НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

СОУ Н НБУ 65.1 СУІБ 1.0:2010

СТАНДАРТ ОРГАНІЗАЦІЇ УКРАЇНИ

НАСТАНОВА

МЕТОДИ ЗАХИСТУ В БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вимоги

(ISO/IEC 27001:2005, MOD)

Видання офіційне

Київ

НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

2010

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: ТК 105 „Банківські та фінансові системи і технології”, Державне підприємство „Український державний науково-дослідний інститут технологій товарно-грошового обігу, фінансових і фондових ринків” (ДП „УКРЕЛЕКОН”)

РОЗРОБНИКИ: **І. Івченко**, канд. фіз.-мат. наук; **М. Карнаух**; **М. Коваленко**, канд. техн. ~~н~~наук; **Т.Тищенко**

ВНЕСЕНО Національним банком України

2 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ Постановою Правління Національного банку України від 28.10.2010 № 474.

3 Цей стандарт відповідає стандарту ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги).

Ступінь відповідності – модифікований (MOD)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

З М І С Т

ВСТУП

Цей стандарт є прийнятий зі змінами стандарт ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги).

Технічний комітет, відповідальний за цей стандарт, - ТК 105 „Банківські та фінансові системи і технології”.

Стандарт містить вимоги, які відповідають чинному законодавству.

До стандарту було внесено окремі зміни зумовлені правовими вимогами і конкретними потребами банківської сфери діяльності. Додаткову інформацію було долучено безпосередньо до пунктів, яких вони стосуються, їх позначено подвійною рамкою та заголовком „Пояснення” та „Доповнення”. Повний перелік змін разом з обґрунтуванням наведено нижче.

До цього стандарту внесено такі редакційні зміни:

- слова “цей міжнародний стандарт”, у зв’язку з його прийняттям, замінено на “цей стандарт”;

- структурні елементи стандарту: „Обкладинку”, „Передмову”, „Вступ”, – оформлено згідно з вимогами національної стандартизації України;

- у розділі „Нормативні посилання” наведено українською мовою „Пояснення”, виділене в тексті рамкою;

- посилання на ISO/IEC 17799:2005 замінено на ISO/IEC 27002:2005 згідно з рішенням ISO.

0 ВСТУП ДО ISO/IEC 27001:2005

0.1 Загальні положення

Цей стандарт створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою (далі - СУІБ). Прийняття СУІБ повинне бути стратегічним рішенням для організації. На проектування та впровадження СУІБ організації впливають потреби та цілі організації, вимоги безпеки, застосовувані процеси, розмір і структура організації. З часом очікуються зміни цих факторів і систем, які їх підтримують. Передбачається, що впровадження СУІБ буде масштабуватися відповідно до потреб організації, наприклад, проста ситуація потребує простого рішення для СУІБ.

Доповнення

Цей стандарт розроблений для банків України і має використовуватися усіма банками України та їх підрозділами

Рекомендується створювати єдину систему управління інформаційною безпекою для банку в цілому.

Далі за текстом стандарту під словом «організація» розуміється банк.

Цей стандарт може бути використаний зацікавленими внутрішніми та зовнішніми сторонами для оцінки відповідності вимогам.

0.2 Процесний підхід

Цей стандарт приймає процесний підхід до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ організації.

Для ефективної діяльності організації необхідно ідентифікувати та управляти багатьма видами діяльності. Будь-яку діяльність, що використовує ресурси та підлягає управлінню з метою забезпечення перетворення вхідних даних у вихідні, можна розглядати як процес. Часто вихідні дані одного процесу є безпосередньо вхідними даними для наступного.

Застосування системи процесів у межах організації разом з ідентифікацією цих процесів та їх взаємодіями, а також управління ними можна розглядати як «процесний підхід».

Процесний підхід до управління інформаційною безпекою, запропонований цим стандартом, заохочує його користувачів робити наголос на важливості:

a) розуміння вимог інформаційної безпеки організації і необхідності розроблення політики та цілей інформаційної безпеки;

b) впровадження заходів безпеки та забезпечення їх функціонування для управління ризиками інформаційної безпеки організації в контексті загальних бізнес-ризиків організації;

c) моніторингу та перегляді продуктивності та ефективності СУІБ; і

d) постійному вдосконаленні, основаному на об’єктивному вимірюванні.

Цей стандарт приймає модель «Плануй-Виконуй-Перевіряй-Дій» («Plan-Do-Check-Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ. Рисунок 1 ілюструє, яким чином СУІБ, використовуючи як вхідні дані вимоги інформаційної безпеки та очікування зацікавлених сторін, за допомогою необхідних дій і процесів формує вихідні дані інформаційної безпеки, що відповідають цим вимогам та очікуванням. Рисунок 1 також ілюструє зв’язки процесів, представлених в розділах 4, 5, 6, 7 та 8.

Прийняття моделі ПВПД (PDCA) буде також відображати принципи, встановлені Настановою ОЕСР[1], які врегульовують безпеку інформаційних систем та мереж. Цей стандарт надає надійну модель для впровадження принципів цієї настанови, що впливають на оцінку ризиків, проектування і впровадження безпеки, управління безпекою та повторну її оцінку.

[1] Настанова ОЕСР щодо безпеки інформаційних систем і мереж – На шляху до культури безпеки. Париж: ОЕСР, липень. www.oecd.org

Пояснення

ОЕСР - Організація економічного співробітництва та розвитку.

Приклад 1

Вимога може полягати в тому, щоб порушення інформаційної безпеки не спричиняли серйозного фінансового збитку та/або перешкод для організації.

Приклад 2

Очікуваним результатом може бути наявність в організації людей, належним чином навчених відповідним процедурам, які дадуть змогу мінімізувати можливі несприятливі наслідки у разі серйозного інциденту, наприклад

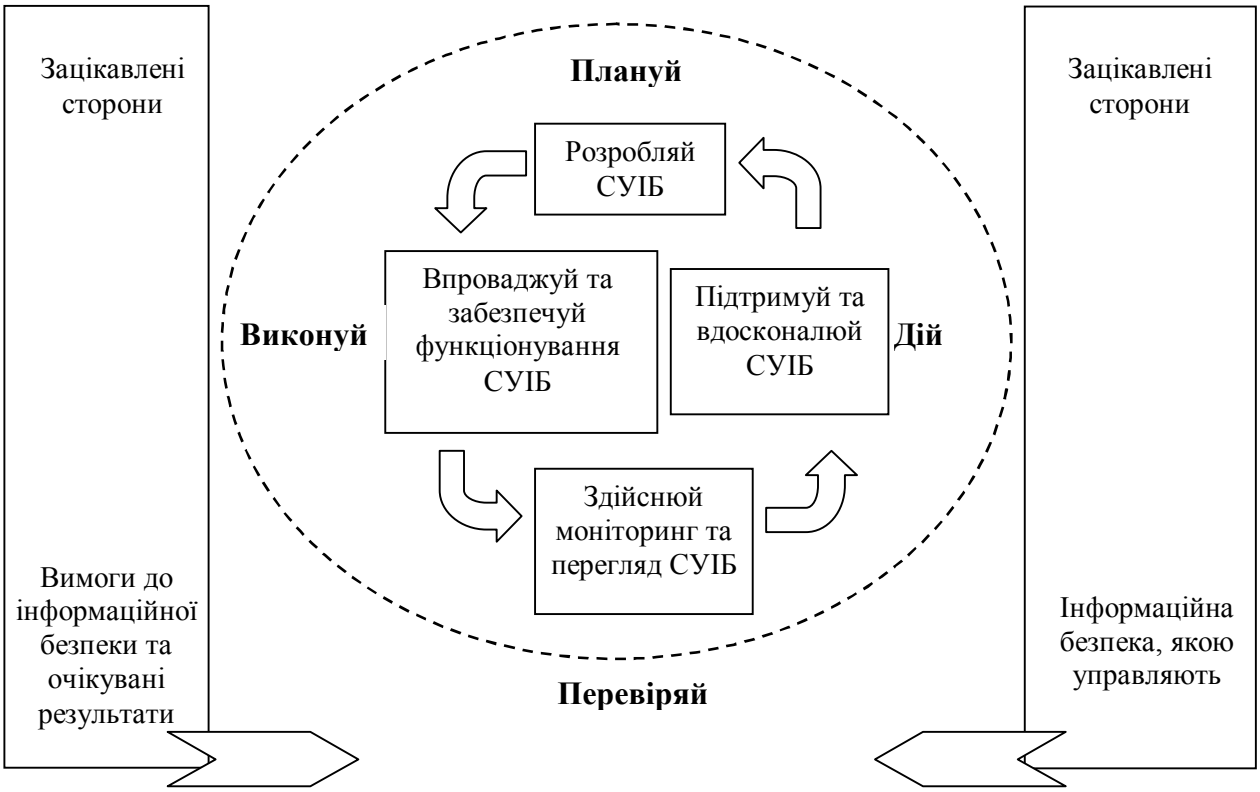

Рисунок 1 – модель ПВПД (PDCA), застосована до процесів СУІБ

Плануй (розробляй СУІБ)	Розробити політику СУІБ, цілі, процеси та процедури, суттєві для управління ризиком та вдосконалення інформаційної безпеки для отримання результатів, які відповідають загальним політикам та цілям організації.
Виконуй (впроваджуй та забезпечуй функціонування СУІБ)	Впровадити та забезпечити функціонування політики інформаційної безпеки, заходів безпеки, процесів та процедур СУІБ.
Перевіряй (здійснюй моніторинг та перегляд СУІБ)	Оцінювати і, за можливості, вимірювати продуктивність процесів згідно з політикою, цілями СУІБ і практичним досвідом та звітувати про результати керівництву для перегляду.
Дій (підтримуй та вдосконалюй СУІБ)	Вживати коригувальні та запобіжні дії на підставі результатів внутрішнього аудиту і перегляду СУІБ з боку керівництва або іншої важливої інформації для досягнення постійного вдосконалення СУІБ.

0.3 Сумісність з іншими системами управління

Цей стандарт узгоджено із стандартами ISO 9001:2000 та ISO 14001:2004 з метою підтримки послідовного та комплексного впровадження і функціонування разом з іншими пов’язаними стандартами управління. Таким чином, одна відповідним чином запроектована система управління може задовольняти вимоги всіх цих стандартів. Таблиця С.1 ілюструє взаємозв'язок між розділами цього стандарту, ISO 9001:2000 та ISO 14001:2004.

