International Science Journal of Engineering & Agriculture
2023; 2(6): 12-22
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20230206.02
ISSN: 2720-6319

INTERNATIONAL SCIENCE GROUP

Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об’єктів критичної інфраструктури

Олексій Скіцько
Центр кібербезпеки, НА СБ України, Київ, Україна
ORCID 0000-0003-4122-0889

Роман Ширшов
Центр кібербезпеки, НА СБ України, Київ, Україна
ORCID 0000-0003-3534-8736

Для цитування цієї статті:
Скіцько Олексій, Ширшов Роман. Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об’єктів критичної інфраструктури. International Science Journal of Engineering & Agriculture. Vol. 2, No. 6, 2023, pp. 12-22. doi: 10.46299/j.isjea.20230206.02
Надійшла до редакції: 01 листопада 2023 р.; **Схвалено:** 30 листопада 2023 р.;
Опубліковано: 01 грудня 2023 р.

Анотація: Стаття присвячена дослідженню системи управління інформаційною безпекою як інструменту підвищення рівня захищеності та ефективності об’єктів критичної інфраструктури. В результаті порівняльного аналізу аналогічних рішень визначено найбільш оптимальні методи і підходи до управління інформаційною безпекою, що сприятимуть підвищенню рівня захищеності та ефективності об’єктів критичної інфраструктури. Здійснено аналіз методів та підходів до управління інформаційною безпекою на об’єктах критичної інфраструктури.

Ключові слова: Система управління інформаційною безпекою, Рівень захищеності, Ефективність, Об’єкт критичної інфраструктури, Аналіз, Порівняльний аналіз, Методи, Підходи, Оптимальність.

1. Вступ

На більшості об’єктів критичної інфраструктури (далі – ОКІ, підприємство) сьогодні широко використовуються інформаційні технології. Зберігання, обробка та передача інформації відбувається через комп'ютерні системи та мережі. В разі порушення безпеки цих систем може виникнути зупинка технологічних процесів, втрата даних та інші втрати (фінансові, авторитетність). Система управління інформаційною безпекою (далі – СУІБ) допомагає забезпечити надійну та безпечну роботу інформаційних систем. Застосування СУІБ підвищує ефективність підприємства. Захист від кіберзагроз та витоку інформації дозволяє уникнути фінансових та репутаційних втрат, забезпечує стале функціонування об’єкту критичної інфраструктури. Крім того, оптимальне використання ресурсів та зменшення ризиків впливає на ефективність функціонування об’єкта критичної інфраструктури.

2. Об’єкт і предмет дослідження

Об’єкт дослідження – процес дослідження, який спрямований на вивчення та аналіз різних аспектів процесу забезпечення інформаційної безпеки, включаючи методології, інструменти,

комунікацію, управління ризиками та якість продукту. Предмет дослідження – методи, підходи та інструменти управління інформаційною безпекою на підприємстві.

3. Мета та задачі дослідження

Метою дослідження є аналіз теоретичних положень і практик діяльності систем управління інформаційною безпекою та розробка рекомендацій та стратегій для підвищення ефективності СУІБ з метою забезпечення захисту даних та запобігання можливим загрозам безпеки.

Ефективна СУІБ об'єкта критичної інфраструктури знизить ризики втрати інформації, порушення конфіденційності та іншої шкоди, що сприятиме уникненню можливих загроз і вразливостей, забезпечуючи стабільну та безпечну роботу об'єкта. У відповідності з метою дослідження поставлені наступні завдання:

- Проаналізувати сучасний стан систем управління інформаційною безпекою на підприємствах та визначити проблеми та виклики, з якими вони зіштовхуються.
- Дослідити існуючі методи та підходи до управління інформаційною безпекою.
- Розробити модель системи управління інформаційною безпекою, що сприяє підвищенню ефективності та рівня захищеності підприємства.
- Запропонувати рекомендації щодо впровадження та оптимізації системи управління інформаційною безпекою.
- Зробити висновки щодо впливу системи управління інформаційною безпекою на ефективність та рівень захищеності підприємства та сформулювати рекомендації для подальшого вдосконалення.

