливу увагу слід приділяти захисту своєї інформаційної системи.

Метою цього документа є надати керівні принципи щодо побудови та експлуатації **захищеного SOC** за допомогою списку функціональних, організаційних та технічних вимог. Крім того, воно охоплює **виявлення інцидентів у галузі безпеки** аж до інциденту звітування перед суб'єктом **введення в експлуатацію без введення поля реагування на аварію**.

Він також може використовуватися в інтересах прийняття найкращих практик незалежно від будь-якої нормативної бази.

1 Сфера дії

Цей документ охоплює 2 типи послуг виявлення аварійних ситуацій: внутрішню та зовнішню.

Вимоги можуть бути реалізовані на 2 різних рівнях: базовий рівень (часткова відповідність), вдосконалений рівень (повна відповідність).

Цей документ структурований наступним чином (після пунктів 2 та 3, відповідно присвячених посиланням та термінам, символи та скорочення):

- **Пункт 4** описує діяльність, до якої належить даний документ.
- **У пункті 5** представлені вимоги, що застосовуються до постачальників послуг (внутрішніх чи зовнішніх), що працюють з SOC.

ПРИМІТКА: Ці вимоги, позначені малими літерами (a, b, c тощо), випливають із вимог подібного довідкова система, опублікована ANSSI [i.12], щоб їх маркування відповідало їм, тобто відсутні листи відповідають відхиленим або невідповідним вимогам.

- **У Додатку А** представлені завдання та навички, які очікуються від працівників постачальника послуг.
- **У Додатку В** представлені рекомендації для об'єктів, що вводять в експлуатацію, під час укладання контрактів з охоронними

провайдерами виявлення інцидентів.

- **Додаток С** визначає базовий та частковий рівень реалізації вимог.

2 Посилання

2.1 Нормативні посилання

Посилання є або конкретними (ідентифікованими за датою публікації та/або номером видання або номером версії) або
неконкретними. Для конкретних посилань застосовується лише цитована версія. Для неконкретних посилань - остання версія
документу, на який посилаються (включаючи будь-які поправки).

Документи, на які посилаються, які не є загальнодоступними в очікуваному місці, можна знайти на https://docbox.etsi.org/Reference/ .

ПРИМІТКА: Хоча будь-які гіперпосилання, включені до цього пункту, були дійсними на момент публікації, ETSI не може гарантувати їх тривалість дії.

Наступні документи, на які посилаються, необхідні для застосування цього документа.

[1] ETSI GS ISI 001-1: "Індикатори інформаційної безпеки (ISI); Індикатори (INC); Частина 1: Повний набір
оперативних показників, які організації повинні використовувати для оцінки своєї безпеки".

[2] ETSI GS ISI 001-2: "Індикатори інформаційної безпеки (ISI); Індикатори (INC); Частина 2: Посібник з
вибору операційних показників на основі повного набору, наведеного в частині 1".

[3] ETSI GS ISI 002: "Індикатори інформаційної безпеки (ISI); Модель події Модель класифікації подій безпеки та таксономія".

[4] ISO/IEC 27002: 2013: "Інформаційні технології - Методи безпеки - Звід практики для засобів управління інформаційною безпекою".

2.2 Інформативні посилання

Посилання є або конкретними (ідентифікованими за датою публікації та/або номером видання або номером версії) або
неконкретними. Для конкретних посилань застосовується лише цитована версія. Для неконкретних посилань - остання версія
документу, на який посилаються (включаючи будь-які поправки).

ПРИМІТКА: Хоча будь-які гіперпосилання, включені до цього пункту, були дійсними на момент публікації, ETSI не може гарантувати їх тривалість дії.

Наступні посилані документи не є необхідними для застосування цього документа, але вони допомагають користувачу щодо певної предметної області.

[i.[1] ETSI GS ISI 003: "Індикатори інформаційної безпеки (ISI); Ключові показники безпеки роботи (KPSI) для оцінки зрілості виявлення подій безпеки".

[i.[2] ETSI GS ISI 004: "Індикатори інформаційної безпеки (ISI); Настанови щодо реалізації виявлення подій".

[i.[3] ETSI GS ISI 005: "Індикатори інформаційної безпеки (ISI); Настанови щодо тестування виявлення подій безпеки та оцінка ефективності виявлення".

[i.[4] ETSI GS ISI 006: "Індикатори інформаційної безпеки (ISI); Вимірювання та відповідність ISI Архітектура управління подіями для кібербезпеки та безпеки

[i.[5] ETSI GS ISI 008: "Індикатори інформаційної безпеки (ISI); Опис загальної організації - широкий підхід до інформації щодо безпеки та управління подіями (SIEM)".

[i.[6] ISO 27035-1: 2016: "Інформаційні технології - Методи безпеки - Інцидент інформаційної безпеки управління - Частина 1: Принципи управління інцидентами".

[i.[7] ISO 27035-2: 2016: "Інформаційні технології - Методи безпеки - Інцидент управління інформаційною безпекою - Частина 2: Настанови щодо планування та підготовки до реагування на інциденти".

[i.[8] ANSSI: "Guide d'hygiène informatique ".

ПРИМІТКА: Доступно за посиланням https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/ для оновленої версії.

[i.[9] Центр кібербезпеки в Інтернеті: "Критичний контроль безпеки для ефективного кіберзахисту Версія 7".

ПРИМІТКА: Доступно за адресою https://www.cisecurity.org/critical-controls.cfm .

[i.[10] Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року щодо заходів щодо високого загального рівня безпеки мережевих та інформаційних систем по всьому Союзу.

ПРИМІТКА: Доступно за посиланням https://eur-lex.europa.eu/eli/dir/2016/1148/oj .

[i.[11] ISO 27000: "Інформаційні технології - Методи безпеки - Управління системами інформаційної безпеки - Огляд та словниковий запас".

[i.[12] ANSSI (Французьке агентство мереж та інформаційної безпеки): "Постачальники послуг виявлення інцидентів у сфері безпеки - Довідковий документ щодо вимог".

ПРИМІТКА: Доступно за адресою https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v1.0_en.pdf .

3 Визначення термінів, символів та скорочень

3.1 Терміни

Для цілей цього документа застосовуються терміни, наведені в ETSI GS ISI 001-2 [2], та наступне:

ПРИМІТКА. Вони переважно взяті зі стандартів ISO 27000 [i.11] та ISO 27035 [i.6] та [i.7].

адміністратор: член служби виявлення з привілейованими правами, що дозволяє їм забезпечити безперебійну роботу
пристроїв служби виявлення

джерело збору: обладнання в інформаційній системі, яке генерує події, пов'язані з безпекою інформації

колектор: пристрій, що дозволяє централізувати події безпеки, що походять з різних джерел збору

ПРИКЛАД: Сервер Syslog, колектор рішень SIEM.

ПРИМІТКА: У контексті цієї послуги місцеві колектори - це колектори, введені в експлуатацію в об’єкті , а центральні колектори - це колектори, що використовуються для централізації подій і розташовані в
інформаційній системі постачальника послуг.

суб'єкт введення в експлуатацію: суб'єкт, який використовує службу виявлення аварійних ситуацій

контекст інциденту безпеки: подія, пов'язана з інцидентом безпеки, разом із усією аналізованою та отриманою інформацією
під час його кваліфікації

ПРИКЛАД: Звіт(и) про кваліфікаційний аналіз.

правило виявлення: перелік технічних елементів, що дозволяють ідентифікувати інцидент на основі однієї або декількох подій

ПРИМІТКА: Правило виявлення може бути сформовано одним або кількома маркерами, одним або кількома підписами або поведінковим правилом на основі ненормальної поведінки. Правило виявлення може походити від постачальника інструментів технічного аналізу, що використовуються для служби виявлення, сам постачальник послуг (моніторинг нових інцидентів, застосовуване правило для іншого суб'єкта введення в експлуатацію за його згодою тощо), партнер, спеціалізований постачальник або можебути створено спеціально для об'єкта введення в експлуатацію.

ефективність: рівень досягнення запланованих заходів та очікувані результати

інформаційна система: організований набір ресурсів (апаратне забезпечення, програмне забезпечення, персонал, дані та процедури) для обробки і передача інформації

розслідування: процес, призначений для збору та аналізу всіх технічних, функціональних або організаційних елементів інформаційної системи для того, щоб кваліфікувати підозрілу ситуацію як інцидент безпеки та зрозуміти набір вторгнень і масштаб інциденту безпеки в інформаційній системі

оператор: член служби виявлення, відповідальний за обслуговування послуги, тобто виконання завдань, пов'язаних з виявленням створення послуги від імені суб'єкта введення в експлуатацію

зонд або система виявлення: технічний пристрій, призначений для виявлення ненормальної, підозрілої або зловмисної діяльності в межах контрольованого периметра

ПРИМІТКА: Призначення зонда - генерувати події безпеки; він вважається джерелом збору в межах служби виявлення аварійних ситуацій.

кваліфікована служба: служба виявлення аварійних ситуацій, що надається об'єкту, що вводить в експлуатацію, відповідно до довідкового документа

кваліфікація інциденту безпеки: визначення характеру та критичності інциденту безпеки

звітність: акт інформування суб'єкта введення в експлуатацію про випадок інциденту безпеки, що загрожує його інформаційній системі

безпека інформаційної системи: усі технічні та нетехнічні засоби контролю, що уможливлюють отримання інформації система управління подіями, які можуть порушити доступність, цілісність або конфіденційність оброблюваних даних або бути передані, та відповідні послуги, які ця система надає або робить доступними

договір про надання послуг: письмова угода між організацією, що вводить в експлуатацію, та постачальником послуг на виконання сервісу

ПРИМІТКА: Коли постачальник послуг є приватною особою, угода про надання послуг включає форму контракту.

постачальник послуг: організація, що надає послугу виявлення інцидентів безпеки відповідно до цього документа

найсучасніший: набір загальнодоступних передових практик, технологій та довідкових документів (а також інформація з якої можна зробити висновок), що стосуються безпеки інформаційних систем.

ПРИМІТКА: Ці документи можуть бути доступними в Інтернеті спільнотою з безпеки інформаційних систем, або розповсюджується довідковими або регулюючими органами.

субпідряд: операція, за допомогою якої постачальник послуг доручає іншій організації повністю або частково виконати договір, укладений із суб'єктом введення в експлуатацію.

контрольований периметр: вся або частина інформаційної системи суб'єкта введення в експлуатацію, що є об'єктом забезпечення служби виявлення інцидентів.

третя сторона: особа або організація, визнані незалежними від постачальника послуг та організації, що здійснює введення в експлуатацію.

3.2 Символи

Для цілей цього документа застосовуються символи, наведені в ETSI GS ISI 001-2 [2].

3.3 Скорочення

Для цілей цього документа застосовуються скорочення, наведені в ETSI GS ISI 001-2 [2], та наступні:

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (Франція)
CERT	Команда комп'ютерного реагування на надзвичайні ситуації
CIS	Центр Інтернет-безпеки
IS	Інформаційна система
ISI	Показники інформаційної безпеки
NIS	Безпека мережі та інформації
SLA	
SOC	

4 Загальний опис інциденту безпеки Послуга виявлення, що надається SOC

4.1 Діяльність служби виявлення аварійних ситуацій

Служба виявлення інцидентів охорони складається з трьох різних видів діяльності:

- Управління інцидентами, що означає всі технічні та організаційні засоби для виявлення та кваліфікації інцидента безпеки на основі зібраних подій. Зберігання та капіталізація інцидентів безпеки для того, щоб покращити послуги також є частиною цієї діяльності.
- Управління подіями, що означає всі технічні та організаційні засоби для забезпечення збору та зберігання подій безпеки.
- Управління звітністю, маючи на увазі всі технічні та організаційні засоби, що дозволяють інформувати доручення органу щодо виявлених випадків безпеки та зберігання цих звітів.

Діяльність з реагування та виправлення не входить до сфери дії цієї послуги.

4.2 Архітектура інформаційної системи служби виявлення

Цей документ не накладає жодної конкретної архітектури на інформаційну систему служби виявлення. Кілька можливих методів реалізації. Зокрема, відповідно до типу служби виявлення (внутрішньої чи зовнішньої), різні зони, представлені в цьому пункті, можуть бути розміщені в різних утвореннях або організмах, за умови, що вимоги цього документа виконуються.

Рисунок 2 - спрощене представлення типової архітектури інформації про виявлення системи аварійних ситуацій, наданої виключно в ознайомлювальних цілях.