Цей стандарт розроблено для надання змоги організації узгодити свою СУІБ з відповідними вимогами системи управління або інтегрувати її в них.

СТАНДАРТ ОРГАНІЗАЦІЇ УКРАЇНИ

НАСТАНОВА

МЕТОДИ ЗАХИСТУ В БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Вимоги

МЕТОДЫ ЗАЩИТЫ В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТІ

Система управления информационной безопасностью

Требования

SECURITY TECHNIQUES FOR BANKING

Information security management systems

Requirements

Чинний від 2010-10-28

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Загальні положення

Цей стандарт стосується всіх типів організацій (наприклад, комерційних і державних установ, неприбуткових організацій). Цей стандарт встановлює вимоги до розроблення, впровадження, функціонування, моніторингу, перегляду, підтримки та вдосконалення задокументованої СУІБ у контексті загальних бізнес-ризиків організації. Він описує вимоги до впровадження заходів безпеки, пристосованих до потреб окремих організацій або їх підрозділів.

СУІБ забезпечує вибір адекватних і взаємопов’язаних заходів безпеки, які убезпечують інформаційні ресурси СУІБ та гарантують конфіденційність зацікавленим сторонам.

Важливо зазначити, що цей стандарт не передбачає врахування всіх

Видання офіційне

необхідних положень контрактів. Відповідальність за їх коректне застосування несуть користувачі стандарту. Відповідність стандарту не звільняє від правових зобов'язань.

Примітка 1. Посилання на термін «бізнес» у цьому стандарті слід інтерпретувати широко для означення тих дій, які є важливими для існування організації.

Примітка 2. В ISO/IEC 27001 надані настанови як впроваджувати СУІБ, вони можуть бути використані під час проектування заходів безпеки.

Пояснення

Стандарт Національного банку України СОУ Н НБУ 65.1 СУІБ 2,0:2010 відповідає стандарту ISO/IEC 27002, ступінь відповідності – модифікований (MOD).

1.2 Застосування

Вимоги, встановлені в цьому стандарті, є загальними та призначені для застосування всіма організаціями незалежно від типу, розміру та сфери діяльності. Вилучення будь-якої з вимог, визначених у розділах 4, 5, 6, 7 і 8 неприпустиме, якщо організація заявляє відповідність цьому стандарту.

Доповнення

Національний банк України не вимагає від банків отримання сертифіката відповідності міжнародному стандарту ISO/IEC 27001. Такий сертифікат банк може отримати за власним бажанням.

Будь-яке вилучення заходів безпеки, яке вважають доцільним для задоволення критерію прийняття ризиків, повинно бути обґрунтоване, і надані докази щодо прийняття відповідних ризиків відповідальними особами. Якщо будь-які заходи безпеки вилучено, заяви щодо відповідності цьому стандарту неприпустимі, крім випадків, коли такі вилучення не впливають на здатність та/або відповідальність організації щодо забезпечення інформаційної безпеки, яка відповідає вимогам безпеки, встановленим оцінкою ризиків і застосовними правовими або нормативними вимогами.

Примітка. Якщо організація вже має функціонуючу систему управління бізнес-процесами (наприклад, відповідно до ISO 9001 або ISO 14001), то в більшості випадків краще задовольнити вимоги цього стандарту в межах цієї існуючої системи управління.

2 НОРМАТИВНІ ПОСИЛАННЯ

Надані нижче посилальні документи є обов'язковими для застосування цього стандарту. Для датованих посилань застосовуються тільки наведені тут видання. Для недатованих посилань застосовують останні видання вказаних тут документів (в тому числі, поправок):

ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management.

Пояснення

ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою.

Пояснення

Стандарт Національного банку України СОУ Н НБУ 65.1 СУІБ 2,0:2010 відповідає стандарту ISO/IEC 27002, ступінь відповідності – модифікований (MOD).

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті застосовують такі терміни та визначення:

3.1 **ресурси СУІБ** (asset)

Усе, що має цінність для організації [2]

3.2 **доступність** (availability)

Властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта [2]

3.3 **конфіденційність** (confidentiality)

Властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів [2]

3.4 інформаційна безпека (information security)

Збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, спостержність, неспростовність та надійність [10]

Доповнення

Для банків України автентичність, спостержність, неспростовність, надійність та автентифікація користувачів та інформаційних ресурсів є обов`язковими вимогами інформаційної безпеки.

3.5 подія інформаційної безпеки (information security event)

Ідентифікована подія системи, служби або мережі, яка вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту чи раніше невідому ситуацію, яка може мати відношення до безпеки [6]

3.6 інцидент інформаційної безпеки (information security incident)

Одна або серія небажаних чи непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації бізнес-операцій і загрози інформаційній безпеці [6]

3.7 система управління інформаційною безпекою СУІБ (information security management system ISMS)

Частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки

3.8 цілісність (integrity)

Властивість захищеності безпомилковості та повноти ресурсів СУІБ [2]

3.9 залишковий ризик (residual risk)

Ризик, що залишається після оброблення ризику [9]

Пояснення

Залишковий ризик є прийнятим ризиком організації. Ризики можуть бути прийняті, якщо, наприклад, оцінено, що ризик є невеликим або вартість оброблення ризику є нерентабельною для організації. Такі рішення повинні бути задокументовані (СОУ Н НБУ 65.1 СУІБ 2.0:2010, п.4.2).

З урахуванням можливих втрат і збитків у випадку інциденту інформаційної безпеки, а також вартості впровадження заходів безпеки і запобіжних дій керівництво приймає рішення щодо критеріїв прийняття ризиків та їх прийнятного рівня (п.5.1, f)), затверджує прийнятний рівень ризику (п.4.2.1, c), 2)), приймає рішення щодо альтернативних варіантів оброблення ризиків (п.4.2.1, f)) і затверджує залишкові ризики (п.4.2.1, h)).

3.10 прийняття ризику (risk acceptance)

Рішення прийняти ризик [9]

3.11 аналізування ризику (risk analysis)

Систематичне використання інформації для ідентифікації джерел ризиків та кількісного оцінювання ризиків [9]

3.12 оцінка ризику (risk assessment)

Загальний процес аналізування ризику та оцінювання ризику [9]

3.13 оцінювання ризику (risk evaluation)

Процес порівняння кількісно оціненого ризику із заданими критеріями ризику для встановлення його значимості [9]

3.14 управління ризиком (risk management)

Скоординовані дії щодо регулювання та контролю ризиків в організації [9]

3.15 оброблення ризиків (risk treatment)

Процес вибору та впровадження заходів щодо модифікації ризику [9]

Примітка. У цьому стандарті термін "захід безпеки" використовується як синонім слова захід.

3.16 положення щодо застосовності (statement of applicability)

Задокументоване положення, яке описує цілі заходів безпеки та заходи безпеки, що є важливими та застосовними в СУІБ організації

Примітка. Цілі заходів безпеки і заходи безпеки базуються на результатах та висновках процесів оцінки і оброблення ризиків, правових або нормативних вимогах, договірних зобов'язаннях та бізнес-вимогах щодо інформаційної безпеки організації.

4 СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

4.1 Загальні вимоги

Організація повинна розробляти, впроваджувати, забезпечувати функціонування, здійснювати моніторинг, переглядати, підтримувати та вдосконалювати задокументовану СУІБ в контексті загальної бізнес-діяльності організації і ризиків, з якими вона стикається. Процес, використаний для цього стандарту, базується на моделі ПВПД (PDCA), яку наведено на рисунку 1.

4.2 Розроблення та управління СУІБ

4.2.1 Розроблення СУІБ

Організація повинна діяти таким чином.

a) Визначити сферу застосування і межі використання СУІБ виходячи з характеристик бізнесу, організації, її розташування, ресурсів СУІБ і технологій, охоплюючи подробиці та обґрунтування будь-яких винятків із сфери застосування (див. 1.2).

Доповнення
Сферою застосування СУІБ повинен бути весь банк в цілому.

b) Визначити політику СУІБ, виходячи з характеристик бізнесу, організації, її розташування, ресурсів СУІБ і технологій, яка:

1) охоплює основні положення щодо встановлення цілей і змістовно визначає загальні напрями та принципи діяльності щодо інформаційної безпеки;

2) враховує вимоги бізнесу, правові чи нормативі вимоги, а також контрактні зобов'язання щодо безпеки;

3) узгоджена з контекстом стратегічного управління ризиками організації, в якому будуть розробляти та підтримувати СУІБ;

4) встановлює критерії, за якими будуть оцінювати ризики (п.4.2.1,c); та

5) повинна бути затверджена керівництвом.

Примітка. У цьому стандарті політику СУІБ розглядають як розширення політики інформаційної безпеки. Обидві ці політики можуть бути викладені в одному документі.

c) Визначити підхід організації до оцінки ризику.

1) Ідентифікувати методологію оцінки ризику, пристосовану до СУІБ і ідентифікованої інформаційної безпеки бізнесу, правових і нормативних вимог.

2) Розробити критерії прийняття ризиків та ідентифікувати прийнятні рівні ризику (див.5.1f).

Вибрана методологія оцінки ризику повинна забезпечувати, що оцінки ризику дають порівнювані та відтворювані результати.

Примітка. Існують різні методології оцінки ризику. Приклади методологій для оцінки ризику наведено в [3].

d) Ідентифікувати ризики:

1) Ідентифікувати ресурси СУІБ в межах сфери застосування СУІБ та власників [2] цих ресурсів СУІБ.

2) Ідентифікувати загрози цим ресурсам СУІБ.

[2] Термін 'власник' визначає особу або об’єкт, на яких покладено ухвалену керівництвом відповідальність щодо контролю створення, розробки, підтримки, використання та безпеки ресурсів СУІБ. Термін 'власник' не означає, що особа дійсно має будь-які права власності на ресурси СУІБ.

3) Ідентифікувати вразливості, які можуть бути використані загрозами.

4) Ідентифікувати значні впливи, які втрата конфіденційності, цілісності та доступності можуть справити на ресурси СУІБ.

e) Проаналізувати та оцінити ризики.

1) Оцінити значні бізнес-впливи на організацію, які можуть бути наслідком порушення безпеки, враховуючи наслідки втрати конфіденційності, цілісності або доступності ресурсів СУІБ.

2) Оцінити реальну ймовірність виникнення порушень безпеки, беручи до уваги переважаючі загрози і вразливості, та значні впливи, пов’язані з цими ресурсами СУІБ, і впроваджені на цей момент заходи безпеки.