4. Методи дослідження

Методи дослідження: аналіз літературних джерел, емпіричні дослідження, порівняльний та статистичний аналіз.

5. Огляд існуючих підходів до управління інформаційною безпекою та їх вплив на ефективність та рівень захищеності.

Існуючі підходи до управління інформаційною безпекою та їх вплив на ефективність діяльності ОКІ є важливою складовою безпеки. Наведемо деякі підходи до управління інформаційною безпекою та їх вплив на діяльність об'єкта критичної інфраструктури [1]:

1. Загальний підхід до управління ризиками: передбачає визначення потенційних ризиків для інформаційної безпеки та прийняття заходів щодо зниження цих ризиків. Впровадження такого підходу може покращити ефективність та захищеність ОКІ, оскільки дозволяє ідентифікувати найбільш критичні ризики та спрямовувати ресурси на їх усунення.
2. Підхід з урахуванням технологічних-процесів: полягає в інтеграції заходів забезпечення інформаційної безпеки в технологічні-процеси ОКІ. Це дозволяє забезпечити безпеку інформації без значного впливу на ефективність технологічних-процесів. Сприяє оптимізації використання ресурсів та зниженню затрат на захист інформації.
3. Стандартизований підхід: використання стандартів і рамок управління інформаційною безпекою, таких як ISO 27001, дозволяє впроваджувати систематичний підхід до забезпечення безпеки інформації. Забезпечує стандартизацію процесів, поліпшує контроль і сприяє ефективному використанню ресурсів.
4. Система неперервного вдосконалення: підхід, спрямований на постійне вдосконалення системи управління інформаційною безпекою на основі аналізу результатів та введення коректив. Це дозволяє виявляти слабкі місця та недоліки в системі та вчасно їх усувати, що сприяє забезпеченню ефективності та економічності заходів інформаційної безпеки.

Одним з ключових аспектів у сфері захисту інформації є організаційно-управлінська діяльність, яка займає важливе місце в комплексі заходів з інформаційної безпеки. Цей аспект є одним з чотирьох основних напрямків у загальній системі заходів і включає в себе використання спеціалізованого програмного забезпечення, виготовлення та використання спеціальних апаратних засобів, а також вдосконалення криптографічних методів захисту інформації (рис. 1.) [2].

Рисунок 1. Організаційна структура діяльності в галузі інформаційної безпеки.

Вплив цих підходів на захищеність та ефективність може бути різним в залежності від конкретних умов і контексту. Однак, взагалі, правильно розроблена та ефективно впроваджена система управління інформаційною безпекою сприяє зниженню ризиків [3], збільшенню надійності та довіри, оптимізації використання ресурсів та забезпеченню стійкого розвитку ОКІ.

6. Принципи та цілі системи управління інформаційною безпекою

Система управління інформаційною безпекою (СУІБ) базується на декількох принципах та має на меті досягнення певних цілей. Нижче наведено загальні принципи та цілі, які відображаються в СУІБ [4]:

Принципи:

- Цілісність: система управління інформаційною безпекою повинна забезпечувати цілісність інформаційних ресурсів, тобто захищати їх від несанкціонованого доступу, модифікації та знищення.
- Конфіденційність: СУІБ повинна гарантувати конфіденційність інформації, що зберігається та обробляється в інформаційних системах ОКІ, шляхом обмеження доступу до неї тільки авторизованим особам.
- Надійність: система повинна забезпечувати надійність інформаційних процесів та систем, що використовуються в ОКІ, шляхом застосування відповідних заходів безпеки та резервування.
- Доступність: СУІБ повинна забезпечувати доступність інформації та ресурсів для авторизованих користувачів у встановлені терміни та в межах встановлених параметрів безпеки.