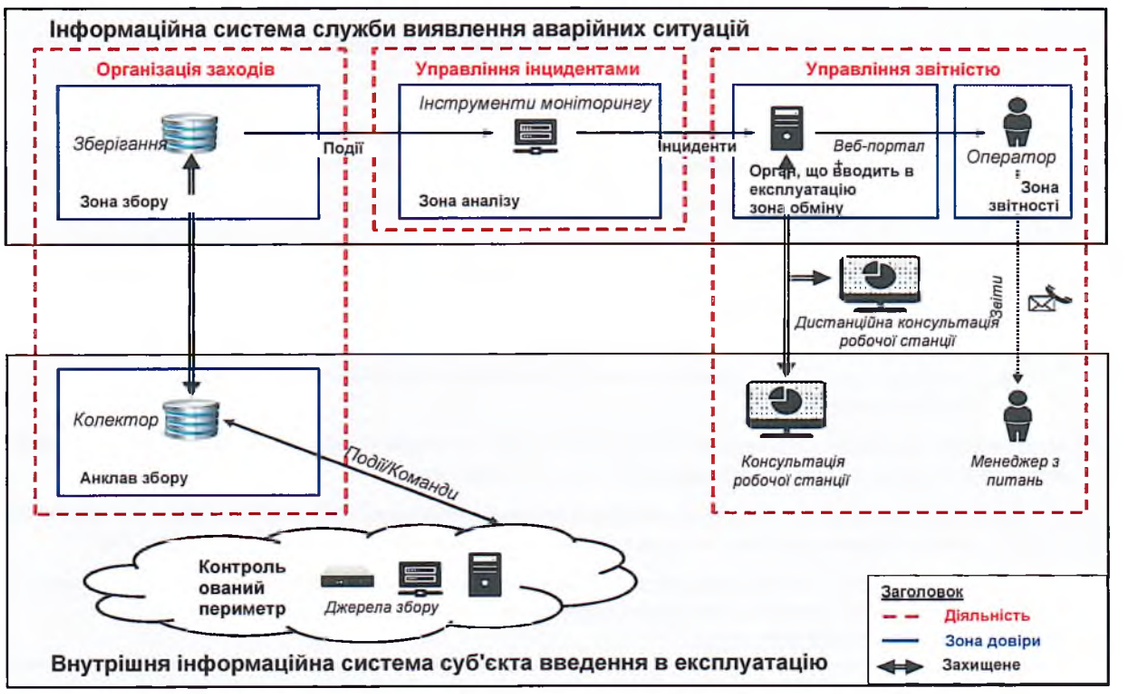

Рисунок 2: Спрощене представлення типової архітектури для інформаційної системи служби виявлення інцидентів безпеки

Інформаційна система служби виявлення організована в зони довіри, розділені за допомогою фільтрації, автентифікації та механізми контролю доступу. Зони довіри в інформаційній системі служби виявлення такі:

- Зона(и) збору (одна або кілька), що включає всі пристрої, що беруть участь у процесі збору, включаючи центральні колектори та системи для зберігання подій та, де це необхідно, довідкової інформації;
- зона(и) аналізу, що включає всі пристрої, що беруть участь у процесі аналізу, включаючи технічні засоби для аналізу інцидентів безпеки;
- зони(и) звітності, що включають системи звітності суб'єкта управління, зокрема системи обміну повідомленнями;
- зона и) обміну об'єкта, що вводиться в експлуатацію, що включає всі пристрої, що дозволяють об'єкту, що вводиться в експлуатацію, перегляд деталей інформації про інциденти, про які повідомляється, зокрема веб-портал, та надання, де це можливо, інформації, необхідної для кваліфікації події;
- адміністративна зона(и), що включає всі інструменти адміністрування та робочі станції адміністрації;
- зона(и) оновлення, що включає всі пристрої, що беруть участь у процесі завантаження оновлень для служби виявлення пристроїв;

- операційна зона(и), що включає робочі станції операторів;
- зони обміну, які є окремими для адміністраторів та операторів, включаючи всі пристрої, що дозволяють зовнішню передачу файлів інформаційної системи служби виявлення інцидентів безпеки.

Крім того, в межах повинна бути встановлена конкретна зона, яка є зовнішньою для інформаційної системи служб виявлення введення в експлуатацію внутрішньої інформаційної системи суб'єкта господарювання, надалі іменованої "анклавами" (через взаємодію з останніми). *Як мінімум* , повинен бути встановлений один анклав збору для розміщення пристроїв збору служб виявлення в межах об'єкта введення в експлуатацію. Зокрема, анклав збору містить одного або більше місцевих колекторів, роль яких полягає в централізації подій безпеки, що виникають у межах контрольованого периметра.

4.3 Сфера застосування вимог цього документа

У пункті 5.1 перераховані загальні вимоги, що стосуються юридичних зобов'язань постачальника послуг, включаючи його обов'язки по відношенню до організації, що вводить в експлуатацію, її гарантії і т. д.

Пункт 5.2 перелічує вимоги, що стосуються діяльності служби виявлення аварійних ситуацій:

- Вимоги щодо діяльності з управління інцидентами, включаючи навички операторів, особливості використовуваних інструментів, реалізацію правил виявлення тощо.
- Вимоги щодо діяльності з управління подіями, включаючи джерела збору, централізацію подій на колекторі тощо.
- Вимоги щодо діяльності з управління звітністю, включаючи засоби звітування, консультації квитків на інцидент тощо.

Пункт 5.3 перелічує вимоги, що стосуються захисту інформації, включаючи шифрування, фільтрацію між зоною довіри, розподілом ролей між адміністраторами та операторами тощо.

Пункт 5.4 перелічує вимоги, що стосуються організації постачальника послуг та управління послугою, включаючи створення етичного кодексу та набору персоналу, зміст нарад оперативно-стратегічного комітету тощо.

Пункт 5.5 перелічує вимоги, що стосуються якості та рівня обслуговування, включаючи характер показників, які мають бути відстежується, зміст угоди про надання послуг, встановленої між постачальником послуг та суб'єктом введення в експлуатацію, тощо

5 Вимоги, яким повинен відповідати постачальник послуг функціонування Центру безпеки операцій (SOC)

5.1 Загальні вимоги

a) Постачальник послуг повинен бути суб'єктом господарювання або частиною суб'єкта господарювання, що має правосуб'єктність, щоб його можна було утримувати юридично відповідальним за послуги, які він надає.

b) Постачальник послуг повинен дотримуватись чинного законодавства, де зберігаються дані SOC і обробляються інструментом аналізу.

c) Постачальник послуг повинен описати організацію діяльності з виявлення інцидентів безпеки, яку він забезпечує до суб'єкта введення в експлуатацію.

d) Постачальник послуг у своїй професійній якості зобов'язаний консультувати організацію, що вводить в експлуатацію.

f) Постачальник послуг повинен отримати страховку професійної відповідальності, що покриває будь-яку шкоду, заподіяну

введеному в експлуатацію суб'єкту господарювання та особливо його інформаційній системі під час надання послуги.

g) Постачальник послуг повинен переконатися, що згода суб'єкта введення в експлуатацію була отримана до будь-якого розкриття інформації, отриманої або надбаної під час надання послуги.

h) Постачальник послуг повинен переконатися, що надана їм інформація, включаючи рекламу, не є ні помилковою, нівводить в оману.

i) Постачальник послуг повинен надати достатньо доказів того, як він працює, особливо з точки зору своїх фінансових операцій, не може порушити його неупередженість або якість його роботи стосовно суб'єкта введення в експлуатацію або викликати конфлікт інтересів.

k) Постачальник послуг повинен мати діючі ліцензії на інструменти (програмне та апаратне забезпечення), що використовуються для надання обслуговування.

l) Постачальник послуг повинен попросити організацію, що вводить в експлуатацію, повідомити її про будь-які конкретні правові чи нормативні акти вимоги, яким він підпорядковується, особливо ті, що стосуються його сектору діяльності.

m) Постачальник послуг повинен інформувати організацію, що вводить в експлуатацію, коли це вимагає суб'єкт введення в експлуатацію
повідомити державний орган про інцидент безпеки (у країні, де знаходиться організація, що вводить в експлуатацію інформаційну систему, яка атакується) і повинна допомагати їй у цьому процесі, якщо суб'єкт введення в експлуатацію просить це зробити.

n) Постачальник послуг повинен укласти договір про надання послуг з організацією, що вводить в експлуатацію. Угода про надання послуг повинна відповідати вимогам пункту 5.5.3 і повинна бути офіційно затверджена письмово, суб'єктом введення в експлуатацію до здійснення послуги.

5.2 Діяльність служби виявлення аварій

5.2.1 Управління аваріями

a) Постачальник послуг повинен скласти з організацією, що вводить в експлуатацію, перелік можливих випадків та наслідків та впливів, пов'язаних з ними, на основі результатів оцінки ризику, підготовленої суб'єктом введення в експлуатацію (принаймні для критичного програмного забезпечення, що контролюється), а також щодо найсучасніших статистичних даних
, пов'язаних з ETSI GS ISI 001, частиною 1 [1] та частиною 2 [2]. Постачальник послуг повинен рекомендувати суб'єкту введення в експлуатацію оновити оцінку ризику у разі зміни його інфраструктури.

c) Постачальник послуг повинен взяти до уваги перелік інцидентів безпеки та їх походження в додатку B до ISO 27035-2 [i.7] , а також ETSI GS ISI 001-1 [1] та ETSI GS ISI 002 [3].

d) Постачальник послуг повинен розробити та впровадити разом із суб'єктом введення в експлуатацію стратегію аналізу, яка дає можливість виявити всі інциденти у списку інцидентів, яких побоюються (див. вимогу 5.2.1.a). Ця стратегія також може включати інші підходи, наприклад, засновані на поведінковому аналізі та пошуку загрози.
Під час засідань оперативного комітету стратегія аналізу повинна бути розглянута разом із замовником як визначено у пункті 5.4.3.

f) Стратегія аналізу повинна включати точний опис реалізації правил виявлення для виявлення інцидентів безпеки на основі зібраних подій.

g) Постачальник послуг повинен створити правила виявлення на основі:

- переліку випадків безпеки, яких побоюється суб'єкт, що вводить в експлуатацію;
- бази знань, придбаних у постачальників та компаній з безпеки інформаційних систем;
- внутрішньої бази знань, отриманих з досвіду постачальника послуг:
  - моніторингу та кваліфікації вразливостей, при цьому пріоритет надається тим, що стосуються виконання довільного коду, локально або віддалено;
  - моніторингу та кваліфікації протоколів командного управління;
  - моніторингу режимів роботи на атаки та зловмисний код;

- контекстуальних елементів, характерних для об'єкта введення в експлуатацію;
- інцидентів безпеки, виявлених будь-якими іншими організаціями, що вводять в експлуатацію.

h) Постачальник послуг повинен розробити та впровадити політику маркування правил виявлення. Ця політика повинна визначати для кожного правила виявлення:

- унікальний ідентифікатор правила виявлення, що пов'язує різні інструменти та пов'язані з ними бази знань;
- номер версії правила виявлення;
- the власник правила виявлення, тобто організація, яка володіє правами на правило виявлення;
- theавтор правила виявлення, маючи на увазі суб'єкт, який створив правило виявлення;
- theджерело правила виявлення, що означає суб'єкт, який є джерелом інформації, що дозволяє

створення правила виявлення, яке не обов'язково є власником або автором правила виявлення (наприклад, партнер, постачальник, організація, що вводить в експлуатацію тощо);

- дата створення правила виявлення;
- дата останньої модифікації правила виявлення;
- терміни розповсюдження правила виявлення, такі як "необмежений розподіл", "можуть поширюватися всередині спільноти, але не публічно", "може поширюватися всередині за необхідності", "може
поширюватися серед визначених осіб і не може бути перерозподілений" або у формі ПРОТОКОЛУ СВІТЛОФОРА (TLP) або інші, відповідно до домовленостей, визначених джерелами виявлення правил;
- чи можна проводити пошук з відкритим кодом залежно від рівня чутливості та методи розподілу;
- опис поведінки, яку правило має на меті виявити:
  - опис загрози;
  - де це можливо, описи та ідентифікатори (наприклад, CVE) вразливостей, для яких експлуатація або спроби експлуатації були виявлені правилом;
  - виявлені правилом фази нападу, такі як: розвідка, початкове проникнення, взаємодія з інфраструктурою управління та керування, ескалацією привілеїв, бічними переміщеннями, ексфільтрацією тощо;
  - будь-яка інша інформація, необхідна для опису поведінки, на яку націлено правило;
- описові елементи для реалізації правила в засобах технічного аналізу:
  - метод аналізу подій та запуску правила виявлення;
  - будь-які потенційні експлуатаційні обмеження, пов'язані з технічними критеріями;
- інструкції з аналізу та кваліфікації, яких повинен дотримуватись оператор у випадку, якщо є правило виявлення спрацьовує.

i) Постачальник послуг повинен встановити та оновлювати для кожного суб'єкта введення в експлуатацію перелік усіх правил виявлення, які були впроваджені або які впроваджуються як частина послуги. У цьому списку слід вказати,
для кожного правила, його ідентифікатор та номер версії:

- дата (дати), коли правило виявлення було включено до засобів технічного аналізу;
- якщо постачальник послуг провів *апостеріорний* аналіз з цим правилом виявлення (див вимога 5.2.1.dd) та дату цього аналізу, якщо це можливо;
- дату (дати), коли правило виявлення було вилучено із засобів технічного аналізу, що використовуються.