3) Визначити величину рівнів ризиків.

4) Використовуючи критерії прийнятності ризиків, встановлені в п.4.2.1 c) 2), визначити чи є ризики прийнятними, чи вимагають оброблення.

f) Ідентифікувати та оцінити альтернативні варіанти оброблення ризиків.

Можливі дії включають:

1) застосування належних заходів безпеки;

2) свідоме та об'єктивне прийняття ризиків, забезпечуючи, що вони чітко задовольняють політику організації та критерії прийняття ризиків (див. п.4.2.1 c) 2);

3) уникнення ризиків; та

4) перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

g) Вибрати цілі заходів безпеки та заходи безпеки для оброблення ризиків.

Цілі заходів безпеки та заходи безпеки треба вибирати й впроваджувати таким чином, щоб задовольняти вимоги, ідентифіковані оцінкою ризиків і

процесом їх оброблення. Цей вибір повинен враховувати як критерії для прийняття ризиків (див. 4.2.1 c) 2)), так і правові, нормативні та контрактні вимоги.

Як частину цього процесу з додатку А треба вибирати цілі заходів безпеки та заходи безпеки, що підходять для задоволення ідентифікованих вимог.

Перелічені у додатку А цілі заходів безпеки та заходи безпеки не є вичерпними, і можна також вибрати додаткові цілі заходів безпеки та заходи безпеки.

Примітка. Додаток А містить докладний перелік цілей заходів безпеки і заходи безпеки, які зазвичай вважаються доречними в організаціях. Користувачів цього стандарту відсилаємо до додатку А як до відправної точки для вибору заходів безпеки, щоб забезпечити, що жоден з важливих варіантів заходів безпеки не було пропущено.

h) Отримати від керівництва затвердження запропонованих залишкових ризиків.

i) Отримати санкцію керівництва на впровадження та функціонування СУІБ;

j) Підготувати Положення щодо застосовності.

Положення щодо застосовності треба підготувати таким чином, щоб воно включало:

1) цілі заходів безпеки і заходи безпеки, вибрані в п.4.2.1 g), та обґрунтування їх вибору;

2) цілі заходів безпеки і заходи безпеки, впроваджені на теперішній час (див.п.4.2.1 e), 2));

3) будь-які вилучені цілі заходів безпеки і заходи безпеки з тих, що наведено у додатку А, і обґрунтування їх вилучення.

Примітка. Положення щодо застосовності надає огляд рішень стосовно оброблення ризиків. Обґрунтування вилучень забезпечує перехресну перевірку того, що жодні заходи безпеки не були випадково пропущені.

4.2.2 Впровадження та функціонування СУІБ

Організація повинна діяти таким чином.

a) Сформулювати план оброблення ризиків, який ідентифікує належні управлінські дії, ресурси, обов'язки та пріоритети щодо управління ризиками інформаційної безпеки (див. розділ 5).

b) Впровадити план оброблення ризиків для досягнення ідентифікованих цілей заходів безпеки, який містить розгляд фінансових питань та розподілу ролей і обов'язків.

c) Для досягнення цілей заходів безпеки впровадити заходи безпеки, вибрані в п.4.2.1g).

d) Визначити, як вимірювати ефективність вибраних заходів безпеки або груп заходів безпеки, і встановити, як треба використовувати такі вимірювання для оцінки ефективності заходів безпеки, щоб отримувати порівнювані та відтворювані результати (див п.4.2.3 c)).

Примітка. Вимірювання ефективності заходів безпеки дозволяє керівникам та персоналу встановити, наскільки добре заходи безпеки досягають запланованих цілей.

e) Впровадити програми з навчання та поінформованості (див.5.2.2).

f) Управляти функціонуванням СУІБ.

g) Управляти ресурсами СУІБ (див.5.2).

h) Впровадити процедури та інші заходи безпеки для уможливлення термінового виявлення подій безпеки та реагування на інциденти безпеки (см. 4.2.3 a)).

4.2.3 Моніторинг та перегляд СУІБ

Організація повинна діяти таким чином.

a) Виконувати процедури моніторингу та перегляду, а також інші заходи безпеки для того, щоб:

1) терміново виявляти помилки в результатах оброблення;

2) терміново ідентифікувати вдалі та невдалі спроби порушень безпеки і інциденти безпеки;

3) надати можливість керівництву встановити, чи є діяльність щодо безпеки, яку доручено персоналу або впроваджено за допомогою інформаційних технологій, очікувано продуктивною;

4) сприяти виявленню подій безпеки і, таким чином, запобігати інцидентам безпеки, використовуючи показники; та

5) встановити, чи були ефективними дії, вжиті для усунення порушення безпеки.

b) Проводити регулярні перегляди ефективності СУІБ (включаючи перевірку відповідності політиці і цілям СУІБ та перегляд заходів безпеки), враховуючи результати аудитів безпеки, інциденти, результати вимірювань ефективності, пропозиції і зворотній зв'язок з усіма зацікавленими сторонами.

c) Вимірювати ефективність заходів безпеки, щоб підтвердити відповідність вимогам безпеки.

d) В заплановані терміни переглядати оцінки ризиків, а також переглядати залишкові ризики та ідентифіковані прийнятні рівні ризиків, враховуючи зміни в:

1) організації;

2) технології;

3) цілях та процесах бізнесу;

4) ідентифікованих загрозах;

5) ефективності впроваджених заходів безпеки; та

6) зовнішніх подіях, наприклад, змінах правового чи нормативного середовища, змінених контрактних зобов'язаннях та змінах соціального клімату.

e) В заплановані терміни проводити внутрішні аудити СУІБ (див. розділ 6).

Примітка. Внутрішні аудити, що інколи називають аудитами першої сторони, проводить для внутрішніх цілей сама організація (або за її дорученням).

f) Здійснювати на регулярній основі перегляд СУІБ з боку керівництва для забезпечення того, що сфера застосування залишається адекватною і вдосконалення в процесах СУІБ є ідентифікованими (див. 7.1).

g) Оновлювати плани впровадження заходів безпеки для врахування результатів діяльності з моніторингу та перегляду.

h) Реєструвати дії та події, що можуть мати значний вплив на ефективність чи продуктивність СУІБ (див. 4.3.3).

4.2.4 Підтримування та вдосконалення СУІБ

Організація повинна регулярно виконувати таке:

a) Впроваджувати в СУІБ ідентифіковані вдосконалення.

b) Здійснювати відповідні коригувальні та запобіжні дії згідно з пп.8.2, 8.3. Застосовувати практичний досвід з безпеки, отриманий як у власній організації, так і в інших організаціях.

c) Доводити до відома всіх зацікавлених сторін інформацію щодо дій та вдосконалень СУІБ із ступенем деталізації, що відповідає обставинам, і, що важливо, погоджувати подальші дії.

d) Забезпечувати, що вдосконалення досягають намічених цілей.

4.3 Вимоги до документації

4.3.1 Загальні положення

Документація повинна містити записи щодо управлінських рішень, забезпечуючи відстежуваність дій відповідно до управлінських рішень і політик, а також забезпечувати, що задокументовані результати відтворювані.

Важливо мати можливість продемонструвати зворотній зв'язок від вибраних заходів безпеки до результатів оцінки ризику і процесу оброблення ризику, а потім і до політики та цілей СУІБ.

Документація СУІБ повинна містити:

a) задокументовані положення щодо політики та цілей СУІБ (див. 4.2.1 b));

b) сфера застосування СУІБ (див.4.2.1 a));

c) процедури та заходи безпеки, що підтримують СУІБ;

d) опис методології оцінки ризиків (див. 4.2.1 c));

e) звіт щодо оцінки ризиків (див. від 4.2.1 c) до 4.2.1 g))

f) план оброблення ризиків (див. 4.2.2 b));

g) задокументовані процедури, необхідні організації для забезпечення ефективного планування, функціонування і контролю її процесів інформаційної безпеки, та опису того, як вимірювати ефективність заходів безпеки (див. 4.2.3 c));

h) записи, яких вимагає цей стандарт (див. 4.3.3); та

i) Положення щодо застосовності.

Примітка 1. Коли в цьому стандарті з'являється термін "задокументована процедура", це означає, що процедура розроблена, задокументована, впроваджена та підтримується.

Примітка 2. Обсяги документації СУІБ можуть відрізнятися від організації до організації залежно від:

- розміру організації та типу її діяльності; а також
- сфери застосування і складності вимог безпеки та системи, якою треба управляти.

Примітка 3. Документи та записи можуть бути в будь-якій формі та на будь-якому носії.

Доповнення

Типовий перелік документів надається Національним банком України.

4.3.2 Контроль документів

Документи, яких вимагає СУІБ, повинні бути захищеними та контрольованими. Повинна бути розроблена задокументована процедура, що визначає управлінські дії, потрібні для:

a) затвердження документів на їх адекватність (перед виданням);

b) перегляду і оновлення, за необхідності, документів та повторного їх затвердження;

c) забезпечення того, що зміни та поточний стан перегляду документів ідентифіковані;

d) забезпечення того, що відповідні версії діючих документів доступні у місцях їх використання;

e) забезпечення того, що документи залишаються чіткими і легко ідентифікованими;

f) забезпечення того, що документи доступні для тих, хто їх потребує, та їх передають, зберігають і врешті-решт знищують згідно з процедурами, застосовними відповідно до їх класифікації;

g) забезпечення того, що документи зовнішнього походження ідентифіковані;

h) забезпечення того, що поширення документів контрольоване;

i) запобігання ненавмисному використанню застарілих документів;

j) застосування до них належної ідентифікації у разі зберігання для будь-яких цілей.

4.3.3 Контроль записів

Треба розробити та підтримувати записи для надання доказів щодо відповідності вимогам і ефективного функціонування СУІБ. Вони повинні бути захищені та контрольовані. СУІБ повинна враховувати будь-які відповідні правові чи нормативні вимоги та контрактні зобов'язання. Записи повинні залишатися чіткими, легко ідентифікованими і відновлюваними. Заходи безпеки, потрібні для ідентифікації, зберігання, захисту та відновлювання, термін зберігання і знищення записів повинні бути задокументовані та впроваджені.

Треба зберігати записи щодо продуктивності процесу, як підкреслено в 4.2, і щодо всіх випадків значних інцидентів безпеки, пов’язаних з СУІБ.

Приклад

Прикладами записів є журнал реєстрації відвідувачів, звіти щодо результатів аудиту та заповнені форми санкціонування доступу.