Для реалізації процесів Системи управління інформаційною безпекою (СУІБ) застосовується модель PDCA (Plan-Do-Check-Act) [5]. Модель PDCA (Plan-Do-Check-Act), також відома як цикл Демінга, є методологією управління, яка використовується для досягнення постійного вдосконалення процесів та результатів в організації. Ця модель складається з чотирьох основних етапів, які взаємодіють між собою:

- Plan (планування): визначаються цілі, стратегії та методи, які необхідні для досягнення бажаних результатів. Відбувається аналіз поточного стану, визначення завдань і розробка плану дій.

- Do (виконання): план реалізується шляхом впровадження запланованих дій. Здійснюються необхідні процеси та заходи для досягнення поставлених цілей.
- Check (перевірка): у цій фазі проводиться оцінка результатів виконаних дій. Здійснюється контроль, аналіз та оцінка зібраних даних для визначення того, наскільки були досягнуті поставлені цілі та якість виконаних процесів.
- Act (дія): на цьому етапі вживаються заходи для покращення результатів. На основі отриманих відомостей з перевірки вносяться необхідні зміни і коригуючі дії з метою вдосконалення процесів і досягнення кращих результатів. Цикл починається знову, і процес повторюється для подальшого вдосконалення.

Модель PDCA є ітеративною, що означає, що вона повторюється в циклах, дозволяючи постійно аналізувати та вдосконалювати процеси, досягати кращої ефективності [6] та якості, а також вирішувати виявлені проблеми. Вона застосовується в багатьох сферах управління, включаючи якість продукції, процеси безпеки, управління проектами та багато інших.

Побудова СУІБ дозволяє чітко визначити взаємозв'язані процеси та підсистеми інформаційної безпеки, визначити відповідальних за них, а також встановити необхідні фінансові та трудові ресурси для їх ефективного функціонування [7].

Основні функції СУІБ включають:

- Виявлення та аналіз ризиків інформаційної безпеки.
- Планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ.
- Контроль цих процесів.
- Внесення необхідних коригувань в процеси мінімізації інформаційних ризиків.
- Якісне управління інформаційною безпекою базується на таких принципах:
- Комплексний підхід, що охоплює всі компоненти інформаційної системи та актуальні ризикоутворюючі фактори.
- Узгодженість з бізнес-задачами і стратегією підприємства.
- Високий рівень керованості.
- Адекватність використовуваної та генерованої інформації.
- Ефективність, яка забезпечує оптимальний баланс між можливостями, продуктивністю і витратами СУІБ.
- Безперервність управління.
- Процесний підхід, що забезпечує зв'язок між етапами планування, впровадження, перевірки, аудиту та коригування.

У відповідності до ISMS Framework [8], який є європейським еквівалентом Системи управління інформаційною безпекою (СУІБ), розробленої міжнародною європейською агенцією з кібербезпеки, управління безпекою здійснюється за схемою (рис. 1.2). ISMS Framework включає в себе визначення політики безпеки, ідентифікацію ризиків, встановлення контрольних заходів, впровадження заходів безпеки, моніторинг та аудит інформаційної безпеки, а також постійне вдосконалення системи управління інформаційною безпекою [9].

Цей фреймворк допомагає організаціям визначити і розуміти свої інформаційні активи, ідентифікувати потенційні загрози та ризики, розробляти та впроваджувати ефективні контрольні механізми, а також забезпечити відповідність вимогам законодавства та регуляторних органів.

ISMS Framework (Information Security Management System Framework) - це систематичний підхід до управління інформаційною безпекою в організації. Він включає набір принципів, процедур, політик і практик, які спрямовані на захист інформації від ризиків та загроз, забезпечуючи конфіденційність, цілісність та доступність інформаційних ресурсів.

ISMS Framework базується на принципах континуального циклу PDCA (Plan-Do-Check-Act), що передбачає постійне планування, впровадження, перевірку та вдосконалення системи управління інформаційною безпекою. Це дозволяє організаціям адаптуватися до змін в

оточуючому середовищі, виявляти та вирішувати потенційні проблеми, забезпечуючи стійкий рівень захисту інформації.

Розробка системи управління інформаційною безпекою (СУІБ) включає шість етапів [10]:

- Визначення політики безпеки.
- Визначення області застосування СУІБ.
- Оцінка ризику як частина процесу управління ризиками.
- Управління ризиками.
- Вибір відповідних засобів контролю.
- Заява про застосовність.