Цей список повинен дати можливість створити історичний запис правил виявлення, враховуючи виявлення правил, які діяли в певний час або протягом певного періоду. Правило виявлення, яке вже було вилучено з технічних інструментів, що використовуються, повинні бути позначені як вилучені та не повинні видалятись з цього списку.

ПРИМІТКА: Справа, в якій були внесені зміни до правила виявлення виключно для субперіметрів контрольованого периметру повинна бути вказана у списку.

j) Постачальник послуг повинен щонайменше раз *на місяць надсилати органу, що вводить* в експлуатацію, правило виявлення, звіт про стан, який представляє:

- кількість правил виявлення, створених, модифікованих або вилучених із використовуваних інструментів аналізу;
- ідентифікатор, номер версії та опис кожного правила, яке було створене, модифіковане або відкликане з інструментів аналізу, що використовуються;
- причина створення, модифікації або скасування правила захисту (наприклад, створення, модифікація або зняття на вимогу суб'єкта введення в експлуатацію тощо).

m) Постачальник послуг повинен застосовувати в засобах технічного аналізу у використанні всі визначені правила виявлення у списку, викладеному у вимозі 5.2.1.i), за винятком правил, позначених як відкликані.

n) Постачальник послуг повинен самостійно додавати нові правила виявлення до використовуваних інструментів технічного аналізу.

q) Після додавання цього типу постачальник послуг повинен оновити документальний запис та надати інформацію про деталі доповнень, внесених для забезпечення моніторингу та простежуваність таких доповнень.

r) Постачальник послуг повинен кваліфікувати виявлені випадки безпеки, щоб оцінити їх правдивість (істинно/невірно позитивними, доведеними інцидентами чи ні) та критичність (функціональний вплив, інформаційний вплив тощо).

s) Постачальник послуг повинен встановити з організацією, що вводить в експлуатацію, шкалу критичності, пов'язану з інцидентами безпеки, яких побоюються, беручи до уваги оцінку ризику і особливо загрози, активи, потенційні наслідки та рівень їх критичності.

t) Постачальник послуг повинен використовувати шкалу критичності для інцидентів інформаційної безпеки, наведену в додатку C до ISO 27035-2 [i.7] .

Як частину кваліфікації інциденту з безпекою, постачальника послуг можна запросити здійснити пошук з відкритим кодом, особливо в Інтернеті, на основі інформації, зібраної або взятої з аналізів (криптографічні відбитки пальців, імена шкідливих файлів або шкідливого програмного забезпечення, ланцюжки символів, що містяться в шкідливих програмах, доменні імена, IP-адреси тощо).

Пошук з відкритим кодом з використанням інформації, зібраної або взятої з аналізів, може привернути увагу зловмисника.
Таким чином, важливо, щоб постачальник послуг проявляв граничну обережність при їх виконанні.
Таким чином, він повинен брати до уваги маркування правил виявлення, що вказують на можливість проведення такого пошуку, чи ні (див. вимогу 5.2.1.h).

Постачальник послуг повинен визначити методологію пошуку з відкритим кодом на основі інформації, зібраної або взятої з аналізів. У ньому має бути вказано, які типи інформації можна шукати та пов'язані з нею умови.

v) Постачальник послуг повинен мати можливість інтегрувати результати тестів на наявність вразливостей та вторгнень що вводиться в експлуатацію суб'єктом власної інформаційної системи, зокрема, це може призвести до:

- створення правил виявлення, пов'язаних з виявленими вразливими місцями;
- розробки баз знань щодо наявних вразливих місць для поліпшення діагностики, будь то через інструменти технічного аналізу (кореляція) або оператори (використання великих літер та використання базових знань з IC під наглядом).

w) Постачальник послуг повинен створити квиток для кожного виявленого інциденту безпеки та зробити його доступним для
суб'єкт введення в експлуатацію. *Як мінімум* один раз квиток на випадок безпеки повинен містити такі елементи:

- дату створення квитка та різні операції, що проводяться за цим квитком (простежуваність дії);
- дата та час виявлення інциденту з безпекою;
- дату набрання чинності подією або подіями, що призвели до інциденту з безпекою;
- опис інциденту з безпекою;
- критичність інциденту з безпекою;
- опис впливу аварії на безпеку для суб'єкта введення в експлуатацію;
- ідентифікатори та номери версій правил виявлення, які були активовані;
- обладнання, яке генерувало та збирало події інцидентів;
- ідентифікатори подій, які дали змогу виявити інцидент;
- ризик, що виникає в результаті інциденту.

x) Постачальник послуг повинен визначити формат квитків на випадок безпеки разом із введенням в експлуатацію об'єкту.

y) Постачальник послуг повинен використовувати формат квитка на випадок безпеки, встановлений у ETSI GS ISI 002 [3] та ISO 27035-2 [i.7] .

z) Постачальник послуг повинен мати інструмент для управління квитками на випадок безпеки.

aa) Постачальник послуг повинен пов'язати кожен квиток на інцидент безпеки з його контекстом (пов'язані події та кваліфікація аналізувати звіт(и) та зберігати ці елементи централізовано, незалежно від того, чи перебувають інциденти безпеки кваліфіковані, перевірені або закриті.

bb) Постачальник послуг повинен впроваджувати та оновлювати централізований хронологічний запис для кожної особа, що вводить в експлуатацію, ідентифікує всі виявлені випадки безпеки.

вв) Постачальник послуг повинен впровадити процес управління ємністю квитків на аварійні ситуації та їх контекст, що дозволяє контролювати його розвиток і мати можливість адаптувати його для забезпечення їх збереження для тривалості послуги, за умови дотримання законодавства та норм, що діють щодо зацікавленої території (див. вимогу 5.1.b).

dd) Стратегія аналізу повинна гарантувати, що для кожного правила виявлення, яке створюється або модифікується, постачальник послуг проводить *апостеріорний* аналіз, маючи на увазі аналіз усіх подій, які зберігалися протягом певного періоду, який визначається разом із суб'єктом введення в експлуатацію в стратегії аналізу.

Ця вимога не застосовується до правил виявлення, що вимагають типів подій, яких ще немає в системи зберігання подій.

Постачальник послуг повинен мати можливість, *як мінімум* , шукати такі типи:

- файли: відбиток пальця (MD5, SHA1, SHA256), відбиток імені, шлях доступу, розмір, розширення, магічне число;
- загальнодоступні IP-адреси;
- домени для наступних протоколів: HTTP, SMTP та DNS;
- URL;
- користувач-агент;
- поля електронної пошти: вихідний домен, домен призначення, відбиток пальця, відмітка часу;
- Поля сертифіката X509:відбиток пальця, емітент, дата дії,предмет, розширення, ім'я хосту, позначка часу.

Рекомендується, щоб постачальник послуг мав можливість шукати комбінації цих показників компромісу.

ee) Постачальник послуг повинен мати можливість на запит суб'єкта введення в експлуатацію провести аналіз сукупності подій, які зберігались за попередні шість місяців.

5.2.2 Управління подіями

a) Постачальник послуг повинен розробити разом із організацією, що вводить в експлуатацію, та запровадити стратегію збору, засновану на переліку інцидентів безпеки, яких побоюються (див. вимогу 5.2.1.a). Стратегія збору повинна бути розглянута з комісією, що вводить в експлуатацію, на засіданнях оперативного комітету, визначених у пункті 5.4.3.

b) Стратегія збору повинна визначати перелік джерел колекції, колекціонерів, події, що збираються, описати методи збору (протоколи, програми, властивості захисту тощо) та визначити частоту збору.

c) Постачальник послуг повинен бути *принаймні* здатним збирати події з наступного джерела збору:

- обладнання безпеки: мережеві брандмауери, брандмауери додатків, шифрувачі, зонди, антивірусне програмне забезпечення, VPN концентратори, шлюзи SSL, проксі, зворотні проксі;
- мережеве обладнання: маршрутизатори, комутатори, обладнання, що генерує дані про потоки, DNS-сервери, балансири навантаження, сервери часу;
- сервери інфраструктури: автентифікація, каталоги, розповсюдження програмного забезпечення, віддалене управління, нагляд, віртуалізація, файлові сервери, резервні копії, пошта, друк;
- бізнес-сервери: веб-сервери, бази даних, сервери додатків, колектори;
- робочі станції: основні операційні системи, програми безпеки;
- мобільні пристрої через сервери управління мобільним парком (Mobile Devices Management).

d) Постачальник послуг повинен мати можливість збирати події, що виникають із обладнання, що включає промислове обладнання інформаційних систем: промислові програмовані автомати, промислові брандмауери, промислові комутатори та промислові маршрутизатори.

f) Постачальник послуг повинен самостійно розвивати свої можливості збору (джерела збору та подій), у зв'язку зі списком інцидентів, що побоюються.

g) У разі виникнення труднощів або неможливості здійснити колекцію однієї або декількох подій із джерела збору, постачальник послуг повинен якомога швидше попередити організацію, що вводить в експлуатацію, та надати докладні причини відмови. Максимальний період між рішенням про здійснення збору та звітом про невдачу впровадження в експлуатацію повинен бути визначений у договорі про надання послуг.

h) Постачальник послуг повинен виконувати свій обов'язок консультувати організацію, що вводить в експлуатацію, щодо розвитку, впровадження та перегляд стратегії збору. У цій якості він повинен порадити суб'єкту введення в експлуатацію щодо розробки та перегляду політики ведення журналу (джерела збору, типи подій, що реєструються періоди зберігання, стандартизація інформації, синхронізація джерел часу тощо) та щодо розгортання реєстраційних пристроїв на контрольованому периметрі в інформаційній системі об'єкта введення в експлуатацію.

i) Постачальник послуг повинен рекомендувати суб'єкту введення в експлуатацію, який він включає в стратегію збору розгортання зондів на кожному з з'єднань контрольованого периметра, і зокрема взаємозв'язки з:

- Інтернетом;
- сторонніми інформаційні системи (партнерами, субпідрядниками тощо);
- інші інформаційні системи суб'єкта введення в експлуатацію більш вразливі або з меншим рівнем безпеки
  класифікації або рівня чутливості.

п) Події з колекційних джерел повинні бути централізованими на одному або декількох колекторах, розташованих у колекції анклав, описаний у вимогах пункту 5.3.14.

ПРИМІТКА: Для простоти, для решти цього документа передбачається, що існує лише один колектор.

o) Колектор анклаву збору повинен дозволяти проводити початкову фільтрацію подій з метою передавати лише зоні збору та аналітичним інструментам ті події, які мають значення для виявлення та визначення в стратегії збору.

r) Колектор повинен мати можливість виявляти насичення та втрату комунікаційних подій, які могли б запобігти цій передачі подій безпеки службі виявлення та затримка передачі подій службі виявлення інструментів аналізу, якщо це необхідно. Постачальник послуг повинен гарантувати ємність колектора в договорі про надання послуг. Еволюція ємності накопичувача колектора слід контролювати та представляти дорученнями органу на засіданнях оперативного комітету, визначених у пункті 5.4.3.

s) Постачальник послуг повинен мати централізоване уявлення про всі зібрані події, включаючи асоціацію кожної події з колектором, з якого воно прийшло.

t) Системні годинники колекторів повинні бути синхронізовані з одним джерелом часу (див. Вимогу 5.3.9.l).

u) Постачальник послуг повинен проіндексувати всі зібрані події та мати можливість здійснювати пошук серед зібраних подій.

v) Постачальник послуг повинен мати можливість знаходити та надавати будь-які зібрані події за запитом суб'єкта введення в експлуатацію.

w) Постачальник послуг повинен запровадити процес управління обробкою та можливостями зберігання подій надання можливості постачальнику послуг контролювати його розвиток і мати можливість змінювати його за необхідності та забезпечувати їх зберігання принаймні шість місяців (див. вимогу 5.2.1.ee) за умови дотримання законодавства та норм, що діють на відповідній території (див. вимогу 5.1.b).