5 ВІДПОВІДАЛЬНІСТЬ КЕРІВНИЦТВА

5.1 Зобов'язання керівництва

Керівництво повинно продемонструвати виконання своїх зобов'язань щодо організації розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ шляхом:

a) контролю розроблення політики СУІБ;

b) контролю того, що цілі та плани СУІБ розроблено;

c) контролю розроблення ролей і обов’язків щодо інформаційної безпеки;

d) доведення до відому організації інформації щодо важливості досягнення цілей інформаційної безпеки та відповідності політиці інформаційної безпеки, відповідальності перед законом та потреби постійного вдосконалення;

e) надання достатніх ресурсів для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ (див. 5.2.1);

f) винесення рішення щодо критеріїв прийняття ризиків і прийнятних їх рівнів;

g) забезпечення проведення внутрішніх аудитів СУІБ (див. розділ 6); та

h) проведення переглядів СУІБ (див. розділ 7) з боку керівництва.

5.2 Управління ресурсами

5.2.1 Забезпечення ресурсами

Організація повинна визначити та забезпечити ресурси, потрібні щоб:

a) розробляти, впроваджувати, забезпечувати функціонування, здійснювати моніторинг, перегляд, підтримку та вдосконалення СУІБ;

b) забезпечувати підтримку вимог бізнесу процедурами інформаційної безпеки;

c) ідентифікувати і враховувати правові та нормативні вимоги, а також контрактні зобов'язання з безпеки;

d) підтримувати адекватний рівень безпеки шляхом коректного застосування усіх впроваджених заходів безпеки;

e) за необхідності виконувати перегляди та відповідним чином реагувати на результати таких переглядів; і

f) за потреби, підвищувати ефективність СУІБ.

5.2.2 Навчання, поінформованість та компетентність

Організація повинна забезпечити, щоб весь персонал, для якого встановлено визначені в СУІБ відповідальності, був компетентним для виконання необхідних завдань шляхом:

a) визначення необхідної компетентності персоналу, який виконує роботи, що впливають на СУІБ;

b) забезпечення навчання або вжиття інших заходів (наприклад, наймання компетентного персоналу) для задоволення цих потреб;

c) оцінювання ефективності вжитих заходів; та

d) підтримування записів щодо освіти, навчання, навиків, досвіду та кваліфікації персоналу (див. 4.3.3).

Організація повинна також забезпечити, що весь відповідний персонал поінформовано щодо значущості та важливості їх діяльності з інформаційної безпеки і їх внеску в досягнення цілей СУІБ.

6 ВНУТРІШНІ АУДИТИ СУІБ

Організація повинна в заплановані терміни проводити внутрішні аудити СУІБ для встановлення чи цілі заходів безпеки, заходи безпеки, процеси та процедури СУІБ:

a) відповідають вимогам цього стандарту та відповідному законодавству або нормативам;

b) відповідають вимогам ідентифікованої інформаційної безпеки;

c) є ефективно впровадженими та підтримуваними; а також

d) виконуються як очікувалося.

Програма аудиту повинна плануватися з урахуванням статусу і важливості процесів і областей, що підлягають аудиту, а також результатів попередніх аудитів. Повинні бути визначені критерії, сфера застосування, частота і методи аудиту. Відбір аудиторів і проведення аудитів повинні забезпечувати об'єктивність і неупередженість процесу аудиту. Аудитори не повинні проводити аудит своєї власної роботи.

Обов'язки та вимоги до планування і проведення аудитів, а також звітування про результати і підтримування записів (див. 4.3.3) повинні бути визначені в задокументованій процедурі.

Керівництво, відповідальне за область, що підлягає аудиту, повинне забезпечити, що дії для усунення виявлених невідповідностей та їх причин виконуються без недоречних затримок. Подальша діяльність повинна містити верифікацію виконаних дій і звітування про результати верифікації (див. 8).

Примітка: [7] може надати корисні настанови щодо виконання внутрішніх аудитів СУІБ.

7 ПЕРЕГЛЯД СУІБ З БОКУ КЕРІВНИЦТВА

7.1 Загальні положення

Керівництво повинне здійснювати перегляд СУІБ організації у заплановані терміни (не менше одного разу на рік) для забезпечення її постійної придатності, адекватності та ефективності. Цей перегляд повинен містити оцінку можливостей вдосконалення і потреби внесення змін у СУІБ, включаючи зміни у політиці інформаційної безпеки і цілі інформаційної безпеки. Результати такого перегляду повинні бути чітко задокументовані, а записи повинні підтримуватись (див.4.3.3).

7.2 Вхідні дані для перегляду

Вхідні дані для перегляду з боку керівництва повинні містити:

a) результати аудитів та переглядів СУІБ;

b) зворотний зв'язок від зацікавлених сторін;

c) методи, продукти або процедури, які може використати організація для вдосконалення продуктивності та ефективності СУІБ;

d) статус запобіжних та коригувальних дій;

e) вразливості або загрози, які не були адекватно враховані в попередній оцінці ризиків;

f) результати вимірів ефективності СУІБ;

g) дії, що є наслідком попереднього перегляду з боку керівництва;

h) будь-які зміни, що можуть мати вплив на СУІБ;

i) рекомендації щодо вдосконалення.

7.3 Вихідні дані перегляду

Вихідні дані перегляду з боку керівництва повинні містити будь-які рішення та дії стосовно наведеного нижче.

a) Вдосконалення ефективності СУІБ.

b) Оновлення оцінки ризиків та плану оброблення ризиків.

c) Модифікації, за необхідності, процедур і заходів безпеки, що впливають на інформаційну безпеку, для адекватного реагування на внутрішні або зовнішні події, які можуть мати значний вплив на СУІБ, включаючи зміни у:

1) бізнес-вимогах;

2) вимогах безпеки;

3) бізнес-процесах, які впливають на існуючі бізнес-вимоги;

4) нормативних чи правових вимогах;

5) контрактних зобов'язаннях;

6) рівнях ризику та/або критеріїв прийняття ризиків.

d) Потреб у ресурсах.

e) Удосконалення того, як вимірюють ефективність заходів безпеки.

8 ВДОСКОНАЛЕННЯ СУІБ

8.1 Постійне вдосконалення

Організація повинна постійно підвищувати ефективність СУІБ шляхом

використання політики інформаційної безпеки, цілей інформаційної безпеки, результатів аудитів, аналізу подій, що підлягають моніторингу, коригувальних і запобіжних дій та перегляду з боку керівництва (див. 7).

8.2 Коригувальні дії

Організація повинна здійснювати дії для усунення причин невідповідностей вимогам СУІБ, щоб запобігати їх повторенню. Задокументована процедура коригувальних дій повинна визначати вимоги до:

a) ідентифікації невідповідностей;

b) встановлення причин невідповідностей;

c) оцінювання потреби у діях для забезпечення того, що невідповідності не будуть повторюватись;

d) встановлення та впровадження потрібних коригувальних дій;

e) реєстрування результатів виконаних дій (див. 4.3.3); та

f) перегляду виконаних коригувальних дій.

8.3 Запобіжні дії

Організація повинна встановити дії для усунення причини потенційних невідповідностей вимогам СУІБ для запобігання їх появі. Здійснені запобіжні дії повинні відповідати величині впливу потенційних проблем. Задокументована процедура запобіжних дій повинна визначити вимоги до:

a) ідентифікації потенційних невідповідностей та їх причин;

b) оцінювання потреби в діях для запобігання виникненню невідповідностей;

c) встановлення та впровадження необхідних запобіжних дій;

d) реєстрування результатів виконаних дій (див. 4.3.3); а також

e) перегляду виконаних запобіжних дій.

Організація повинна ідентифікувати ризики, що змінилися, та ідентифікувати вимоги до запобіжних дій, зосередивши увагу на ризиках, що істотно змінилися.

Пріоритети запобіжних дій повинні бути встановлені на основі результатів оцінки ризику.

Примітка: Дії, що запобігають невідповідностям, часто рентабельніші за коригувальні дії.

ДОДАТОК А

(обов'язковий)

ЦІЛІ ЗАХОДІВ БЕЗПЕКИ ТА ЗАХОДИ БЕЗПЕКИ

Цілі заходів безпеки та заходи безпеки, наведені в таблиці А.1, безпосередньо виведені та узгоджені з тих цілей заходів безпеки та заходів безпеки, що наведені в СОУ Н НБУ 65.1 СУІБ 2.0:2010, розділи з 5 по 15. Переліки, наведені в таблиці А.1, не є вичерпними, і організація може вважати необхідними додаткові цілі заходів безпеки та заходи безпеки. Цілі заходів безпеки та заходи безпеки повинні бути вибирані з цих таблиць, як частина процесу СУІБ, специфікованого в 4.2.1.

Розділи з 5 по 15 стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010 надають рекомендації щодо впровадження і настанову з практичного досвіду підтримки контролів заходів безпеки, специфікованих в розділах з А.5 до А.15.