Етапи 3 і 4, оцінка та управління ризиками, є основою СУІБ і представляють собою процеси, які перетворюють політику безпеки та цілі в конкретні плани реалізації контрольних засобів і механізмів, спрямованих на мінімізацію загроз і вразливостей. Важливо зазначити, що кроки 3 і 4 розглядаються як єдиний процес, а саме - управління ризиками.

Процеси і дії, пов'язані з кроками 5 і 6, не стосуються інформаційних ризиків. Вони скоріше пов'язані з оперативними діями, необхідними для технічного впровадження, обслуговування та контролю безпеки.

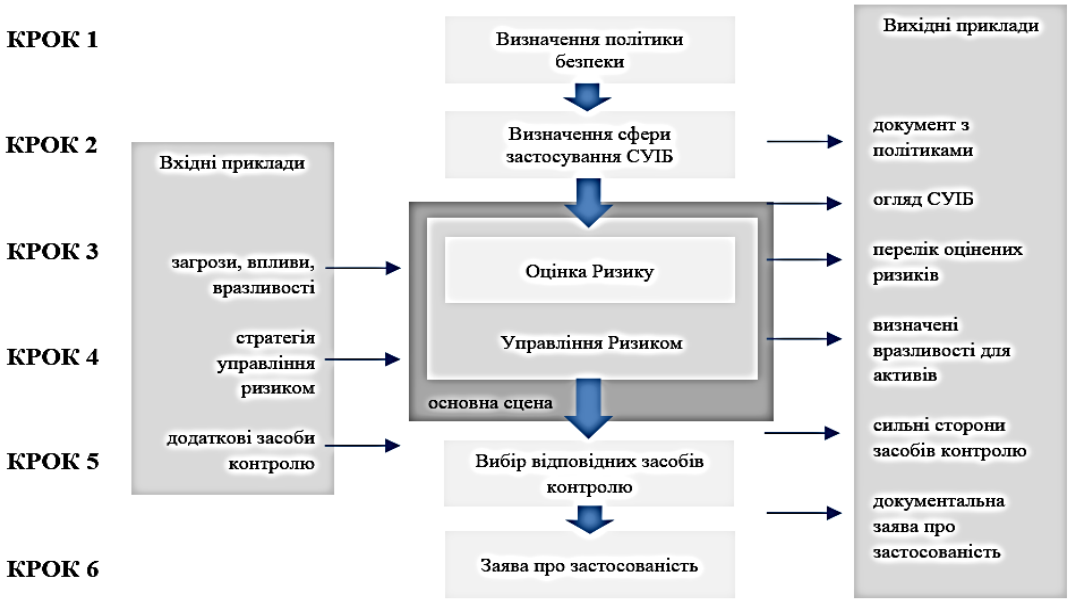

Рисунок 2. СУІБ відповідно до фреймворку ISMS від ENISA.

Нарешті, варто відзначити що , кроки 1 і 2 повторюються в більш тривалому циклі порівняно з кроками 3, 4, 5 і 6. Це пояснюється переважно тим, що встановлення політики безпеки та визначення області застосування СУІБ частіше відносяться до управлінських і, до певної міри, стратегічних питань, тоді як процес управління ризиками є оперативною проблемою [2].

Один з ключових факторів успіху системи управління інформаційною безпекою підприємства полягає у побудові її на основі міжнародних стандартів ISO/IEC 27001 [11]. Міжнародний стандарт ISO 27001 є ефективним інструментом для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою. Він надає організаціям можливість розглядати інформаційні ризики з точки зору бізнесу і приймати обґрунтовані рішення щодо їх управління.

Стандарт ISO 27001 допомагає визначити та оцінити ризики, пов'язані з інформаційною безпекою, і встановити відповідні контрольні заходи для зниження цих ризиків до прийнятного рівня. Він сприяє створенню систематичного підходу до управління

інформаційною безпекою, забезпечує збалансованість між захистом інформації та бізнес-потребами організації.