5.2.3 Управління звітністю

a) Постачальник послуг повинен мати один або кілька захищених інформаційних каналів, доступних для введення в експлуатацію суб'єкта господарювання, зокрема щодо звітності (див. вимогу 5.2.3.b) та обміну детальною інформацією (див вимога 5.2.3.l).

b) Постачальник послуг повинен мати принаймні два доступні методи звітування: номінальний метод та вторинний метод. Метод вторинної комунікації слід випробовувати принаймні кожні шість місяців та кожен раз вносити зміни до інформаційної системи служби виявлення інцидентів безпеки. Наприклад, методи звіту можуть складатися з:

- електронна пошта;
- коротке текстове повідомлення (СМС);
- телефон.

c) Постачальник послуг повинен розробити разом із організацією, що вводить в експлуатацію, та впровадити безпеку
стратегії звітності про аварії, що дозволяє йому повідомити організацію, що вводить в експлуатацію, у випадку, якщо це інцидент безпеки виявлено. Стратегію складання звітності слід переглянути разом із суб'єктом введення в експлуатацію в оперативному засіданні комітетів, визначеному у пункті 5.4.3.

d) Стратегія звітування повинна визначати, *як мінімум* , перелік інцидентів безпеки, про які слід повідомити, формат, зміст, обмеження часу та рівень чутливості або класифікації звітів, а також осіб, яким потрібно звітувати, особливо стосовно інциденту з безпекою та рівня його критичності.

e) Постачальник послуг повинен виконувати свій обов'язок консультувати організацію, що вводить в експлуатацію, у розробці, впровадженні та перегляді стратегії звітності. У цій якості він повинен проконсультувати об'єкта введення в експлуатацію щодо посадовців, яким слід повідомити, та методи звітування.

f) Постачальник послуг повинен рекомендувати органу, що вводить в експлуатацію, включення конкретних звітів до стратегії звітування у разі виявлення серйозних інцидентів безпеки в її інформаційній системі.

h) Постачальник послуг повинен централізувати всі звіти в системі зберігання звітів. Наступну інформацію

слід зберігати:

- дата і час звіту;
- метод звітності;
- одержувач(і) звіту; і
- зміст звіту, зокрема, зокрема номер квитка на інцидент.

ПРИМІТКА: Вищевказана інформація стосовно звітів може бути включена до квитків на інциденти.

j) Постачальник послуг повинен запровадити та постійно оновлювати централізовані та хронологічні записи, суб'єктом введення в експлуатацію, посилаючись на всі звіти, складені для об'єкта введення в експлуатацію. Зокрема, звіт повинен містити: дату та час звіту, метод звітування, одержувача (ів) звіту, зміст звіту, включаючи, зокрема, номер квитка на випадок.

k) Постачальник послуг повинен запровадити процес управління ємністю зберігання звітів, який допоміг би постачальнику послуг контролювати його розвиток і мати можливість змінювати його, щоб забезпечити їх збереження для тривалості служби за умови дотримання законодавства та норм, що діють в межах території зацікавленої сторони (див. вимогу 5.1.b).

l) Постачальник послуг повинен надати замовнику:

- веб-портал, який дозволяє йому переглядати та оновлювати стан інцидентів та вжитих заходів безпеки;
- запам'ятовуючий пристрій, що дозволяє замовнику:
  - отримати контекст інцидентів безпеки (пов’язані з ними події та звіт(и) про кваліфікаційний аналіз) щодо нього;
  - де необхідно, довідкова інформація, необхідна операторам для кваліфікації інциденту;
  - доступ до показників безпеки.

5.3 Захист інформації

5.3.1 Політика безпеки інформаційних систем

a) Постачальник послуг повинен розробити аналіз ризиків та пов'язаний з ним план лікування ризиків, що охоплює повну інформацію сфери дії служби виявлення інцидентів.

c) *Постачальник послуг повинен переглянути* оцінку ризику та відповідний план лікування ризику мінімум раз на рік та у разі будь-яких структурних змін служби виявлення, особливо тих, що стосуються її хостингу, інфраструктури або архітектури.

e) Постачальник послуг повинен розробити та впровадити політику безпеки інформаційних систем на основі оцінки ризику.

5.3.2 Рівні чутливості або класифікації

b) Постачальник послуг повинен застосовувати гігієну інформаційних технологій до служби виявлення інцидентів інформаційної системи, заснованої на загальних довідкових системах, таких як французька "Guide d'hygiene informatique" [i.8], the US "CIS Critical Security Controls for Effective Cyber Defense" [i.9] or standards such as the ISO/IEC 27002 [4].

5.3.3 Територіальність послуги

a) Постачальник послуг повинен розміщувати дані, що стосуються служби виявлення інцидентів безпеки, виключно всередині
Європейського Союзу. У випадку, якщо деякі колекційні джерела знаходяться за межами Європейського Союзу,
події, що походять з цих джерел, передаватимуться колектору, який знаходиться в межах Європейського Союзу.

5.3.4 Огляд безпеки

a) Постачальник послуг повинен задокументувати та впровадити план перевірки безпеки, що визначає сферу застосування та
частоти перевірок безпеки відповідно до управління змінами, політики та результатів
оцінки ризику.

b) Цей план перевірки безпеки повинен перевірити правильність впровадження інформаційної безпеки та захисту
механізмів, за які відповідає постачальник послуг. Цей план перевірки безпеки повинен містити, зокрема,
мінімум :

- огляд логічного та фізичного контролю доступу, реалізований для захисту пристроїв послуг виявлення ;
- перегляд привілеїв та прав доступу до служби виявлення інцидентів безпеки. Цей огляд повинен включати перевірку облікових записів адміністратора та оператора *мінімум* раз на місяць.

c) Постачальник послуг повинен періодично переглядати план перевірки безпеки, а також у випадку будь-якої структурної
зміни в службі виявлення, особливо такої, що стосується її хостингу, інфраструктури чи архітектури.

e) План перегляду безпеки повинен включати трирічну програму аудиту, що включає, зокрема:

- аудит конфігурації серверів та мережевого обладнання, що входять до сфери послуг виявлення . Ці перевірки проводяться шляхом вибірки та повинні включати всі типи обладнання та серверів присутніх в інформаційній системі служби;
- випробування на проникнення інформаційної системи обслуговування (особлива увага вимагається щодо взаємозв'язків);
- якщо послуга отримує вигоду від внутрішніх розробок, перевірки вихідного коду щодо впровадженої
функції безпеки, а також функції високого ризику (наприклад: введення/виведення).

f) Програма аудиту повинна включати мінімум один зовнішній аудит на рік.

h) Постачальник послуг повинен оновити план лікування ризиків (див. вимогу 5.3.1.a) з метою інтеграції результатів аудитів.

i) Постачальник послуг повинен повідомляти результати перевірок своїй управлінській групі. Результати аудиту повинні бути офіційно затверджені письмово керівною групою постачальника послуг.

5.3.5 Фізична безпека

a) Постачальник послуг повинен розробити та оновлювати список осіб, уповноважених на доступ до приміщення
розміщення служби виявлення інцидентів безпеки.

b) Постачальник послуг повинен запровадити механізми, що дозволяють забезпечити можливість лише уповноваженим особам
отримати доступ до приміщення, де розміщена служба виявлення аварійних ситуацій.

c) Постачальник послуг повинен впровадити механізми, що дозволяють йому реєструвати доступ до приміщень, де розміщується
служба виявлення інцидентів безпеки, одночасно забезпечуючи цілісність журналів доступу.

5.3.6 Безперервність обслуговування

a) Постачальник послуг повинен розробити та впровадити для служби виявлення аварій безпеки план безперервності послуг, який повинен враховувати ризики щодо його доступності. Цей план повинен включати кілька різних
компонентів, включаючи мінімум такі компоненти:

- резервні копії системи;

- резервні копії конфігурації;
- резервні копії даних.

b) Постачальник послуг повинен перевіряти план безперервності обслуговування як мінімум раз на рік.

5.3.7 Служба виявлення послуг (SOC SOC)

a) Постачальник послуг повинен впровадити, для власного рахунку, службу виявлення інцидентів безпеки, надалі
згадується як "служба виявлення послуг", що стосується інформаційної системи інциденту безпеки служби виявлення.

b) Постачальник послуг повинен на основі оцінки ризику (див. вимогу 5.3.1.a) розробити стратегію збору, стратегію аналізу та стратегію звітування як частина послуги виявлення послуги.

h) Постачальник послуг повинен розробити процес управління інцидентами безпеки служби. Цей процес повинен включати звіт суб'єктам, що вводять в експлуатацію, про виникнення інциденту з охороною на безпеці служба виявлення інцидентів. У звіті повинно бути зазначено характер інциденту з безпекою та вжиті заходи постачальником послуг, щоб відповісти на нього.

5.3.8 Розділення інформаційної системи послуг

a) Постачальник послуг повинен використовувати інформаційну систему служби виявлення інцидентів безпеки за певних обставин де спільне використання послуг різного рівня безпеки не знижує рівень безпеки найвищого рівня інформаційної системи обслуговування.

b) Постачальник послуг повинен розділити інформаційну систему служби виявлення інцидентів безпеки на кілька зон довіри, в яких знаходяться всі пристрої, що беруть участь у службі виявлення:

- зона(и) збору (одна або декілька), що включає всі пристрої, задіяні в процесі збору, включаючи центральні колектори та системи для зберігання подій та, де це необхідно, довідкової інформації;
- зона(и) аналізу, що включає всі пристрої, задіяні в процесі аналізу, включаючи технічні інструменти для аналізу випадків безпеки;
- зони(и) звітності, що включає системи звітності суб'єкта введення в експлуатацію, зокрема їх системи повідомлень;
- зона(и) обміну об'єкта введення в експлуатацію, що містить усі пристрої, що забезпечують безпечний обмін інформацією з замовником, зокрема веб-порталом;
- адміністративні зони, що включають усі адміністративні інструменти та робочі станції адміністраторів;
- зона(и) оновлення, що включає всі пристрої, задіяні в процесі завантаження оновлень для пристрої обслуговування виявлення;
- операційна зона(и), що включає робочі станції операторів;
- зони обміну, які є окремими для адміністраторів та операторів, включаючи пристрої, що дозволяють
передачу файлів з інформаційної системи служби виявлення інцидентів безпеки та до неї.

c) Постачальник послуг повинен запровадити заходи для забезпечення розподілу між різними зонами довіри, зокрема за допомогою механізмів фільтрації, автентифікації та контролю доступу.

d) Постачальник послуг повинен створити та оновлювати матрицю еталонних потоків для інциденту безпеки системи виявлення, разом із відповідною політикою фільтрації, дозволяючи лише ті потоки, які суворо необхідні для роботи служби виявлення аварійних ситуацій.

e) Постачальник послуг повинен впроваджувати рішення для шифрування та аутентифікації IP між цими зонами довіри як тільки інформація, якою обмінюються між цими зонами, проходить через транспортні мережі, які не є присвяченими службі виявлення.

f) Постачальник послуг повинен створити та оновлювати детальний опис архітектури безпеки Інформаційної система служби виявлення інцидентів. Цей опис повинен ідентифікувати всю

інформаційну систему пристроїв та зони довіри служби виявлення.

g) Постачальник послуг повинен розподілити між організаціями, що вводять в експлуатацію:

- системи зберігання та обробки подій та супутньої довідкової інформації;
- системи зберігання та обробки інцидентів безпеки, засоби технічного аналізу та інструменти інцидентів безпеки
  для управління квитками;
- звіти, веб-портал та система обміну повідомленнями.

Це розділення повинно бути досягнуто за допомогою логічних механізмів контролю доступу *як мінімум* , іреалізовано відповідно до конкретних експлуатаційних вимог (права, привілеї, автентифікація тощо).

5.3.9 Адміністрування та функціонування служби

a) Адміністратори повинні керувати пристроями служби виявлення випадків безпеки через спеціальні адміністративні робочі станції, розміщені в адміністративній зоні та відокремлені від робочих станцій оператора.

b) Адміністрація пристроїв служби виявлення інцидентів безпеки повинна бути дозволена лише від адміністративної зони через мережеві інтерфейси пристроїв, призначених для адміністрування.

c) Постачальник послуг повинен реєструвати кожен доступ до пристроїв служби виявлення аварій безпеки та виконаних дій.

d) Постачальник послуг повинен створити централізований каталог, призначений для автентифікації адміністраторів та операторів служби, що дозволяє, зокрема, автентифікацію також на своїх робочих станціях
як і на всіх пристроях служби виявлення.