Таблиця А.1 - Цілі заходів безпеки та заходи безпеки

А.5 Політика безпеки		
А.5.1 Політика інформаційної безпеки *Ціль*: Забезпечити регулювання та підтримку з боку керівництва інформаційної безпеки згідно з вимогами бізнесу та відповідними законами і нормативами.		
А.5.1.1	Документ щодо політики інформаційної безпеки	*Заходи безпеки* Документ щодо політики інформаційної безпеки повинен бути затверджений керівництвом, виданий та доведений до відома всього найманого персоналу та потрібних зовнішніх сторін.
А.5.1.2	Перегляд політики інформаційної безпеки	*Заходи безпеки* Політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її

		постійної придатності, адекватності та ефективності.
А.6 Організація інформаційної безпеки		
А.6.1 ***Внутрішня організація*** *Ціль:* Управляти інформаційною безпекою в організації.		
А.6.1.1	Зобов'язання керівництва щодо інформаційної безпеки	*Заходи безпеки* Керівництво повинно активно підтримувати безпеку в межах організації шляхом чіткого регулювання, підтверджених зобов’язань, чітких призначень та визнання відповідальності за інформаційну безпеку.
А.6.1.2	Координація інформаційної безпеки	*Заходи безпеки* Діяльність щодо інформаційної безпеки повинна бути узгодженою між представниками різних підрозділів організації з відповідними ролями та посадовими обов’язками.
А.6.1.3	Розподіл обов’язків щодо інформаційної безпеки	*Заходи безпеки* Усі обов’язки щодо інформаційної безпеки необхідно чітко визначити.
А.6.1.4	Процес санкціонування використання засобів оброблення інформації	*Заходи безпеки* Процес управління санкціонуванням використання нових засобів оброблення інформації треба визначити та впровадити.
А.6.1.5	Угоди щодо конфіденційності	*Заходи безпеки* Вимоги щодо конфіденційності або угоди щодо нерозголошення, які відображують потреби організації у захисті інформації,

		повинні бути ідентифіковані та підлягають регулярному перегляду.
А.6.1.6	Контакти з повноважними органами	*Заходи безпеки* Необхідно підтримувати належні контакти з відповідними повноважними органами.
А.6.1.7	Контакти з групами фахівців з певної проблематики	*Заходи безпеки* Необхідно підтримувати належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об'єднаннями.
А.6.1.8	Незалежний перегляд інформаційної безпеки	*Заходи безпеки* Підхід організації до управління інформаційною безпекою та її впровадження (тобто, цілі заходів безпеки, заходи безпеки, політики, процеси та процедури інформаційної безпеки) підлягають незалежному перегляду в заплановані терміни або за виникнення значних змін у впровадженій безпеці.
А.6.2 Зовнішні сторони *Ціль*: Підтримування безпеки інформації організації та її засобів оброблення інформації, до яких мають доступ, обробляють, якими управляють або з якими підтримують зв'язок зовнішні сторони.		
А.6.2.1	Ідентифікація ризиків, пов'язаних з зовнішніми сторонами	*Заходи безпеки* Ризики бізнес-процесів, до яких залучені зовнішні сторони, для інформації організації та засобів її оброблення повинні бути ідентифіковані і до надання доступу повинні бути впроваджені належні заходи безпеки.

А.6.2.2	Врахування безпеки під час роботи з клієнтами	*Заходи безпеки* Перш ніж надавати клієнтам доступ до інформації або ресурсів СУІБ організації, повинні бути враховані всі ідентифіковані вимоги безпеки.
А.6.2.3	Врахування безпеки в угодах з третьою стороною	*Заходи безпеки* Угоди з третіми сторонами щодо доступу, оброблення, передавання або управління інформацією організації або засобами оброблення інформації, або щодо додавання продуктів чи послуг до засобів оброблення інформації повинні охоплювати усі відповідні вимоги безпеки.
А.7 Управління ресурсами СУІБ		
А.7.1 ***Відповідальність за ресурси СУІБ*** *Ціль:* Досягти та підтримувати належний захист ресурсів СУІБ організації		
А.7.1.1	Інвентаризація ресурсів СУІБ	*Заходи безпеки* Усі ресурси СУІБ необхідно чітко ідентифікувати та скласти і підтримувати інвентарний опис усіх важливих ресурсів СУІБ
А.7.1.2	Володіння ресурсами СУІБ	*Заходи безпеки* Уся інформація і ресурси СУІБ, пов'язані із засобами оброблення інформації, повинні «бути у власності»[3] призначеного підрозділу організації

[3] Термін «власник» ідентифікує особу або організацію, що має ухвалену керівництвом відповідальність щодо контролювання створення, розвитку, підтримування, використання та безпеки ресурсів СУІБ. Термін «власник» не означає, що особа дійсно має права власності на ресурс СУІБ.

А.7.1.3	Припустиме використання ресурсів СУІБ	*Заходи безпеки* Правила щодо припустимого використання інформації та ресурсів СУІБ, пов'язаних з засобами оброблення інформації, повинні бути ідентифіковані, задокументовані та впроваджені.
А.7.2 *Класифікація інформації*		
Ціль: Забезпечити, що інформація одержує належний рівень захисту		
А.7.2.1	Настанови щодо класифікації	*Заходи безпеки* Інформація повинна бути класифікована в термінах її цінності, правових вимог, конфіденційності та критичності для організації
А.7.2.2	Маркування та оброблення інформації	*Заходи безпеки* Повинна бути розроблена та впроваджена належно множина процедур для маркування та оброблення інформації згідно зі схемою класифікації, прийнятою організацією.
А.8 Безпека людських ресурсів		
А.8.1 Перед наймом[4] *Ціль:* Гарантувати, що найманий персонал, підрядники та користувачі третьої сторони розуміють свої обов'язки, придатні до ролей, на які претендують, і зменшити ризик розкрадання, шахрайства чи зловживання обладнанням.		
А.8.1.1	Ролі та обов'язки	*Заходи безпеки* Ролі та обов'язки щодо безпеки найманого персоналу, підрядників та користувачів третьої сторони повинні бути визначені та

[4] Пояснення: Слово «найм» тут призначене, щоб охопити всі різноманітні ситуації: найм людей (тимчасовий чи постійний), призначення на посади, зміну посад, підписання контрактів та припинення дії будь-якої з цих угод.

		задокументовані відповідно до політики інформаційної безпеки організації.
A.8.1.2	Ретельна перевірка	*Заходи безпеки* Підтверджувальні перевірки біографічних даних щодо всіх кандидатів на найм, підрядників та користувачів третьої сторони повинні виконуватись згідно з усіма відповідними законами, нормативами та морально-етичними нормами, а також співвідносно до бізнес-вимог, класифікації інформації, до якої потрібен доступ, і усвідомлюваних ризиків.
A.8.1.3	Терміни та умови найму	*Заходи безпеки* Як частину своїх зобов'язань за контрактом, найманий персонал, підрядники та користувачі третьої сторони повинні погодити і підписати терміни та умови свого контракту з найму, який повинен встановити взаємні відповідальності щодо інформаційної безпеки.
A.8.2 Протягом найму *Ціль:* Впевнитись, що весь найманий персонал, підрядники та користувачі третьої сторони поінформовані щодо загроз і проблем інформаційної безпеки, своїх відповідальностей та обов'язків, а також забезпечені всім необхідним, щоб підтримувати політику безпеки організації в ході своєї повсякденної роботи і зменшити ризик суб'єктивної помилки.		
A.8.2.1	Відповідальності керівництва	*Заходи безпеки* Керівництво повинне вимагати від найманого персоналу, підрядників та користувачів

		третьої сторони застосування безпеки згідно з установленими в організації політиками та процедурами.
А.8.2.2	Поінформованість, освіта і навчання щодо інформаційної безпеки	*Заходи безпеки* Увесь найманий персонал організації, і там, де це суттєво, і підрядники та користувачі третьої сторони повинні одержати належне навчання для поінформованості та регулярно отримувати оновлені дані щодо політик і процедур організації, суттєвих для їх посадових функцій.
А.8.2.3	Дисциплінарний процес	*Заходи безпеки* Повинен існувати офіційно оформлений дисциплінарний процес щодо найманого персоналу, який здійснив порушення безпеки.
А.8.3 Припинення або зміна умов найму *Ціль:* Впевнитись, що весь найманий персонал, підрядники та користувачі третьої сторони залишають організацію чи змінюють умови найму в установленому порядку.		
А.8.3.1	Припинення відповідальностей	*Заходи безпеки* Повинні бути чітко визначені та встановлені відповідальності за виконання процедур припинення найму або зміну умов найму.
А.8.3.2	Повернення ресурсів СУІБ	*Заходи безпеки* Увесь найманий персонал, підрядники та користувачі третьої сторони повинні повернути всі ресурси СУІБ організації, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди.

А.8.3.3	Вилучення прав доступу	*Заходи безпеки* Після припинення найму, контракту чи угоди будь-якого найманого персоналу, підрядників і користувачів третьої сторони права їх доступу до інформації та засобів оброблення інформації повинні бути вилучені або пристосовані до зміни.
А.9 Фізична безпека та безпека інфраструктури		
А.9.1 Зони безпеки *Ціль:* Запобігти несанкціонованому фізичному доступу, ушкодженню та вторгненню до службових приміщень організації та втручанню в її інформацію.		
А.9.1.1	Периметр фізичної безпеки	*Заходи безпеки* Для захисту зон, що містять інформацію чи засоби оброблення інформації, треба використовувати периметри безпеки (бар'єри, наприклад, стіни, картково- контрольовані вхідні брами або пости чергових).
А.9.1.2	Заходи безпеки фізичного прибуття	*Заходи безпеки* Зони безпеки повинні бути захищені належними заходами безпеки прибуття, щоб забезпечити, що доступ дозволений тільки персоналу, який отримав санкцію.
А.9.1.3	Убезпечення офісів, кімнат і обладнання	*Заходи безпеки* Повинна бути розроблена і застосована фізична безпека офісів, кімнат і обладнання.
А.9.1.4	Захист від зовнішніх та інфраструктурних загроз	*Заходи безпеки* Повинен бути розроблений та застосований фізичний захист від пошкодження внаслідок пожежі, повені, землетрусу, вибуху, акцій

		громадської непокори та інших форм стихійного або спричиненого людьми лиха.
A.9.1.5	Робота в зонах безпеки	*Заходи безпеки* Повинні бути розроблені та застосовані фізичний захист і настанови щодо роботи в зонах безпеки.
A.9.1.6	Зони загального доступу, доставки та відвантаження	*Заходи безпеки* Щоб уникнути несанкціонованого доступу, повинні бути контрольовані і, за можливості, ізольовані від засобів оброблення інформації точки доступу, наприклад, зони доставки та відвантаження, а також інші точки, через які особи, доступ яких не санкціоновано, можуть увійти до службових приміщень
A.9.2 Безпека обладнання *Ціль:* Запобігти втратам, ушкодженню, крадіжці або компрометації ресурсів СУІБ та перериванню діяльності організації.		
A.9.2.1	Розміщення та захист обладнання	*Заходи безпеки* Обладнання повинне бути розміщене чи захищене таким чином, щоб зменшити ризики інфраструктурних загроз і небезпек та можливостей несанкціонованого доступу.
A.9.2.2	Допоміжні комунальні служби	*Заходи безпеки* Обладнання повинне бути захищене від аварійних відключень живлення та інших порушень, внаслідок аварій засобів життєзабезпечення.
A.9.2.3	Безпека кабельних мереж	*Заходи безпеки* Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних

		послуг, повинні бути захищені від перехоплювання чи ушкоджень.
A.9.2.4	Обслуговування обладнання	*Заходи безпеки* Обладнання повинне правильно обслуговуватися, щоб забезпечити його постійну доступність та цілісність.
A.9.2.5	Безпека обладнання поза службовими приміщеннями	*Заходи безпеки* До обладнання поза службовими приміщеннями повинен бути застосовний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації.
A.9.2.6	Безпечне вилучення або повторне використання обладнання	*Заходи безпеки* Всі елементи обладнання, які містять носії пам'яті, повинні бути перевірені для забезпечення того, що будь-які конфіденційні дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення.
A.9.2.7	Переміщення майна	*Заходи безпеки* Обладнання, інформація чи програмне забезпечення не повинні виноситись назовні без попередньої санкції на ці дії.
A.10 Управління комунікаціями та функціонуванням		
***A.10.1* Процедури експлуатації та відповідальності** *Ціль:* Забезпечити коректне та безпечне функціонування засобів оброблення інформації.		
A.10.1.1	Задокументовані процедури експлуатації	*Заходи безпеки* Процедури експлуатації повинні бути задокументовані, підтримувані та зроблені

		доступними для всіх користувачів, що їх потребують.
А.10.1.2	Управління змінами	*Заходи безпеки* Зміни у засобах оброблення інформації та системах повинні бути контрольованими.
А.10.1.3	Розподілення обов’язків	*Заходи безпеки* Повинні бути розподілені обов’язки та сфери відповідальності для зменшення можливості несанкціонованої або ненавмисної модифікації ресурсів СУІБ організації чи зловживання ними.
А.10.1.4	Відокремлення засобів розробки, тестування та експлуатації	*Заходи безпеки* Засоби розроблення, тестування та експлуатації повинні бути відокремлені для зменшення ризиків несанкціонованого доступу до системи, яка знаходиться в промисловій експлуатації, або її несанкціонованої зміни.
А.10.2 Управління наданням послуг третьою стороною *Ціль:* Впровадити і підтримувати належний рівень інформаційної безпеки та надання послуг відповідно до угод щодо надання послуг третьою стороною.		
А.10.2.1	Надання послуг	*Заходи безпеки* Треба забезпечити, що заходи безпеки, визначення послуг та рівень їх надання, які містить угода щодо надання послуг третьою стороною, впроваджені, функціонують та підтримуються третьою стороною.
А.10.2.2	Моніторинг та перегляд послуг третьої сторони	*Заходи безпеки* Послуги, звіти та записи, надавані третьою стороною, повинні підлягати регулярному

		моніторингу і перегляду та повинні проводитись регулярні аудити
A.10.2.3	Управління змінами у послугах третьої сторони	*Заходи безпеки* Зміни у наданні послуг, включаючи підтримування і вдосконалювання існуючих політик інформаційної безпеки, процедур і заходів безпеки, повинні управлятися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків.
A.10.3 Планування та приймання системи *Ціль:* Мінімізувати ризик відмови систем.		
A.10.3.1	Управління потужністю	*Заходи безпеки* Для забезпечення потрібної продуктивності системи необхідно здійснювати моніторинг та регулювати використання ресурсів і проектувати вимоги до майбутньої потужності.
A.10.3.2	Приймання системи	*Заходи безпеки* Повинні бути розроблені критерії приймання нових інформаційних систем, їх модернізацій та нових версій і виконані відповідні тести систем протягом розроблення і перед прийманням
A.10.4 Захист від зловмисного та мобільного коду *Ціль:* Захистити цілісність програмного забезпечення та інформації.		
A.10.4.1	Заходи безпеки проти зловмисного коду	*Заходи безпеки* Повинні бути впроваджені заходи безпеки щодо виявлення, запобігання та відновлення для захисту від зловмисного коду і належні

		процедури поінформовування користувачів.
A.10.4.2	Заходи безпеки проти мобільного коду	*Заходи безпеки* Там, де використання мобільного коду санкціоновано, конфігурація повинна гарантувати, що санкціонований мобільний код використовується згідно з чітко визначеною політикою безпеки, та необхідно запобігти виконанню несанкціонованого мобільного коду.
A.10.5 Резервне копіювання *Ціль:* Підтримувати цілісність і доступність інформації та засобів оброблення інформації.		
A.10.5.1	Резервне копіювання інформації	*Заходи безпеки* Згідно з затвердженою політикою резервного копіювання треба регулярно робити і тестувати резервні копії інформації та програмного забезпечення.
A.10.6 Управління безпекою мережі *Ціль:* Забезпечити захист інформації в мережах та захист інфраструктури, що їх підтримує.		
A.10.6.1	Заходи безпеки мережі	*Заходи безпеки* Треба відповідним чином управляти і захищати мережі, щоб вони були захищеними від загроз і підтримувалася безпека систем та прикладних програм, які використовують мережу, включаючи інформацію, що передається.
A.10.6.2	Безпека послуг мережі	*Заходи безпеки* Характеристики безпеки, рівні послуг, а також вимоги управління всіма послугами

		мережі повинні бути ідентифіковані і міститись у будь-якій угоді щодо послуг мережі, як для послуг, що надаються організацією, так і для аутсорсингових.
А.10.7 Поводження з носіями *Ціль:* Запобігти несанкціонованому розголошенню, модифікації, вилученню або знищенню ресурсів СУІБ та перериванню бізнес-діяльності.		
А.10.7.1	Управління змінними носіями	*Заходи безпеки* Повинні бути наявними процедури управління змінними носіями.
А.10.7.2	Вилучення носіїв	*Заходи безпеки* Коли носії більше не потрібні, вони повинні безпечно і надійно вилучатися із застосуванням офіційно оформлених процедур.
А.10.7.3	Процедури поводження з інформацією	*Заходи безпеки* Для захисту інформації від несанкціонованого розголошення або зловживання повинні бути розроблені процедури поводження з інформацією та її збереження.
А.10.7.4	Безпека системної документації	*Заходи безпеки* Системна документація повинна бути захищена від несанкціонованого доступу.
А.10.8 Обмін інформацією *Ціль:* Підтримувати безпеку інформації і програмного забезпечення, якими обмінюються в організації та з зовнішнім об’єктом.		
А.10.8.1	Політики та процедури обміну інформацією	*Заходи безпеки* Повинні бути наявними офіційно оформлені політики, процедури та заходи безпеки для

		захисту обміну інформацією з використанням всіх видів засобів комунікації.
А.10.8.2	Угоди щодо обміну	*Заходи безпеки* Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо обміну інформацією та програмним забезпеченням.
А.10.8.3	Фізичні носії під час передавання	*Заходи безпеки* Носії, що містять інформацію, повинні бути захищені від несанкціонованого доступу, зловживання або руйнування під час транспортування поза фізичними межами організації.
А.10.8.4	Електронний обмін повідомленнями	*Заходи безпеки* Інформація, яка міститься в електронних повідомленнях, повинна бути захищена належним чином.
А.10.8.5	Системи бізнес-інформації	*Заходи безпеки* Повинні бути розроблені та впроваджені політика і процедури захисту інформації, пов'язаної з взаємозв'язком систем бізнес-інформації.
А.10.9 Послуги електронної комерції *Ціль:* Забезпечити захист послуг електронної комерції та їх безпечне використання.		

Пояснення

Цей розділ використовується в банках України тільки в частині продажу банківських продуктів, в тому числі віддаленого обслуговування рахунків клієнтів.

А.10.9.1		*Заходи безпеки*

	Електронна комерція	Інформація, залучена в електронну комерцію, яка проходить через загальнодоступні мережі, повинна бути захищена від шахрайської діяльності, контрактних суперечок і несанкціонованого розголошення та модифікації.
A.10.9.2	Інтерактивні трансакції	*Заходи безпеки* Інформація, залучена в інтерактивні трансакції, повинна бути захищена для запобігання неповній передачі, неправильній маршрутизації, несанкціонованій зміні повідомлення, несанкціонованому розголошенню, несанкціонованому дублюванню повідомлення або його повторенню.
A.10.9.3	Загальнодоступна інформація	*Заходи безпеки* Повинна забезпечуватись цілісність інформації, яка буде зроблена доступною у загальнодоступній системі, для запобігання її несанкціонованій модифікації.
A.10.10 Моніторинг *Ціль:* Виявити несанкціоновану діяльність з оброблення інформації.		
A.10.10.1	Журнал аудиту	*Заходи безпеки* Журнал аудиту, в якому записується діяльність користувачів, винятки та події інформаційної безпеки, повинен вестися і зберігатися протягом погодженого періоду для сприяння в майбутніх розслідуваннях і

		моніторингу контролю доступу.
A.10.10.2	Моніторинг використання системи	*Заходи безпеки* Повинні бути розроблені процедури моніторингу використання засобів оброблення інформації та результати моніторингу діяльності повинні регулярно переглядатися.
A.10.10.3	Захист інформації журналів реєстрації	*Заходи безпеки* Засоби реєстрування і інформація реєстрації повинні бути захищені від фальсифікації та несанкціонованого доступу.
A.10.10.4	Журнали реєстрації адміністратора та оператора	*Заходи безпеки* Діяльність системного адміністратора та системного оператора повинна реєструватися.
A.10.10.5	Реєстрація несправностей	*Заходи безпеки* Несправності треба реєструвати, аналізувати та вживати належні дії.
A.10.10.6	Синхронізація годинників	*Заходи безпеки* Годинники всіх важливих систем оброблення інформації в організації або домені безпеки повинні бути синхронізовані з джерелом часу погодженої точності.
A.11 Контроль доступу		
A.11.1 Бізнес-вимоги до контролю доступу *Ціль:* Контролювати доступ до інформації.		
A.11.1		*Заходи безпеки*

	Політика контролю доступу	Політика контролю доступу повинна бути розроблена, задокументована та переглядатись на основі вимог бізнесу та безпеки щодо доступу.
А.11.2 Управління доступом користувача *Ціль:* Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до інформаційних систем.		
А.11.2.1	Реєстрація користувача	*Заходи безпеки* Для надання та відміни доступу до всіх інформаційних систем і послуг повинні бути наявними офіційно оформлені процедури реєстрації та зняття з реєстрації.
А.11.2.2	Управління повноваженнями	*Заходи безпеки* Призначення та використання повноважень повинно бути обмеженим та контрольованим.
А.11.2.3	Управління паролем користувача	*Заходи безпеки* Призначення паролів повинне контролюватися за допомогою офіційно оформленого процесу управління.
А.11.2.4	Перегляд прав доступу користувача	*Заходи безпеки* Керівництво повинне переглядати права доступу користувача у встановлені терміни, використовуючи офіційно оформлену процедуру.
А.11.3 Відповідальності користувача *Ціль:* Запобігти несанкціонованому доступу користувача і компрометації або викраденню інформації та засобів оброблення інформації.		
А.11.3.1		*Заходи безпеки*