Застосування стандарту ISO 27001 дозволяє створити рамки для ефективного управління інформаційною безпекою, враховуючи контекст своєї діяльності, її ризики та вимоги зацікавлених сторін. Цей стандарт сприяє забезпеченню надійності, конфіденційності та цілісності інформації, а також підвищує довіру клієнтів, партнерів та інших зацікавлених сторін до організації.

Отже, використання стандарту ISO 27001 дозволяє ефективно управляти інформаційною безпекою, знижуючи ризики та забезпечуючи відповідність вимогам законодавства та стандартів.

Цілі, які відображаються в СУІБ:

- Захист інформації: одна з основних цілей СУІБ − забезпечити захист інформації від несанкціонованого доступу, втрати, порушення цілісності та розголошення.
- Забезпечення безпеки інформаційних систем: система управління інформаційною безпекою повинна забезпечувати безпеку інформаційних систем на ОКІ шляхом застосування відповідних технологій та політик безпеки.
- Виконання вимог законодавства: ціллю СУІБ є виконання вимог інформаційно-безпекового законодавства та нормативних актів, що регулюють захист інформації.
- Мінімізація ризиків: система повинна мінімізувати ризики виникнення інцидентів безпеки, шляхом виявлення потенційних загроз, їх аналізу та впровадження відповідних заходів запобігання.
- Управління інформаційною безпекою: СУІБ має на меті ефективне управління інформаційною безпекою на підприємстві, забезпечення відповідного рівня контролю та координації заходів безпеки.

Ці принципи та цілі є основою для розробки та впровадження системи управління інформаційною безпекою на підприємстві, спрямованої на забезпечення ефективності та надійності інформаційних процесів.

7. Компоненти та етапи впровадження системи управління інформаційною безпекою

Впровадження системи управління інформаційною безпекою включає ряд компонентів і етапів, які допомагають забезпечити ефективність та надійність захисту інформації на підприємстві. Нижче наведено загальний опис цих компонентів та етапів [4]:

1. Аналіз інформаційних потреб: передбачає визначення інформаційних потреб підприємства, ідентифікацію цінної інформації та визначення рівня її захисту. В результаті проводиться аналіз загроз безпеці інформації та оцінка ризиків.
2. Розробка політик безпеки: розробляються політики, стандарти та процедури, що визначають правила та вимоги щодо захисту інформації. Вони охоплюють такі аспекти, як доступ, конфіденційність, цілісність, резервне копіювання, відновлення даних тощо.
3. Реалізація технічних заходів безпеки: впроваджуються технічні засоби та рішення, що забезпечують захист інформації. Це можуть бути файрволи, системи ідентифікації та автентифікації, системи контролю доступу, шифрування даних, системи моніторингу тощо.
4. Навчання та свідомість персоналу: важливим компонентом впровадження системи управління інформаційною безпекою є навчання персоналу щодо правил та процедур безпеки, виявлення загроз і реагування на них. Також важливо забезпечити свідомість персоналу щодо важливості захисту інформації та його відповідальності.
5. Моніторинг та аудит безпеки: після впровадження системи управління інформаційною безпекою необхідно забезпечити постійний моніторинг стану безпеки, виявлення вразливостей та інцидентів, а також проведення аудиту системи безпеки для перевірки її ефективності та відповідності вимогам.

6. Постійне вдосконалення та оновлення: система управління інформаційною безпекою повинна бути постійно вдосконалювана, оновлювана та адаптована до змінних умов та загроз. На цьому етапі проводяться аналіз результатів, впроваджуються виправлення та вдосконалення політик та технічних засобів безпеки.

Впровадження системи управління інформаційною безпекою є комплексним процесом, який вимагає взаємодії різних компонентів та етапів. Цей підхід дозволяє забезпечити надійний захист інформації та підвищити ефективність роботи підприємства.