Впроваджене рішення повинно забезпечити чітке логічне розділення груп адміністраторів та операторів в централізованому каталозі для автентифікації, авторизації та управління ідентифікаторами.

e) Постачальник послуг повинен встановити засоби контролю, щоб гарантувати, що адміністратори керують пристроями з виявлення інцидентів безпеки, що використовують адміністративні облікові записи, присвячені цим завданням і доступні лише для
адміністраторів.

f) Адміністратори не повинні мати адміністративних прав на своїх робочих станціях адміністрації.

g) Постачальник послуг повинен впроваджувати засоби контролю, щоб гарантувати, що адміністратори та оператори можуть мати доступ лише
ті ресурси, які мають відношення до їх завдань (див. додаток A).

h) Постачальник послуг повинен застосовувати засоби контролю, що позбавляють операторів адміністративних прав на пристрої служби виявлення
, у тому числі на власних робочих станціях.

i) Робочі станції адміністраторів та операторів повинні бути підключені безпосередньо виключно до системи безпеки Інформаційної системи виявлення інцидентів.

У разі необхідності отримати доступ до Інтернету або інших інформаційних систем (внутрішніх постачальника послуг інформаційної системи, наприклад), адміністратори та оператори повинні отримувати до них доступ через спеціальний шлюз за спеціальним протоколом (див. вимогу 5.3.15.a).

j) Постачальник послуг повинен створити зону обміну для передачі файлів із зовнішньої сторони інформаційної системи служби виявлення як частина адміністрування або роботи служби виявлення.

l) Постачальник послуг повинен розміщувати в адміністративній зоні контрольний сервер часу, щоб переконатися, так що всі
годинники, що використовуються пристроями служб виявлення, синхронізуються.

5.3.10 Взаємозв'язки з інформаційною системою послуг

a) Єдиним дозволеним взаємозв’язком із службою виявлення аварійних ситуацій є:

- інформаційна система суб'єкта введення в експлуатацію:
  - для збору подій та довідкової інформації через анклав збору;
  - для адміністрування пристроїв збору;
  - для роботи інкасаційних пристроїв;
  - для надсилання нечутливої інформації по незахищеному каналу, зокрема звітності інцидентів безпеки;
  - для відправки конфіденційної інформації через захищений канал, зокрема звітування про повну та детальну інформацію, пов'язану з інцидентами в галузі безпеки;
- віддалених робочих станцій адміністрування та експлуатації (див. пункт 5.3.16) через певні шлюзи;
- віддалені робочі станції консультацій через певний шлюз (див. пункт 5.3.16);
- сервери оновлення для завантаження оновлень пристроїв служби виявлення інцидентів безпеки за допомогою оновлення зони (див. пункт 5.3.11);
- Інтернет-шлюз, що забезпечує доступ іззовні (див. пункт 5.3.15).

b) Постачальник послуг повинен фільтрувати потоки на всіх взаємозв'язках із службою виявлення аварійних ситуацій інформаційної системи з використанням фільтруючих рішень.

c) Потоки при взаємозв'язках із службою виявлення аварій безпеки повинні шифруватися за допомогою IPsec Рішення для шифрування та автентифікації VPN.

Єдині винятки з цієї вимоги за умови дотримання вимог пунктів 5.3.11 та 5.3.12, є взаємозв'язками з:

- серверами оновлення для завантаження оновлень пристроїв служби виявлення інцидентів безпеки через оновлення зони (див. пункт 5.3.11);
- зокрема, інформаційна система суб'єкта введення в експлуатацію для надсилання нечутливої інформації в звіті про аварії (див. пункт 5.3.12).

e) Постачальник послуг повинен захищати конфіденційність, цілісність та достовірність усієї інформації, якою обмінюються між інформаційною системою служби виявлення інцидентів безпеки та інформаційною системою суб'єкта введення в експлуатацію.

5.3.11 Зона оновлення

a) Постачальник послуг може реалізувати зону оновлення, що містить одну або кілька ретрансляційних станцій, підключених до виділеного Інтернет-шлюзу, що дозволяє завантажувати оновлення служби виявлення інцидентів безпеки пристроїв.

ПРИМІТКА: Термін "оновлення" також охоплює оновлення з офіційних джерел довідкових документів, що використовуються при виявленні сервісних пристроїв.

ПРИКЛАД: Засоби моніторингу та аналізу загроз.

b) Виконавець повинен здійснювати ручне автономне оновлення пристроїв виявлення інцидентів безпеки , які не можуть бути оновлені через ретрансляційну станцію.

Наступні вимоги застосовуються лише у тому випадку, якщо встановлена зона оновлення:

c) Виконавець повинен застосувати фільтр білого переліку для забезпечення завантаження ретрансляційною станцією (станціями) офіційного оновлення для пристроїв виявлення інцидентів безпеки з офіційних джерел оновлення постачальника.

d) Виконавець повинен забезпечувати справжність і цілісність оновлень, що завантажуються із авторизованого джерела оновлення.

e) Виконавець повинен налаштувати рішення фільтрації (див. Вимогу 5.3.10.b) таким чином, щоб вони лише дозволяли потоки, що ініціюються від ретрансляційної станції (станцій) до Інтернет-шлюзу.

5.3.12 Зона звітності

b) Пристрій фільтрування (див. вимогу 5.3.10.b) при взаємодії інформації системи інформації служби виявлення між зовнішньою інформаційною системою служби та зоною звітності повинен дозволяти лише потоки, що направляються із зони звітності для надсилання нечутливої інформації.

ПРИКЛАД: Повідомлення про інциденти безпеки.

5.3.13 Зона обміну замовника послуг

a) Виконавець повинен створити зону обміну замовника послуг, що включає *як мінімум* :

- веб-портал, що дозволяє переглядати та оновлювати стан інцидентів безпеки та вжитих дій;
- пристрій для зберігання, що дозволяє надання інформації замовнику послуг про контекст інцидентів безпеки, виявлених в межах контрольованого ним периметра (пов'язані події та звіт (звіти) кваліфікаційного аналізу), що дозволяє замовнику послуг, за його бажанням, зберігати інформацію, необхідну для кваліфікації інциденту, та надає можливість замовнику послуг отримати доступ до показників безпеки.

ПРИМІТКА. Засоби аналізу шкідливого контенту можуть використовуватися між зоною обміну і зоною збору замовника послуг.

Що стосується інструментів аналізу шкідливого контенту, Виконавець повинен спланувати конкретну обробку файлів, що зашифровані або не піддаються аналізу аналізу.

Виконавець повинен реєструвати відмітку часу, назву та криптографічний відбиток усіх файлів, що обробляються інструментами аналізу шкідливого контенту.

b) Виконавець повинен виділити одну віртуальну машину для кожного замовника послуг для розміщення примірника веб-порталу та пристрою зберігання даних про випадки безпеки та звіти.

c) Виконавець повинен створити каталог, призначений для автентифікації замовника послуг в пристроях, розміщених у зоні обміну замовника послуг. Виконавець повинен здійснити автентифікацію замовника послуг використовуючи:

- зареєстровані облікові записи та щонайменше два фактори для автентифікації особи щодо машини;
- взаємна автентифікація для автентифікації від машини до машини.

Виконавець повинен вести список облікових записів, яким надано доступ до цієї зони, разом пов'язаними привілеями.

e) Виконавець повинен запровадити засоби контролю для забезпечення того, щоб замовник послуг мав доступ лише до тих ресурсів, що мають значення для його послуг.

f) Виконавець повинен застосовувати засоби контролю, що позбавляють замовника послуг від адміністративних чи операційних прав на пристрої виявлення.

g) Виконавець повинен встановити брандмауер веб-додатків для фільтрування запитів до веб-порталу.

h) Пристрій фільтрування (див. Вимогу 5.3.10.b) між зоною обміну замовника послуг та внутрішньою інформаційною системою замовника послуг повинна забороняти всі потоки, за винятком:

- потоки, що перебувають між згаданою зоною обміну замовника послуг та консультативним анклавом в межах внутрішньої інформаційної системи замовника послуг, що забезпечує виключно консультації та оновлення статусу інцидентів та дій, здійснених через веб-портал, та безпечний обмін інформацією
  між цими двома зонами;
- потоки між згаданою зоною замовника послуг та віддаленими робочими консультаційними станціями (див
  вимога 5.3.16.l) виключно створюючи можливості для консультацій та оновлення стану інцидентів та дій, здійснених через веб-портал та безпечний обмін інформацією з цими робочими станціями.

5.3.14 Анклав збору даних в системі інформації замовника послуг

a) Всі пристрої виявлення інцидентів безпеки, які з'єднані з контрольованим периметром (зокрема, пристроями збирання даних) повинні розташовуватися в межах одного або кількох анклавів збору даних у внутрішній інформаційній системі замовника послуг.

ПРИМІТКА: Задля кращого розуміння — для іншої частини цього документа передбачається, що існує лише один анклав збору даних.

b) У договорі про надання послуг Виконавець повинен визначити з замовником послуг обов'язки щодо права власності на пристрої, розміщені в анклаві збору даних.

c) Виконавець повинен визначити у договорі про надання послуг наступні обов'язки щодо адміністрування та експлуатації пристроїв, розміщених у збірному анклаві:

- замовник послуг повинен відповідати за адміністрування пристрою фільтрування між цим анклавом збору даних та внутрішньою інформаційною система замовника послуг, в разі наявності (див вимога 5.3.14.l);
- Виконавець повинен нести відповідальність за адміністрування та функціонування всіх інших пристроїв, розміщених у анклаві збору даних, включаючи пристрій фільтрування між цим анклавом збору даних та обладнанням, що використовується для шифрування IPsec та автентифікації потоків, якими обмінюється інформаційна система виконавця.

e) До анклаву збору даних слід застосовувати гігієну інформаційних технологій на основі загальних довідкових настанов,таких як настанова Франції "Guide d'hygiène informatique" [i.8], Настанова США «Критичний контроль безпеки CIK для ефективного кіберзахисту» [i.9] або такі стандарти як ISO/IEC 27002 [4].

i) Виконавець повинен управляти та використовувати пристрої, розміщені в анклаві збору даних з зон адміністрування та функціонування інформаційної системи служби виявлення інцидентів відповідно (див. вимогу 5.3.8.b).

j) Виконавець за жодних обставин не повинен мати прав на пристрій фільтрування міжанклавом збору даних та внутрішньою інформаційною системою замовника послуг, якщо така існує (див вимога 5.3.14.l).

l) Поділ анклаву збору даних повинен здійснюватися за допомогою:

- пристрою фільтрування між цим анклавом та інформаційною системою безпеки виконавця для виявлення інцидентів;
- пристрою фільтрування між цим анклавом та внутрішньою інформаційною системою замовника послуг (лише для просунутого та повного рівня впровадження).

m) Для просунутого та повного рівня впровадження, пристрій фільтрування між цим анклавом збору даних та внутрішньою інформаційною системою замовника послуг повинен забороняти всі потоки, крім тих, що мають контрольований периметр і забезпечують можливість:

- джерел збору, розміщених на контрольованому периметрі, обмінюватися подіями з цією зоною;
- деяким пристроям у цій зоні надсилати командні дії іншим пристроям виявлення на контрольованій інформаційній системі;
- у доцільних випадках, централізованим довідковим документам замовника послуг автоматично вносити файли довідкової інформації, що належать до власної інформаційної системи на ретрансляційній станції.

ПРИКЛАД: База даних управління конфігурацією.

p) Проміжний блок збору даних повинен впроваджуватися під відповідальність замовника послуг, якщо джерела збору не можуть передавати події безпосередньо пристроям збирання даних у зоні збору.

q) Пристрій фільтрування між анклавом збору даних та інформаційною системою виконавця

виявлення інцидентів безпеки повинен блокувати всі потоки, за винятком:

- потоків, що походять з цього анклаву збору даних в інформаційну систему безпеки виконавця виявлення інцидентів, і які лише дозволяють передавати події та основні інформаційні файли, передані замовником послуг з цього анклаву до зони збору. Виконавець повинен максимально обмежити кількість потоків, що дозволяють події та файли цього анклаву для передачі до інформаційної системи служби виявлення;
- потоків, що походять з цього анклаву збору даних в інформаційну систему системи безпеки виконавця служби виявлення інцидентів, та які дозволяють отримати доступ до деяких збережених подій безпеки за умови, що кібер ризики опановані виконавцем та прийняті замовником послуг;
- потоків, що дозволяють виконавцю керувати пристроями, розміщеними в цьому анклаві збору даних із зони адміністрування (див. вимогу 5.3.8.b);
- потоків, що дозволяють виконавцю використовувати пристрої, розміщених у цьому анклаві збору даних із зони функціонування (див. вимогу 5.3.8.b);
- потоків, що дозволяють оновлення пристроїв анклаву збору даних із зони оновлення (див вимогу 5.3.8.b).

r) У анклаві збору даних можна встановити ретрансляційну станцію для автоматичної передачі основної інформації з внутрішньої інформаційної системи замовника послуг.