	Використання паролів	Треба вимагати від користувачів додержання визнаних практик безпеки у виборі та використанні паролів.
А.11.3.2	Обладнання користувачів, залишене без нагляду	*Заходи безпеки* Користувачі повинні забезпечити, що залишене без нагляду обладнання належним чином захищене.
А.11.3.3	Політика чистого стола та чистого екрану	*Заходи безпеки* Повинна бути ухвалена політика чистого стола щодо паперів і змінних носіїв пам'яті та політика чистого екрану щодо засобів оброблення інформації.
А.11.4 Контроль доступу до мережі *Ціль:* Запобігти несанкціонованому доступу до послуг мережі.		
А.11.4.1	Політика використання послуг мережі	*Заходи безпеки* Користувачам повинен надаватися доступ тільки до послуг, на використання яких вони мають санкцію.
А.11.4.2	Автентифікація користувача у зовнішніх підключеннях	*Заходи безпеки* Для контролю доступу віддалених користувачів повинні використовуватись відповідні методи автентифікації.
А.11.4.3	Ідентифікація обладнання в мережах	*Заходи безпеки* Автоматична ідентифікація обладнання повинна розглядатися як засіб автентифікації підключень з певного місця та певного обладнання.
А.11.4.4	Захист порту віддаленої	*Заходи безпеки* Фізичний і логічний доступ до портів

	діагностики та конфігурування	віддаленої діагностики та конфігурування повинен бути контрольований.
A.11.4.5	Сегментація у мережах	*Заходи безпеки* У мережі повинні бути сегментовані групи інформаційних послуг, користувачів, а також інформаційні системи.
A.11.4.6	Заходи безпеки щодо підключень до мережі	*Заходи безпеки* Для спільно використовуваних мереж, особливо тих, що поширюються поза межі організації, спроможність користувачів підключитися до мережі повинна бути обмежена відповідно до політики контролю доступу та вимог прикладних програм бізнесу (див.1.1)
A.11.4.7	Заходи безпеки щодо маршрутизації в мережі	*Заходи безпеки* Для мереж повинні бути впроваджені заходи безпеки щодо маршрутизації для забезпечення того, що підключення комп'ютерів і потоки інформації не порушують політику контролю доступу прикладних програм бізнесу.
A.11.5 Контроль доступу до операційної системи *Ціль:* Запобігти несанкціонованому доступу до операційних систем.		
A.11.5.1	Процедури безпечної реєстрації	*Заходи безпеки* Доступ до операційних систем повинен контролюватися процедурою безпечної реєстрації.
A.11.5.2	Ідентифікація та	*Заходи безпеки* Всі користувачі повинні мати унікальний

	автентифікація користувача	ідентифікатор (ID користувача) тільки для свого персонального використання та треба вибрати придатну методику автентифікації для підтвердження заявленої ідентичності користувача.
А.11.5.3	Система управління паролем	*Заходи безпеки* Системи для управління паролями повинні бути інтерактивними і забезпечувати якісні паролі.
А.11.5.4	Використання системних утиліт	*Заходи безпеки* Використання програм утиліт, що можуть бути спроможні скасовувати заходи безпеки системи та прикладних програм, повинно бути обмежене та суворо контрольоване.
А.11.5.5	Блокування неактивних сеансів	*Заходи безпеки* Неактивні сеанси повинні бути перервані після визначеного періоду бездіяльності.
А.11.5.6	Обмеження часу підключення	*Заходи безпеки* Для забезпечення додаткового захисту прикладних програм з високим ризиком треба використовувати обмеження часу підключення.
А.11.6 Контроль доступу до прикладних програм та інформації *Ціль:* Запобігти несанкціонованому доступу до інформації, що міститься в прикладних системах.		
А.11.6.1	Обмеження доступу до інформації	*Заходи безпеки* Доступ користувачів та обслуговуючого персоналу до інформації та функцій прикладних систем повинен бути

		обмежений відповідно до визначеної політики контролю доступу.
A.11.6.2	Ізоляція конфіденційних систем	*Заходи безпеки* Конфіденційні системи повинні мати спеціально призначене (ізольоване) комп'ютерне середовище.
A.11.7 Мобільні обчислення та дистанційна робота *Ціль:* Забезпечити безпеку інформації при використанні мобільних обчислень та засобів дистанційної роботи.		
A.11.7.1	Мобільні обчислення та комунікації	*Заходи безпеки* Для захисту від ризиків використання мобільного обчислення та комунікаційних засобів повинна бути наявною офіційно оформлена політика і повинні бути ухвалені відповідні заходи безпеки.
A.11.7.2	Дистанційна робота	*Заходи безпеки* Повинні бути розроблені та впроваджені політика, плани експлуатації та процедури щодо дистанційної роботи.
A.12 Придбання, розроблення та підтримка інформаційних систем		
A.12.1 Вимоги безпеки для інформаційних систем *Ціль:* Забезпечити, що безпека є невід'ємною частиною інформаційних систем.		
A.12.1.1	Аналіз та специфікація вимог безпеки	*Заходи безпеки* Положення щодо бізнес-вимог до нових інформаційних систем або модернізацій до існуючих інформаційних систем повинні визначати вимоги до заходів безпеки.

А.12.2 Коректне оброблення в прикладних програмах *Ціль:* Запобігти помилкам, втратам, несанкціонованій модифікації або зловживанню інформацією в прикладних програмах.		
А.12.2.1	Підтвердження вхідних даних	*Заходи безпеки* Вхідні дані для прикладних програм повинні бути підтверджені для забезпечення того, що ці дані є коректними та відповідними.
А.12.2.2	Заходи безпеки щодо внутрішньої обробки	*Заходи безпеки* Підтверджувальні перевірки повинні бути вбудовані у прикладні програми для виявлення будь-якого викривлення інформації через помилки обробки або навмисні дії.
А.12.2.3	Цілісність повідомлення	*Заходи безпеки* Повинні бути ідентифіковані вимоги щодо забезпечення автентичності та захисту цілісності повідомлень у прикладних програмах, належні заходи безпеки повинні бути ідентифіковані та впроваджені.
А.12.2.4	Підтвердження вихідних даних	*Заходи безпеки* Вихідні дані прикладної програми повинні бути підтверджені для забезпечення того, що оброблення інформації, яку зберігають, є коректним та відповідним до обставин.

А.12.3 Криптографічні заходи безпеки *Ціль:* Захистити конфіденційність, автентичність або цілісність інформації криптографічними засобами.		
А.12.3.1	Політика використання криптографічних засобів	*Заходи безпеки* Повинна бути розроблена і впроваджена політика використання криптографічних засобів для захисту інформації.
А.12.3.2	Управління ключами	*Заходи безпеки* Для підтримки використання в організації криптографічних методів повинно бути наявним управління ключами.
А.12.4 Безпека системних файлів *Ціль:* Забезпечити безпеку системних файлів.		
А.12.4.1	Заходи безпеки щодо програмного забезпечення, яке знаходиться в експлуатації	*Заходи безпеки* Повинні бути наявними процедури контролю інсталяції програмного забезпечення в системах, що знаходяться в експлуатації.
А.12.4.2	Захист даних для тестування системи	*Заходи безпеки* Дані для тестування повинні бути ретельно відібрані, захищені та контрольовані.
А.12.4.3	Контроль доступу до початкових кодів програми	*Заходи безпеки* Доступ до початкових кодів програми повинен бути обмежений.

А 12.5 Безпека у процесах розроблення та підтримки *Ціль :* Підтримувати безпеку прикладного програмного забезпечення та інформації.		
А.12.5.1	Процедури контролю змін	*Заходи безпеки* Впровадження змін повинно бути контрольованим за допомогою офіційно оформлених процедур контролю змін.
А.12.5.2	Технічний перегляд прикладних програм після змін операційної системи	*Заходи безпеки* Коли операційні системи змінено, критичні для бізнесу прикладні програми повинні бути переглянуті та протестовані, щоб забезпечити, що відсутній негативний вплив на функціонування та безпеку організації.
А.12.5.3	Обмеження на зміни до пакетів програмного забезпечення	*Заходи безпеки* Модифікації пакетів програмного забезпечення не повинні заохочуватися, бути обмеженими найнеобхіднішими змінами і всі зміни повинні суворо контролюватися.
А.12.5.4	Витік інформації	*Заходи безпеки* Треба запобігати можливостям витоку інформації.
А.12.5.5	Аутсорсингове розроблення програмного забезпечення	*Заходи безпеки* Організація повинна здійснювати нагляд над аутсорсинговим розробленням програмного забезпечення та його моніторинг.

А.12.6 Управління технічною вразливістю *Ціль:* Зменшити ризики в результаті використання відомостей щодо технічних вразливостей.		
А.12.6.1	Заходи безпеки, які стосуються технічних вразливостей	*Заходи безпеки* Треба отримувати своєчасну інформацію щодо технічних вразливостей інформаційних систем, що використовуються, оцінювати підвладність організації таким вразливостям і вживати належні заходи, щоб врахувати пов'язаний з цим ризик.
А.13 Управління інцидентом інформаційної безпеки		
А.13.1 Звітування щодо подій та слабких місць інформаційної безпеки *Ціль:* Забезпечити, що події інформаційної безпеки та слабкі місця, пов’язані з інформаційними системами, доведені до відома у спосіб, який дозволяє своєчасно вжити коригувальну дію.		
А.13.1.1	Звітування про події інформаційної безпеки	*Заходи безпеки* Необхідно якнайшвидше звітувати стосовно подій інформаційної безпеки через належні канали управління.
А.13.1.2	Звітування щодо слабких місць інформаційної безпеки	*Заходи безпеки* Треба вимагати від усього найманого персоналу, підрядників та користувачів третьої сторони, які користуються інформаційними системами та послугами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць у системах чи послугах.