8. Методи та інструменти оцінки ефективності системи управління інформаційною безпекою

Оцінка ефективності системи управління інформаційною безпекою включає в себе використання різних методів та інструментів. Основні методи інструменти оцінки ефективності системи управління інформаційною безпекою включають [10]:

- Аудит безпеки: використовується для перевірки відповідності системи безпеки встановленим стандартам, політикам та процедурам. Аудит включає аналіз наявних контролів безпеки, оцінку їх ефективності та виявлення вразливостей. При проведенні аудиту рекомендовано керуватися міжнародним стандартом ISO 19011[12].
- Тестування на проникнення: використовується для активного тестування системи на наявність потенційних вразливостей. Він включає в себе спробу зламу або проникнення в систему з метою виявлення слабких місць та оцінки рівня її захищеності.
- Метрики безпеки: використовуються для кількісної оцінки рівня безпеки системи. Вони включають такі показники, як рівень виявлення загроз, час відновлення після інциденту, кількість успішно відхилених атак тощо. Метрики дозволяють оцінити ефективність застосованих заходів безпеки та визначити області для подальшого вдосконалення.
- Сертифікація та відповідність стандартам є важливим інструментом для оцінки ефективності системи управління інформаційною безпекою. Це включає впровадження визначених стандартів безпеки та проходження офіційної сертифікації, яка підтверджує відповідність системи встановленим вимогам.
- Оцінка ризиків є необхідним етапом для визначення потенційних загроз та вразливостей системи. Цей процес дозволяє ідентифікувати ризики, оцінити їх ймовірність та вплив на підприємство, а також визначити необхідні заходи для зменшення ризиків.
- Для оцінки ефективності системи управління інформаційною безпекою важливо проаналізувати витрати, пов'язані з її впровадженням та утриманням. Це включає оцінку витрат на заходи безпеки, вартість втрат від можливих інцидентів та визначення економічної ефективності системи.

Використання цих методів та інструментів дозволяє провести комплексну оцінку ефективності системи управління інформаційною безпекою та виявити області для подальшого вдосконалення.

9. Роль системи управління інформаційною безпекою у підвищенні ефективності та захищеності ОКІ

Система управління інформаційною безпекою відіграє ключову роль у підвищенні ефективності та захищеності підприємства. Вона спрямована на захист інформаційних активів, забезпечення безпеки та надійності інформаційних систем та процесів, а також зменшення ризиків, пов'язаних зі збитками внаслідок інцидентів безпеки [9].

Структура системи управління інформаційною безпекою підприємства включає наступні компоненти :

- Політика і стратегія: передбачає розробку політик, стандартів та стратегій, що визначають загальні принципи та цілі інформаційної безпеки підприємства. Включає в себе

встановлення правил доступу до інформації, управління паролями, захист від несанкціонованого доступу і т.д.

- Організаційна структура: визначає організаційну структуру та ролі в управлінні інформаційною безпекою. Включає призначення відповідальних осіб, формування команд та встановлення процедур звітності та комунікації.
- Оцінка ризиків: включає ідентифікацію потенційних загроз і вразливостей інформаційної системи підприємства, а також оцінку ризиків, пов'язаних з цими загрозами. Включає проведення аудитів безпеки, аналіз вразливостей і розробку планів зменшення ризиків.
- Заходи безпеки: включає прийняття технічних, фізичних і організаційних заходів для захисту інформації підприємства. Включає в себе застосування шифрування, встановлення файерволів, регулярне оновлення програмного забезпечення, навчання персоналу та інші заходи безпеки.
- Моніторинг та аудит: передбачає систему моніторингу та аудиту інформаційної безпеки, яка дозволяє виявляти потенційні загрози, вразливості та несанкціоновані дії. Включає проведення регулярних перевірок, аналіз журналів подій, аудит безпеки та розробку заходів для виявлення та вирішення відхилень.
- Неперервність бізнесу: визначає процедури та плани для забезпечення неперервності бізнесу в разі виникнення інцидентів, таких як катастрофи, вторгнення або системні збої. Включає резервне копіювання даних, плани відновлення після кризи, альтернативні системи та інші заходи для забезпечення продовження діяльності підприємства.