5.3.15 Зовнішній доступ

a) Виконавець повинен запровадити спеціальний шлюз із спеціальним захищеним протоколом, щоб надати доступ адміністраторам а операторам до Інтернету чи інших інформаційних систем.

ПРИКЛАД: Внутрішня інформаційна система виконавця.

c) Усі потоки, що виходять із шлюзу до Інтернету, повинні проходити через проксі-сервіс, за яким слідує окремий вихід в Інтернет, порівняно з тим, що використовується інформаційною системою замовника послуг.

f) Виконавець повинен проставляти позначку часу та реєструвати здійснені пошуки з відкритим вихідним кодом.

h) Журнали шлюзів повинні забезпечувати аналітичними інструментами служби виявлення інцидентів, пов'язаних з внутрішньою безпекою.

i) Збір журналів шлюзу повинен здійснюватися за допомогою однієї із зон обміну виявлення інцидентів.

j) Пристрій фільтрування між Інтернетом або іншими інформаційними системами та шлюзом (див. вимогу 5.3.10.b) повинен блокувати всі потоки, крім:

- потоків, що походять від шлюзу до проксі-служби;
- потоків, що дозволяють шлюзу передавати журнали подій до зони обміну служби внутрішнього виявлення інцидентів.

5.3.16 Віддалений доступ

a) У разі віддаленого доступу до інформаційної системи служби виявлення аварійних ситуацій, виконавець повинен встановити:

- *як мінімум* шлюз адміністрування та функціонування для пристроїв служби виявлення;
- у доцільних випадках, шлюз, призначений для віддаленого доступу замовника послуг до зони обміну замовника послуг, яка відокремлена від шлюз (шлюзів) адміністрування та функціонування.

b) У випадку, якщо надано доступ до зони обміну замовника послуг через віддалені консультаційні робочі станції, Виконавець, разом із замовником послуг, повинен вказати в договорі про надання послуг

обов'язки, що стосуються:

- права власності на віддалені консультаційні робочі станції;
- управління та оновлення цих пристроїв;
- дотримання відповідності заходам безпеки, визначеним у вимозі 5.3.16.1.

f) У разі використання унікального шлюзу для віддаленого доступу адміністраторами та операторами, Виконавець повинні впровадити рішення, що забезпечує суворий поділ між:

- потоками адміністрування з віддалених робочих станцій адміністрування до адміністративної зони;
- потоками функціонування з віддалених робочих станцій до зони функціонування.

g) Потоки між віддаленими робочими станціями та шлюзами повинні шифруватися за допомогою IPsec VPN шифрування та рішення для автентифікації.

h) Адміністратори, оператори та користувачі віддалених консультаційних робочих станцій повинні пройти автентифікацію за допомогою мінімум двох факторів.

j) Віддалені робочі станції повинні бути укріплені, налаштовані таким чином, щоб вони могли поєднуватися лише виключно із виділеним шлюзом віддаленого доступу через зашифроване та автентифіковане з'єднання IPsec VPN,
дозволяти лише використання знімних носіїв інформації, дозволених політикою безпеки інформаційних систем та мати повні диски, зашифровані за допомогою рішення для шифрування.

k) Виконавець повинен передбачити механізми оновлення та управління віддаленими робочими станціями в разі, якщо він постачає ці робочі станції замовнику послуг та управляє ними.

l) Виконавець повинен налаштувати рішення для фільтрування (див. вимогу 5.3.10.b) таким чином, щоб вони дозволяли лише потоки, які:

- походять з робочих станцій віддаленого адміністрування в зону адміністрування (див. вимогу 5.3.8.b);
- походять з віддалених робочих станцій в зону функціонування (див. вимогу 5.3.8.b);
- походять із віддалених консультаційних робочих станцій до зони обміну замовника послуг (див. вимогу 5.3.8.b);
- походять із зони адміністрування (див. вимогу 5.3.8.b) до віддалених робочих станцій для управління
робочими станціями, які вона постачає та управляє;
- походять із віддалених робочих станцій в зону оновлення (див. вимогу 5.3.8.b) для оновлення робочих станцій, які вона постачає та управляє.

5.4 Організація виконавця, що використовує ЦОБ (SOC) та Управління

5.4.1 Кодекс етики та найму

a) Виконавець повинен перевірити підготовку, кваліфікацію та рекомендації щодо працевлаштування кандидатів
служби виявлення та правдивість їхніх автобіографій, перш ніж наймати їх роботу.

b) Виконавець повинен вимагати від заявників надати докази того, що вони не мають судимості.

d) Виконавець повинен мати кодекс етики, що є частиною його внутрішніх положень, який передбачає, зокрема, що:

- послуги надаються лояльно, розсудливо та неупереджено;
- працівники використовують лише ті методи, засоби та техніки, які були схвалені виконавцем;
- працівники зобов'язуються не розголошувати інформацію будь-якій третій особі, навіть якщо вона

знеособлена та розглядається поза контекстом, яка була отримана або створена як частина послуги, без офіційного письмового дозволу замовника послуг;

- працівники зобов'язуються попереджати виконавця про всі очевидно незаконні матеріали, виявлені під час надання послуги;
- працівники зобов'язуються дотримуватись відповідного чинного законодавства та норм та рекомендованих стандартів, пов'язаних з їхньою діяльністю.

e) Виконавець повинен забезпечити, щоб перш ніж почати надання послуг, усі його працівники підписали кодекс етики, згаданий у попередній вимозі.

f) Виконавець повинен забезпечити відповідність кодексу етики та передбачити дисциплінарні стягнення для операторів, адміністраторів та експертів служби виявлення, які порушили правила безпеки або положення кодексу етики.

g) Виконавець повинен розробити та впровадити план підвищення обізнаності своїх працівників стосовно безпеки інформаційної системи та пов'язаних із нею заходів безпеки, а також відповідного чинного законодавства та правил, що стосуються послуги виявлення інцидентів.

5.4.2 Організація та управління професійними якостями

a) Виконавець повинен мати команду, яка:

- забезпечує виконання, як мінімум, завдань, описаних у додатку A;
- має навички, пов'язані з цими завданнями.

b) Виконавець повинен визначити та офіційно задокументувати вичерпний перелік:

- функціональних обов'язків адміністратора для послуги виявлення інцидентів безпеки та супутніх завдань;
- функціональних обов'язків оператора для послуги виявлення інцидентів безпеки та супутніх завдань.

Цей перелік повинен включати *щонайменше* функціональні обов'язки оператора-аналітика та адміністратора інфраструктури (див. додаток A).

Виконавець повинен довести сумісність між різними функціональними обов'язками оператора та різними функціональними обов'язками адміністратора, зокрема щодо ресурсів, до яких здійснюється доступ, відповідно до принципів надання найменших прав та необхідності володіння інформацією.

c) Виконавець повинен працевлаштовувати достатню кількість працівників і може використовувати субпідряд (див п. 5.5.3.7 «Субпідряд»), щоб гарантувати, що надана послуга є належної якостіу всіх відношеннях.

d) Виконавець повинен створити та впровадити план навчання, розроблений для використання командою, що надає послуги виявлення, та який адаптований до її завдань.

e) Виконавець повинен написати та надати працівникам настанови щодо функціонування та адміністрування пристроїв послуги виявлення інцидентів.

f) Виконавець повинен запровадити мобілізаційну систему, яка дозволяє мобілізувати частину його команди поза робочим часом.

g) Виконавець повинен мати серед своїх послуг Команду реагування на комп'ютерні надзвичайні події або мати підписку на таку послугу.

i) Виконавець повинен надавати замовнику послуги віддалену підтримку, яка дозволяє,

зокрема:

- замовнику послуг повідомити виконавця про підозру чи підтвердження інциденту безпеки;
- виконавцю допомогти замовнику послуг вирішити виробничі проблеми, пов'язані з пристроями, якими управляє виконавець;
- виконавцю надавати допомогу та консультації замовнику послуг.

j) Виконавець повинен забезпечити доступ до служби підтримки через номер телефону або електронну адресу.

l) Виконавець повинен призначити особу, яка буде контактною особою

замовника послуг. Ця особа є основною контактною особою щодо операційного функціонування послуги виявлення інцидентів безпеки
та моніторингу виявлених інцидентів безпеки. Виконавець повинен повідомляти
замовника послуг про будь-які зміни контактної особи з питань послуги виявлення інцидентів безпеки.

m) Замовник послуги повинен призначити контактну особу з питань послуги виявлення інцидентів безпеки.

n) Особи, що виконують функції контактних осіб, повинні брати участь в операційних та стратегічних засідання комітетів, зазначених у пункті 5.4.3.

5.4.3 Операційні та стратегічні комітети

5.4.3.1 Операційний комітет

а) Виконавець повинен створити та головувати на засіданні операційного комітету, у присутності замовника послуги, *щонайменше* раз на квартал.

в) Операційний комітет повинен обговорювати *щонайменше* такі теми:

— загальна оцінка послуги виявлення інцидентів безпеки:

- огляд функціональних показників (див. пункт 5.5.1) відповідно до циклу огляду для кожного показника, погоджений із замовником послуг;
- огляд виявлених інцидентів безпеки;
- огляд стратегій збирання даних, аналізу та звітності;
- огляд переліку правил виявлення (див. вимогу 5.2.1.i);
- огляд оновлення статусу правил виявлення (див. вимогу 5.2.1.j);

— обсяг послуги виявлення інцидентів безпеки:

- огляд середовища замовника послуг;
- огляд змін, що впливають на інформаційну систему замовника послуг;
- презентація розвитку будь-яких проектів, що впливають на обсяг послуги;
- перегляд переліку загрозливих інцидентів безпеки;

- можливі вдосконалення послуги виявлення інцидентів безпеки:
  - огляд показників якості (див. пункт 5.5.1) відповідно до циклу огляду для кожного показника, погодженого з замовником послуги;
  - аналіз операційних змін у послузі виявлення засобів безпеки (вдосконалення засобів, зміни операційних процесів тощо);
  - презентація правил виявлення, які були створені, змінені або скасовані.

d) Виконавець повинен готувати звіт після кожного засідання операційного комітету та надсилати його замовнику послуг для затвердження. Цей звіт повинен містити *якнайменше* перелік учасників, рішення, прийняті на засіданні комітету, та відповідний план дій.

e) Виконавець повинен захищати звіт операційного комітету, зокрема щодо конфіденційності, беручи до уваги рівень чутливості або класифікацію його змісту.

f) Виконавець повинен зберігати та архівувати носії інформації операційного комітету та відповідні звіти у конкретному місці в інфраструктурі послуги виявлення, з логічним розподілом даних, *якнайменше*, між замовниками послуг.

5.4.3.2 Стратегічний комітет

а) Виконавець повинен організувати та головувати на засіданні стратегічного комітету у присутності

представників вищого керівництва замовника послуг *принаймні* раз на рік.

c) Стратегічний комітет повинен розглядати *щонайменше* такі теми:

- огляд стратегічних показників (див. пункт 5.5.1);
- перегляд договору про надання послуг;
- огляд плану зворотності;
- короткий виклад ефективності послуги виявлення;
- огляд та прогнози загроз.

d)

e) Виконавець повинен готувати звіт після кожного засідання стратегічного комітету та надсилати його замовнику послуг для затвердження. Цей звіт повинен містити *якнайменше* перелік учасників та

f) рішення, прийняті на засіданні комітету.

Виконавець повинен захищати звіт стратегічного комітету, зокрема щодо конфіденційності, беручи до уваги рівень чутливості або класифікацію його змісту.

5.5 Виконавець повинен зберігати та архівувати носії інформації стратегічного комітету та відповідні звіти у конкретному місці в інфраструктурі послуги виявлення, з логічним розподілом даних, *якнайменше*, між замовниками послуг.

5.5.1 Якість та рівень послуг

b)

Якість послуг

c) Виконавець повинен розробити та впровадити процес використання обізнаності щодо виявлених інцидентів безпеки з метою постійного підвищення ефективності послуги виявлення інцидентів.

e) Виконавець повинен визначити разом із замовником операційні та стратегічні показники для послуги виявлення інцидентів безпеки, застосовуючи, зокрема, ETSI GS ISI 001-1 [1].

Виконавець повинен встановити *як мінімум* такі показники операційної діяльності:

- Управління підтримкою інфраструктури послуги виявлення:
  - ступінь заповнення систем зберігання інцидентів;
  - залишок потужності систем зберігання інцидентів;
  - рівень доступності технічних пристроїв послуги виявлення:
    - веб-портал зони обміну замовника послуги;
    - пристрій анклаву збору даних;
    - система надсилання повідомлень про інциденти;
    - засоби технічного аналізу;
    - тощо

— Управління безпекою взаємозв'язків послуги виявлення БІ:

- кількість невдалих та успішних спроб автентифікації, а також відповідний детальний перелік щодо:
  - доступу до зони обміну замовника послуги;
  - доступ з віддалених робочих станцій;
  - доступ з робочих станцій віддаленого адміністрування.