Кожен з цих компонентів взаємодіє між собою, утворюючи систему управління інформаційною безпекою, яка сприяє захисту інформації, запобіганню загрозам та забезпеченню безперебійної роботи підприємства.

Основні ролі системи управління інформаційною безпекою в контексті підвищення ефективності та захищеності такі [10]:

- Захист інформаційних активів.
- Забезпечення безпеки бізнес-процесів.
- Відповідність вимогам та регуляторному середовищу.
- Залучення інвестицій та партнерів.
- Підвищення репутації.

10. Вимірювання ефективності та показників оцінки впровадження системи управління інформаційної безпеки

Вимірювання ефективності системи управління інформаційною безпекою і встановлення показників оцінки є важливими аспектами для оцінки її успішності [13] і внесення відповідних рішень. Деякі з основних показників оцінки ефективності і вимірювання включають:

1. Зниження витрат на інциденти безпеки: вимірювання скорочення витрат, пов'язаних з інцидентами безпеки, таких як втрата даних, перерви в роботі системи або штрафи за порушення вимог безпеки.
2. Збільшення продуктивності: вимірювання покращення продуктивності співробітників та збільшення ефективності роботи завдяки забезпеченню безпеки і надійності інформаційних систем.
3. Зниження ризиків: вимірювання скорочення ризиків, пов'язаних з інформаційною безпекою, шляхом ідентифікації та усунення потенційних загроз, зменшення ймовірності виникнення вразливостей і збільшення реагування на інциденти.
4. Відновлення після інцидентів: вимірювання часу і ресурсів, необхідних для відновлення роботи після інциденту, і оцінка впливу таких інцидентів на продуктивність і ефективність підприємства.

5. Забезпечення відповідності: вимірювання ступеня відповідності системи управління інформаційною безпекою вимогам законодавства, регуляторних вимог або стандартів безпеки.

Ці показники можуть бути виміряні та оцінені за допомогою різних методів, таких як фінансовий та статистичний аналіз, опитування співробітників, аудит безпеки тощо. Важливо вибрати ті показники, які найкраще відображають ефективність системи управління інформаційною безпекою в контексті конкретного об’єкту критичної інфраструктури.

11. Перспективи подальших досліджень

Після завершення дослідження можливі наступні перспективи подальших досліджень[14]:

1. Розробка більш детального фреймворку для оцінки ефективності систем управління інформаційною безпекою на підприємствах. Це може включати розробку нових методик вимірювання, розширення показників оцінки та розробку моделей для прогнозування ефективності.

2. Дослідження впливу нових технологій, таких як штучний інтелект, блокчейн або Інтернет речей, на ефективність систем управління інформаційною безпекою. Вивчення цих технологій може допомогти виявити нові можливості для оптимізації безпеки та зниження витрат.

3. Аналіз впливу розвитку міжнародних стандартів безпеки та законодавчих змін на ефективність систем управління інформаційною безпекою. Дослідження можуть включати оцінку впливу впровадження нових стандартів на витрати, ризики та продуктивність підприємств.

4. Вивчення ефективності застосування систем управління інформаційною безпекою в різних галузях і типах підприємств. Це дозволить зрозуміти специфічні виклики та переваги, що виникають у різних контекстах, і розробити рекомендації для конкретних секторів.

5. Дослідження розширених аспектів інформаційної безпеки, таких як соціальна інженерія [15], культура безпеки та психологічні аспекти. Вивчення цих аспектів може допомогти розробити більш повне розуміння впливу людського фактора на ефективність систем управління інформаційною безпекою.

Ці перспективи можуть стати основою для подальших досліджень у галузі систем управління інформаційною безпекою та їх впливу на ефективність підприємств.

12. Висновки

Система управління інформаційною безпекою допомагає ідентифікувати критичні інформаційні активи підприємства і встановлює заходи для їх захисту. Це дозволяє уникнути втрати конфіденційної інформації, витоку даних або пошкодження систем, що може призвести до фінансових збитків та втрати довіри клієнтів.