— Управління можливостями виявлення:

- кількість виявлених попереджень щодо безпеки за місяць;
- кількість підтверджених інцидентів після кваліфікації на місяць;
- кількість правил виявлення, реалізованих в засобах технічного аналізу;

- кількість правил виявлення, створених, змінених або скасованих на місяць, за походженням запиту (діяльність щодо моніторингу за запитом замовника тощо);
- класифікація 20 найбільш спрацьованих правил виявлення.

— Управління інцидентами:

- кількість нових тікетів (зареєстрованих запитів), відкритих на місяць;
- кількість тікетів (зареєстрованих запитів) про інциденти безпеки, закритих на місяць;
- кількість відкритих тікетів (зареєстрованих запитів), накопичених за місяць;
- мінімальний, середній та максимальний час між створенням та закриттям тікета (зареєстрованого запиту);
- кількість інцидентів, створених відповідно до критичності інциденту.

— Управління подіями:

- кількість подій, не визнаних і, отже, не врахованих засобами технічного аналізу;
- ступінь подій, що не визнаний а, отже, не врахований засобами технічного аналізу;
- кількість джерел збору даних на тип вихідного обладнання;
- кількість пристроїв збирання даних;
- кількість подій, зібраних за день та місяць;
- кількість подій, зібраних пристроєм збирання даних за день та місяць;
- кількість подій, що надсилаються до системи зберігання за день та місяць;
- ступінь заповнення кожної із систем зберігання подій, включаючи пристрої збирання даних в анклаві;
- залишок ємності кожної із систем зберігання подій, включаючи пристрої збирання даних в анклаві;
- утримуюча здатність пристроїв збирання даних, якщо зв'язок неможливий (наприклад, коли зв'язок з мережею розірваний) із пристроєм збирання даних вищого рівня (за обсягом та часом).

— Управління звітністю:

- кількість облікових записів, яким надано доступ до веб-порталу та які можуть отримати доступ до інформації замовника послуг;
- кількість облікових записів доступу до веб-порталу, створених за місяць;
- кількість облікових записів доступу до веб-порталу, видалених за місяць.

f) Виконавець повинен встановити, *як мінімум*, такі показники операційної ефективності:

— Управління можливостями виявлення:

- середній час, необхідний для оновлення правил виявлення відповідно до запиту замовника;
- середній час, необхідний для пошуку показника компрометації під час *апостеріорного пошуку* в системі зберігання за типом показника компрометації.

— Управління інцидентами:

- середній час, необхідний для кваліфікації інцидентів, за типом інциденту та рівнем критичності.

— Управління подіями:

- мінімальний, середній та максимальний час між генеруванням події джерелом збирання даних та його зберіганням в системах зберігання подій.

— Управління звітністю:

- мінімальний, середній та максимальний час між виявленням події безпеки та наданням повідомлення про пов'язаний інцидент за рівнем критичності.

g) Виконавець повинен встановити, *як мінімум*, такі стратегічні показники:

— Управління безпекою взаємозв'язків послуги виявлення БІ:

- еволюція кількості відхилень та інцидентів, що спостерігаються щодо різних зовнішніх доступів до послуги виявлення БІ.

— Управління підтримкою інфраструктури послуги виявлення:

- щомісячний розвиток рівня доступності технічних пристроїв послуги виявлення:
  - веб-портал зони обміну замовника послуги;
  - пристрій анклаву збору даних;
  - система надсилання повідомлень про інциденти;
  - засоби технічного аналізу;
  - тощо

— Управління можливостями виявлення:

- виявлені відхилення стосовно різних Договорів про рівень послуг.

— Управління інцидентами:

- еволюція середньої кількості часу, необхідної для обробки тікетів (зареєстрованих запитів) про інциденти, за рівнем критичності, на місяць;
- зміна кількості відкритих накопичених тікетів (зареєстрованих запитів) про інциденти, за рівнем критичності, на місяць;
- кількість підтверджених інцидентів на місяць у межах послуги виявлення замовника послуги.

— Управління подіями:

- зміна рівня покриття збирання даних журналів для обладнання, визначеного в стратегії збирання.

h) Виконавець повинен встановити та постійно оновлювати процес оцінки показників, який для кожного з описаних операційних та стратегічних показників описує методи та засоби, що використовуються виконавцем для оцінки показника.

5.5.2 Оборотність

a) Виконавець повинен розробити разом із замовником план зворотності для послуги виявлення інцидентів безпеки, що дозволяє відновити послугу замовником або іншою виконавцем послуги.

b) План зворотності повинен містити *щонайменше* такі елементи:

- повний перелік інформації та матеріалів, що підлягають відновленню;
- тривалість зворотності;
- залучені люди та дії, які кожен з них повинен виконати;
- формати інформації, що підлягає відновленню;
- засоби відновлення.

Виконавець повинен мати можливість, якщо замовник послуги вимагає, відновити збережені події безпеки, разом із конкретними правилами виявлення, замовнику послуги.

c) Тривалість зворотності повинна становити *мінімум* три місяці.

e) Виконавець повинен підтримувати послугу виявлення аварійних ситуацій в робочому стані протягом реалізації плану зворотності.

f) Виконавець повинен знищити всю інформацію, що стосується замовника послуги наприкінці виконання плану зворотності, за винятком інформації, якою володіє замовник послуги, який надав йому право на її збереження (див. вимогу 5.5.3.4.a).

5.5.3 Договір про надання послуг

5.5.3.1 Умови надання послуги

а) Договір про надання послуг повинен:

- описувати обсяг та цілі послуги, що надається, послугу виявлення інцидентів безпеки, включаючи, зокрема, діяльність з управління подіями, інцидентами та наданням звітності;
- описувати технічні та організаційні заходи, що здійснюються виконавцем у межах виконання послуги;
- описувати місце зберігання та обробки даних, а також місце функціонування та адміністрування послуги виявлення;
- визначати кінцеві результати, які очікуються як частина наданої послуги, передбачуваних одержувачів та їхній рівень чутливості або класифікації, разом із пов'язаними з ними умовами;
- описувати способи зв'язку між виконавцем та замовником послуги, які будуть використовуватися в процесі надання послуги;
- визначати правила власності на об'єкти, що охороняються правом інтелектуальною власністю, такі як кінцеві результати, засоби та правила виявлення, спеціально розроблені виконавцем у межах наданняпослуги;
- описувати процес реєстрації та розгляду скарг на послуги, надані замовником послуги або третіми особами, а також процедури надання скарги.

5.5.3.2 Організація послуги

а) Договір про надання послуг повинен:

- передбачати, що Виконавець призначить контактну особу для замовника послуги, яка буде відповідати за забезпечення операційного моніторингу послуги;
- передбачати, що Виконавець та замовник послуги зазначать необхідну інформацію про імена та прізвища, посади, обов'язки, права та потреби осіб, які беруть участь у наданні послуги. Цей пункт є особливо важливим, якщо відбувся інцидент безпеки, який не повинен оприлюднюватися;
- передбачати, що Виконавець не залучає працівників, які не мають з ним договірних відносин, не підписав кодекс етики або був суб'єктом кримінального правопорушення;
- визначати, чи надає Виконавець віддалений доступ адміністраторів або операторів до інформаційної системи послуги виявлення інцидентів безпеки. 5.5.3.3 Обов'язки

а) Договір про надання послуг повинен:

- передбачати, що Виконавець інформує замовника послуг, у разі будь-яких недоліків у договорі про надання послуг;
- передбачати, що Виконавець інформує замовника послуг, у випадку, якщо виявлено інцидент безпеки в інформаційній системі послуги виявлення інцидентів безпеки, та максимальний дозволений час для передачі інформації після інциденту;
- передбачати, що Виконавець виконує лише ті дії, які чітко відповідають цілям послуги;
- передбачити, що замовник послуги має всі права власності та права доступу, необхідні для обсягу послуги (інформаційні системи, фізичні носії інформації тощо) або те, що він отримала згоду будь-якої третьої сторони, включаючи її виконавців послуг або партнерів, чиї інформаційні системи включені в обсяг послуги;
- передбачати, що замовник послуги відповідає всім правовим вимогам, необхідним для послуги та зокрема тим, що стосуються збирання та аналізу інформації;
- визначати обов'язки та запобіжні заходи, яких слід дотримуватися всім сторонам щодо

потенційних ризиків пов'язані із послугою, особливо щодо конфіденційності зібраної інформації та проаналізовано щодо доступності та цілісності інформаційної системи замовника послуги;

- передбачати, що виконавець має страхування професійної відповідальності, що покриває будь-яку шкоду, заподіяну замовнику послуг та, зокрема, його інформаційній системі в результаті його послуги, уточнюючи покриття страхування, включаючи страховий поліс;
- визначати відповідальність між виконавцем та замовником послуги щодо анклавів збирання даних в інформаційній системі замовника послуги відповідно до вимоги 5.3.14.b та 5.3.14.c;
- передбачати, що виконавець запровадив процедуру управління змінами для власної системи інформації;
- передбачати, що у виконавця є процес постійного підвищення ефективності його послуги виявлення, базуючись, зокрема, на операційних показниках, зазначених у пункті 5.5.1.

5.5.3.4 Конфіденційність та захист інформації

а) Договір про надання послуг повинен:

- визначати рівень чутливості або класифікацію послуги виявлення інцидентів безпеки, впровадженої виконавцем;
- визначати рівень чутливості або класифікацію контрольованого периметра;
- передбачати, що виконавець збирає та аналізує лише ту інформацію, яка суворо вимагається для безперебійного функціонування послуги;
- передбачати, що виконавець не розголошує будь-яку інформацію, що стосується послуги, третім особам без офіційного письмового дозволу замовника послуги;
- визначати пункти, що стосуються етичних вимог виконавця та включати кодекс етики виконавця;
- визначати умови доступу, зберігання, передачі, відтворення, знищення та відновлення інформації, яка збирається та аналізується виконавцем. За необхідності Виконавець разом із замовником повинен визначити терміни, відповідно до типів інформації:
  - передбачати, що виконавець може, крім випадків офіційної письмової відмови замовника послуги, зберігати певні типи інформації, що стосуються послуги, і що він вказує ці типи інформації (наприклад, виявлення: правила, зловмисне програмне забезпечення, сценарії атак, показники компрометації тощо);
  - передбачати, що виконавець знеособлює та виводить з контексту (видаляючи будь-яку інформацію, яка може бути використана для ідентифікації замовника, будь-яку інформацію особистого характеру тощо) інформація, на яку замовник надає дозвіл зберігати або передавати третій стороні;
  - передбачати, що виконавець, за винятком випадків письмової офіційної відмови замовника, передаватиме до місцевого органу захисту інформації знеособлену та виведену з контексту інформацію разом із рівнем чутливості та умовами використання;
  - передбачати, що виконавець повинен захищати дані, передані третій стороні, в конфіденційності відповідно до рівня чутливості або класифікації;
  - передбачати, що Виконавець наприкінці надання послуги знищує всю інформацію замовника послуги або протягом строку зберігання, залежно від того, що настає раніше, за винятком інформації, на яку замовник надав інструкцію зберігати;
- визначати повторюваність, з якою виконавець повинен перевіряти план резервного копіювання та відновлення послуги виявлення інцидентів безпеки.

5.5.3.5 Зворотність

а) Договір про надання послуг повинен визначати умови реалізації плану зворотності послуги: тривалість,впровадження, будь-які додаткові витрати тощо (див. пункт 5.5.2).

5.5.3.6 Закони та інші нормативно-правові акти

а) Договір про надання послуг повинен:

- зазначати законодавство, що регулює договір про надання послуг;
- зазначати технічні та організаційні заходи, що застосовуються виконавцем з метою дотримування чинного законодавства, зокрема того, що стосується:
  - персональних даних;
  - порушення довіри;
  - конфіденційності приватної кореспонденції;
  - медичної таємниці;
  - порушення приватності;
  - шахрайського доступу до або обслуговування в інформаційній системі;
  - професійної таємниці;
- визначати будь-які конкретні нормативно-правові вимоги, які поширюються на замовника послуги, зокрема, ті, що стосуються його сектору діяльності;
- встановлювати заходи, які повинні вживатися виконавцем в умовах судових, цивільних або арбітражних проваджень. У цьому випадку рекомендується звернутися до юриста;
- визначати термін зберігання інформації, що стосується послуги, зокрема щодо отриманих даних про події та виявлені інциденти безпеки. За необхідності можна розрізняти періоди зберігання за різними типами інформації. Мінімальний строк зберігання, згідно з європейським чинним законодавством та нормативно-правовими актами повинен бути:
  - шість місяців для отриманих даних про події;
  - весь строк тривалості послуги для інцидентів безпеки та для пов'язаного з ними контексту (пов'язані звіти про події) та кваліфікаційний аналіз та звіти.