Система управління інформаційною безпекою дозволяє ідентифікувати ризики, пов'язані з бізнес-процесами підприємства, та розробляє заходи для їх управління. Це допомагає запобігти перервам у функціонуванні та зниженню продуктивності.

Система управління інформаційною безпекою допомагає ОКІ відповідати вимогам законодавства, стандартам безпеки та регуляторним вимогам.

Захист інформації та дотримання стандартів безпеки сприяють підвищенню репутації підприємства в очах клієнтів, партнерів та інших зацікавлених сторін. Це може мати позитивний вплив на економічні відносини, збільшення клієнтської бази та збільшення обсягу продажів.

Отже, система управління інформаційною безпекою необхідна для підвищення ефективності підприємства, забезпечує захист інформаційних активів, зменшує ризики, відповідає вимогам та регуляторному середовищу, сприяє залученню інвестицій та партнерів, підвищує репутацію та забезпечує стабільність функціонування ОКІ та його систем.

Список літератури:

1) Ю.С.Тарасенко, В.Ю.Клим, С.В.Гарагатая, В.Г.Солянников. Аспекти безпеки та захищеності критичної інфраструктури. Збірник матеріалів міжнародної науково - практичної інтернет - конференції «Інноваційні технології, моделі управління кібербезпекою - «ІТМК - 2021», ч.2, Дніпро, 13 – 15 грудня 2021 р. 2021 р

2) Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

3) Ford, N. (2019, March 19). The benefits of implementing an ISMS. Retrieved from https://www.itgovernance.eu/blog/en/the-benefits-of-implementing-an-isms

4) Кавун С. В. К12 Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с.

5) Wikipedia contributors. (2023, July 1). PDCA. In Wikipedia, The Free Encyclopedia. Retrieved November 13, 2023, from https://en.wikipedia.org/wiki/PDCA

6) Toynton, J. (2023, August 17). Plan-Do-Check-Act (PDCA): Driving Efficiency and Success in Business Management. Retrieved from https://www.linkedin.com/pulse/plan-do-check-act-pdca-driving-efficiency-success-business-toynton

7) Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL: http://ibo.tneu.edu.ua/index.php/ibo/article/view/124/123

8) European Union Agency for Cybersecurity (ENISA). (n.d.). The ISMS Framework. Retrieved from https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms/framework

9) Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак. – 2015. – №2

10) Кириленко А., Бабинюк О. Кібербезпека на захисті бізнесу. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31417/ZE_2019_118.pdf?sequence=1

11) International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements

12) International Organization for Standardization. (2018). ISO 19011:2018, Guidelines for auditing management systems. Retrieved from https://www.iso.org/standard/70017.html

13) FitzGerald, J. (2023, May 16). Measuring Information Security Effectiveness - ISO/IEC 27004:2016. Retrieved from https://info.degrandson.com/blog/information-security-effectiveness

14) Бурак М.В. Інформаційна безпека як складова національної безпеки України. Економічна та інформа ційна безпека: проблеми та перспективи. Матеріали Всеукраїнської науково практичної конференції. 2017. С. 21—24

15) Cisco. (n.d.). What Is Social Engineering? Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

---

Information security management system as a tool for enhancing the protection and efficiency of critical infrastructure objects

Oleksiy Skitsko
Cybersecurity Center, NA SSU, Kyiv, Ukraine
ORCID 0000-0003-4122-0889

Roman Shyrshov
Cybersecurity Center, NA SSU, Kyiv, Ukraine
ORCID 0000-0003-3534-8736

Abstract: This article is dedicated to the study of the information security management system as a tool for increasing the level of protection and efficiency of critical infrastructure objects. A comparative analysis of similar solutions has identified the most optimal methods and approaches for managing information security, which will contribute to enhancing the level of protection and efficiency of critical infrastructure objects. An analysis of the methods and approaches to information security management in critical infrastructure objects has been carried out.

Keywords: Information Security Management System, Level of Protection, Efficiency, Critical Infrastructure Object, Analysis, Comparative Analysis, Methods, Approaches, Optimality."