5.5.3.7 Субпідряд

а) Договір про надання послуг повинен зазначати, що виконавець може, за необхідності, укладати домовленості щодо субпідряду щодо всієї або частини послуги з іншим виконавцем за умови, що:

- між виконавцем та субпідрядником укладено договір про надання послуг;
- використання умов субпідряду відоме і офіційно прийняте замовником у письмовій формі ;
- субпідрядник відповідає вимогам цього документа.

5.5.3.8 Рівень послуги

а) Договір про надання послуг повинен:

- визначати операційні та стратегічні показники, що використовуються для оцінки рівня послуги;
- визначати операційні години послуги виявлення інцидентів безпеки;
- передбачає, що Виконавець повинен проводити засідання операційного та стратегічного комітетів у присутності замовника послуги;
- визначити цілі та періодичність таких засідань комітету;
- визначати для виконавця та замовника рівень людських ресурсів, які спрямовано на управління правилами виявлення і, зокрема, їхнє створення і внесення змін;
- визначати повторюваність, з якою виконавець передає замовнику звіт про статус правил виявлення ;
- передбачити, що виконавець повинен забезпечувати замовнику доступ до служби підтримки та години, протягом яких ця служба підтримки працюватиме;
- зазначати тип служби підтримки (телефон, електронна пошта тощо), її доступність та рівень

чутливості або класифікацію інформації, якою можна обмінюватися;

- визначати рівень компетентності співробітників, які чергують, відповідно до потреб замовника послуги, і в разі запровадження обслуговування за викликом.

Додаток А (інформативний):

Завдання та вміння працівників виконавця ЦОБ

А.1 Оператор-аналітик

А. 1 .1 Завдання

- виявлення, аналіз та кваліфікація інцидентів безпеки;
- надання підтримки групам розслідування у процесі врегулювання інцидентів.

А. 1.2 Вміння

- знання протоколів та архітектур мережі;
- досвід аналізу журналів (систем або додатків);
- знання безпеки інформаційних систем;
- навички аналізу мережевого трафіку;
- оволодіння діловими функціональними можливостями послуги виявлення, включаючи пошук подій у системи зберігання подій.

А.2 Адміністратор інфраструктури

А.2.1 Завдання

- управління пристроями технічної інфраструктури послуги виявлення інцидентів безпеки;
- підтримка пристроїв технічної інфраструктури послуги виявлення інцидентів в робочих умовах;
- оновлення та підтримка пристроїв технічної інфраструктури послуги виявлення інцидентів у безпечних умовах.

А.2.2 Навички

- управління пристроями для послуги виявлення інцидентів безпеки, особливо тих, що пов'язані з подією, інцидентом та управлінням звітністю.

А.3 Експерт з архітектури

А.3.1 Завдання

- проектування та ведення архітектури послуги виявлення;
- інтеграція або розробка та обслуговування компонентів послуги виявлення;
- інтеграція або розробка та ведення нових механізмів кореляції подій.

А.3.2 Навички

- робота з датчиками та знання засобів кореляції журналу подій;
- володіння вміннями управління типовими протоколами фунціонування послуги;
- добре знання найпоширеніших програм та їхню безпеку (веб-сервери, поштові сервери, бази даних сервери, DNS-сервери, проксі-сервери, брандмауери тощо);
- добре знання архітектури глобальної мережі та безпеки її компонентів (маршрутизаторів, комутаторів тощо).

A.4 Експерт із збирання та аналізу журналів

A.4.1 Завдання

- сприяння визначенню та перегляду стратегії збирання;
- участь у визначенні політики замовника ведення журналу у сфері обліку за типом обладнання (операційні системи,
  послуги інфраструктури, мережеве обладнання, обладнання безпеки тощо);
- надання підтримки адміністраторам інфраструктури при розгортанні систем виявлення (тестування, обслуговування
  системи в робочому стані, підтримка аналітиків, що використовують ці системи тощо);
- участь у розробці та підтримці механізмів та правил кореляції подій.

A.4.2 Навички

- поглиблені знання про аналіз журналів подій системи, мережі та додатків;
- знання засобів та прийомів кореляції журналу подій;
- знання журналу аналізу або систем моніторингу безпеки (інформація про безпеку та управління подіями —
  SIEM).

A.5 Експерт з виявлення інцидентів

A.5.1 Завдання

- розширення внутрішніх баз знань із використанням інформації про загрози, вразливості та шкідливий код;
- управління правилами виявлення протягом їхнього життєвого циклу (концепція, впровадження, документація,
  зміна, відключення тощо);
- забезпечення постійного вдосконалення процесів надання послуг.

A.5.2 Навички

- знання вразливостей;
- знання протоколів управління та контролю;
- знання операційних режимів атак та шкідливих кодів;
- досвід у розробці засобів правил виявлення.

A.6 Менеджер з питань прав доступу

A.6.1 Завдання

- управління створенням та деактивацією облікових записів для операційних засобів послуги;
- управління присвоєнням, змінами та видаленням прав доступу до операційних засобів послуги.

A.6.2 Навички

- майстерність в управлінні операційними засобами послуги;
- знання ролей послуги виявлення та супутніх прав.

Додаток B (інформативний):

Рекомендації для замовників послуги

B.0 Вступ

У цьому додатку наведені рекомендації замовників стосовно послуги виявлення інцидентів безпеки.

B.1 До початку надання послуги

a) Рекомендується, щоб замовник послуги призначив особу, яка буде виконувати функції внутрішнього операційного координатора, відповідального за те, що він є основною контактною особою з замовником стосовно операційного функціонування послуги виявлення інцидентів безпеки та для моніторингу виявлених інцидентів безпеки.

b) Рекомендується, щоб замовник зберіг затвердженого постачальника аудиторських послуг із забезпечення безпеки інформаційної системи для проведення оцінки ризиків з метою складання переліку можливих інцидентів безпеки і пов'язаних з ними наслідків (див. вимогу 5.2.1.a), за якими проводиться збирання даних; розробка стратегій аналізу та звітності.

c) Рекомендується, щоб замовник оновлював свою оцінку ризику щоразу, коли відбувається зміна його інфраструктури або послуг, і що він повідомляє про ці зміни та їхні наслідки виконавцю.

d) Рекомендується, щоб замовник зазначив у договорі про надання послуг будь-які конкретні юридичні та нормативні вимоги, які поширюються на нього, включаючи ті, що стосуються його сектору діяльності.

e) Рекомендується, щоб замовник вимагав від виконавця частоти проведення засідань операційного комітету (див. пункт 5.4.3.1), що повинне бути зазначене в договорі про надання послуг, один раз на квартал.

f) Рекомендується, щоб замовник вимагав від виконавця частоти проведення засідань стратегічного комітету (див. пункт 5.4.3.2), що повинне бути зазначене в договорі про надання послуг, один раз на рік.

g) Рекомендується, щоб замовник вимагав від виконавця частоти оновлення статусу правила виявлення (див. вимогу 5.2.1.j), що повинне бути зазначене в договорі про надання послуг, один раз на місяць.

h) Рекомендується, щоб замовник обирав стратегічні та операційні показники, які слід зазначати в договорі про надання послуг, і які дозволяють оцінити рівень послуг, що надаються послуга серед показників ETSI GS ISI 001-1 [1].

i) Рекомендується, щоб замовник застосовував ETSI GS ISI 002 [3] для визначення формату та змісту тікетів про інцидент безпеки.

j) Рекомендується, щоб замовник вимагав від виконавця включення до стратегії збирання даних (див. вимогу 5.2.2.a) розгортання апаратного засобу для збирання інформації на кожному з взаємозв'язків його системи інформації, і, зокрема, такі взаємозв'язки з:

- Інтернетом;
- сторонніми інформаційні системи (партнерами, субпідрядниками тощо);
- іншими системами інформації замовника з нижчим або більш вразливим захистом класифікації або рівня чутливості.

l) Замовнику рекомендується:

- синхронізувати джерела збору, розміщені в його інформаційній системі, з одним джерелом часу;
- розробити та впровадити політику ведення журналу подій.

m) Замовнику рекомендується запровадити процес антикризового управління на випадок виявлення серйозного інциденту безпеки в його інформаційній системі.

n) Замовнику рекомендується вимагати від виконавця інтеграції конкретних звітів у стратегію звітності (див. вимогу 5.2.3.f), у разі виявлення серйозних інцидентів безпеки в межах їїінформаційної системи.

o) Замовнику рекомендується застосовувати гігієну інформаційних технологій для доступу до вуб-порталу, на основі загальних довідкових настановах, таких як французька " Guide d'hygiène informatique " [i.8], Настанова США «Критичний контроль безпеки СІК для ефективного кіберзахисту"»[i.9] або такі стандарти як ISO / IEC 27002 [4].

B.2 Під час надання послуги

a) Замовнику рекомендується регулярно передавати інформацію виконавцю протягом усього періоду надання послуги, всю інформацію, необхідну для створення виконавцем нових правил виявлення, що відповідають потребам замовника.

b) З цією метою замовник, може, зокрема, надати результати тестів на вразливість та вторгнення, що проводяться у його інформаційній системі.

c) Замовнику рекомендується інформувати виконавця про будь-які зміни його інформаційної системи, які може вплинути на ефективність послуги виявлення інцидентів безпеки.

d) Замовнику рекомендується запровадити процес управління змінами, що дозволятиме його постійно інформувати виконавця про будь-які зміни в його контрольованій інформаційній системі (конфігурація, налаштування, версії програмного забезпечення тощо).

Додаток C (інформативний):

Визначення базового рівня реалізації

У таблиці C.1 описується базовий рівень реалізації цього документа (комплект).

Таблиця C.1

Вимога	Базовий рівень (комплект)
Пункт 5.1	
a, b, c	X
d	
f, g, h, i, k	X
l, m	
n	X
Пункт 5.2.1	
a, c	X
d, f	
g	X
h, i, j, m, n	
q	X
r, s, t	
v, w	X
x	X
y, z, aa, bb, cc, dd, ee	X
Пункт 5.2.2	
a, b, c	X
f	
g	X
h	
i, n, o, r, s, t	X
u, v	
w	X

Пункт 5.2.3	
a	X
b	
c, d, e, f, h, j, k	X
l	
Пункт 5.3.1	
a, c, e	X
Пункт 5.3.2	
b	X
Пункт 5.3.3	
a	X
Пункт 5.3.4	
a, b, c, e, f, h, i	X
Пункт 5.3.5	
a, b	X
c	
Пункт 5.3.6	
a, b	X
Пункт 5.3.7	
a, c, h	
Пункт 5.3.8	
a, b, c, d, e, f, g	X
Пункт 5.3.9	
a, b, c	X
d	
e	X
f, g	
h, i, j, l	X
Пункт 5.3.10	
a, b, c, e	X

Вимога	Базовий рівень (комплект)
Пункт 5.3.11	
a, b, c, d, e	
Пункт 5.3.12	
b	
Пункт 5.3.13	
a, b, c, e, f, g, h	
Пункт 5.3.14	
a, b, c, e, i, j	X
l, m, p, q, r	
Пункт 5.3.15	
a, c, i	X
f, h, i	
Пункт 5.3.16	
a, f, g, h, j, l	X
b	
Пункт 5.4.1	
a, b, d, e, f, g	X
Пункт 5.4.2	
a, b, c, d, e	X
f	
g, i, i, l, m, n	X
Пункт 5.4.3.1	
a, c, d, e, f	
Пункт 5.4.3.2	
a, c, d, e, f	X
Пункт 5.5.1	
b, c, e	X
h	
Пункт 5.5.2	
a, b, c, d, e, f	X
Пункт 5.5.3	
1a, 2a, 3a, 4a, 5a, 6a, 7a, 8a	X

Додаток D (інформативний):

Автори та учасники

Під час підготовки цього документу взяли участь такі особи:

Доповідач:

Жерар Годен (Gerard Gaudin) , G²C , Голова ISG ISI

Інші учасники:

Герве Дебар (Herve Debar),Institut Telecom, Заступник Голови ISG ISI

Арно Філлетт (Arnaud Fillette), Thales, секретар ISG ISI

Та в алфавітному порядку:

Ян ДеМер (Jan deMeer), SmartSpaceLabs.eu

Аксель Реннок (Axel Rennoch), Fraunhofer Fokus

Філіп Сааде (Philippe Saade), ESI-Group

Жульєн Сажо (Julien Saugeot), BNP Paribas

Історія

Історія документів		
V1.1.1	Грудень 2018	Публікація