А.13.2 Управління інцидентами інформаційної безпеки та вдосконаленням *Ціль:* Забезпечити застосування до управління інцидентами інформаційної безпеки послідовного та ефективного підходу.		
А.13.2.1	Відповідальності та процедури	*Заходи безпеки* Повинні бути розроблені відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.
А.13.2.2	Вивчення інцидентів інформаційної безпеки	*Заходи безпеки* Повинні бути наявними механізми, які дозволяють визначати кількість і здійснювати моніторинг типів, обсягів та вартості інцидентів інформаційної безпеки.
А.13.2.3	Збирання доказів	*Заходи безпеки* У випадках подальших дій проти особи чи організації після інциденту інформаційної безпеки, що тягнуть за собою судовий позов (цивільний або кримінальний), треба зібрати, зберегти та надати докази згідно з правилами щодо доказів відповідної юрисдикції.
А.14 Управління безперервністю бізнесу		
А.14.1 Аспекти інформаційної безпеки управління безперервністю бізнесу *Ціль:* Протидіяти перериванням у бізнес-діяльності та захищати критичні бізнес-процеси від впливу серйозних відмов інформаційних систем чи лиха і забезпечити їх своєчасне відновлення.		
А.14.1.1	Залучення інформаційної безпеки в процес	*Заходи безпеки* Для безперервності бізнесу в усій організації треба розробити та

	управління безперервністю бізнесу	підтримувати процес, що управляється, який враховує вимоги інформаційної безпеки, необхідні для безперервності бізнесу в організації.
А.14.1.2	Безперервність бізнесу та оцінка ризику	*Заходи безпеки* Події, що можуть спричинити переривання в бізнес-процесах, повинні бути ідентифіковані разом з імовірністю та впливом таких переривань і їх наслідків для інформаційної безпеки.
А.14.1.3	Розроблення та впровадження планів безперервності бізнесу, які включають інформаційну безпеку	*Заходи безпеки* Повинні бути розроблені та впроваджені плани для підтримки або поновлення функціонування і забезпечення доступності інформації на потрібному рівні та в потрібні проміжки часу після переривання чи відмови критичних бізнес процесів.
А.14.1.4	Структура планування безперервності бізнесу	*Заходи безпеки* Для забезпечення узгодженості всіх планів, узгодженого врахування вимог інформаційної безпеки та ідентифікації пріоритетів тестування і підтримки, повинна підтримуватись єдина структура планів безперервності бізнесу.

A.14.1.5	Тестування, підтримування та переоцінка планів безперервності бізнесу	*Заходи безпеки* Плани безперервності бізнесу треба регулярно тестувати та оновлювати, щоб забезпечити, що вони актуальні та ефективні.
A.15 Відповідність		
A.15.1 Відповідність правовим вимогам *Ціль:* Уникнути порушень будь-якого закону, вимог, що діють на підставі закону, нормативних або контрактних зобов'язань та будь-яких вимог безпеки.		
A.15.1.1	Ідентифікація застосовного законодавства	*Заходи безпеки* Усі важливі вимоги, що діють на підставі закону, нормативні або контрактні вимоги та підхід організації до задоволення цих вимог повинні бути чітко визначені, задокументовані та актуалізовані для кожної інформаційної системи та організації.
A.15.1.2	Права інтелектуальної власності (IPR)	*Заходи безпеки* Повинні бути впроваджені належні процедури забезпечення відповідності законодавчим, нормативним та контрактним вимогам щодо використання матеріалу, відносно якого можуть існувати права інтелектуальної власності, та щодо використання запатентованих продуктів програмного забезпечення.
A.15.1.3	Захист організаційних записів	*Заходи безпеки* Відповідно до вимог, що діють на підставі закону, нормативних, контрактних і бізнес вимог, важливі записи повинні бути

		захищені від втрати, знищення та фальсифікації.
A.15.1.4	Захист даних та конфіденційність персональних даних	*Заходи безпеки* Захист даних і конфіденційність повинні забезпечуватися згідно з вимогами відповідного законодавства, нормативів і, за наявності, статей контракту.
A.15.1.5	Запобігання зловживанню засобами оброблення інформації	*Заходи безпеки* Треба утримувати користувачів від використання засобів оброблення інформації для несанкціонованих цілей.
A.15.1.6	Нормативи щодо криптографічних засобів	*Заходи безпеки* Криптографічні засоби повинні використовуватися відповідно до усіх застосовних угод, законів та нормативів.
A.15.2 Відповідність політикам та стандартам безпеки і технічна відповідність *Ціль:* Забезпечити відповідність систем політикам та стандартам безпеки організації.		
A.15.2.1	Відповідність політикам та стандартам безпеки	*Заходи безпеки* Для досягнення відповідності політикам та стандартам безпеки керівники повинні забезпечити, що всі процедури безпеки в межах сфери їх відповідальності виконуються коректно.
A.15.2.2	Перевірка технічної відповідності	*Заходи безпеки* Інформаційні системи повинні регулярно перевірятися на відповідність стандартам впровадження безпеки.

А.15.3 Розгляд аудиту інформаційних систем *Ціль:* Мінімізувати втручання в процес аудиту інформаційних систем та максимізувати ефективність цього процесу.		
А.15.3.1	Заходи безпеки аудиту інформаційних систем	*Заходи безпеки* Вимоги аудиту та діяльність, що охоплює перевірки систем, що знаходяться в експлуатації, повинні бути ретельно сплановані та погоджені, щоб мінімізувати ризик порушення бізнес-процесів.
А.15.3.2	Захист інструментів аудиту інформаційних систем	*Заходи безпеки* Доступ до інструментів аудиту інформаційних систем повинен бути захищений, щоб запобігти будь-якому можливому зловживанню чи компрометації.

ДОДАТОК В

(довідковий)

ПРИНЦИПИ OECD І ЦЕЙ СТАНДАРТ

Принципи, наведені в Настановах OECD щодо безпеки інформаційних систем і мереж застосовні до всієї політики та функціональних рівнів, які впливають на безпеку інформаційних систем і мереж. Цей стандарт надає структуру системи управління інформаційною безпекою для впровадження деяких з принципів OECD з використанням моделі PDCA та процесів, описаних у розділах 4, 5, 6 та 8, згідно з указаним у таблиці В.1.

Таблиця В.1 - Принципи OECD і модель PDCA

Принципи OECD	**Відповідний ISMS процес та фаза PDCA**
Поінформованість Учасники повинні бути поінформовані щодо необхідності безпеки інформаційних систем і мереж і того, що вони можуть зробити для поліпшення безпеки.	Ця діяльність є частиною фази **Виконуй** (див. 4.2.2 та **5.2.2**).
Відповідальність Всі учасники є відповідальними за безпеку інформаційних систем і мереж.	Ця діяльність є частиною фази **Виконуй** (див. 4.2.2 та **5.1**).
Реагування Учасники повинні діяти своєчасно та спільно, щоб запобігати, виявляти та реагувати на інциденти безпеки.	Це є частиною діяльності з моніторингу фази **Перевіряй** (див. 4.2.3 і від 6 до 7.3) та діяльності з реагування **Дій** (див. 4.2.4 і від 8.1 до

	8.3). Також це може охоплюватися деякими аспектами фаз **Плануй** та **Перевіряй**.
Оцінка ризику Учасники повинні проводити оцінку ризику.	Ця діяльність є частиною фази **Плануй** (див. 4.2.1), а переоцінка ризику є частиною фази **Перевіряй** (див. 4.2.3 і від 6 до 7.3).
Проектування та впровадження безпеки Учасники повинні вбудовувати безпеку як суттєвий елемент інформаційних систем і мереж.	Після завершення оцінки ризику, як частина фази **Плануй** (див. 4.2.1)**,** обираються контролі для обробки ризиків. Далі фаза **Виконуй** (див. 4.2.2 та 5.2) охоплює впровадження та функціональне використання цих контролів.
Управління безпекою Учасники повинні прийняти комплексний (всебічний) підхід до управління безпекою.	Управління ризиком – це процес, що охоплює запобігання, виявлення та реагування на інциденти, поточну підтримку, перегляд і аудит. Усі ці аспекти здійснюють у фазах **Плануй, Виконуй**, **Перевіряй** та **Дій.**
Переоцінка Учасники повинні здійснювати перегляд і переоцінку безпеки інформаційних систем і мереж, і вносити належні модифікації у політики, практики, заходи і процедури безпеки.	Переоцінка інформаційної безпеки є частиною фази **Перевіряй** (див. 4.2.3 і від 6 до 7.3), де треба виконувати регулярні перегляди для перевірки ефективності системи управління інформаційною безпекою, а вдосконалення безпеки є частиною фази **Дій** (див. 4.2.4 і від 8.1 до 8.3).

ДОДАТОК С

(довідковий)

ВІДПОВІДНІСТЬ МІЖ ISO 9001:2000, ISO 14001:2004 ТА ЦИМ СТАНДАРТОМ

Таблиця С.1 показує відповідність між ISO 9001:2000, ISO 14001:2004 та цим стандартом.

Таблиця С.1 - Відповідність між ISO 9001:2000, ISO 14001:2004 та цим стандартом

Цей стандарт	ISO 9001:2000	ISO 14001:2004
0 Вступ 0.1 Загальні положення 0.2 Процесний підхід 0.3 Сумісність з іншими системами управління	**0 Вступ** 0.1 Загальні положення 0.2 Процесний підхід 0.3 Взаємозв'язок з ISO 9004 0.4 Сумісність з іншими системами управління	**Вступ**
1 сфера застосування 1.1 Загальні положення 1.2 Застосування	**1 Сфера застосування** 1.1 Загальні положення 1.2 Застосування	**1 Сфера застосування**
2 Нормативні посилання	**2 Нормативні посилання**	**2 Нормативні посилання**
3 Терміни та визначення понять	**3 Терміни та визначення понять**	**3 Терміни та визначення понять**
4 Система управління інформаційною безпекою 4.1 Загальні вимоги 4.2 Розроблення та	**4 Система управління якістю** 4.1 Загальні вимоги	**4 Вимоги системи управління навколишнім середовищем** 4.1 Загальні вимоги

управління СУІБ 4.2.1 Розроблення СУІБ 4.2.2 Впровадження та функціонування СУІБ 4.2.3 Моніторинг і перегляд СУІБ 4.2.4 Підтримування та впровадження СУІБ	 8.2.3 Моніторинг і вимірювання процесів 8.2.4 Моніторинг і вимірювання продукту	 4.4 Впровадження та функціонування 4.5 Моніторинг і вимірювання
4.3 Вимоги до документації 4.3.1 Загальні положення 4.3.2 Контроль документів 4.3.3 Контроль записів	4.2 Вимоги до документації 4.2.1 Загальні положення 4.2.2 Настанови щодо якості 4.2.3 Контроль документів 4.2.4 Контроль записів	 4.4.5 Контроль документації 4.5.4 Контроль записів
5 Відповідальність керівництва 5.1 Обов’язки керівництва	**5 Відповідальність керівництва** 5.1 Обов’язки керівництва 5.2 Користувацькі аспекти 5.3 Політика якості 5.4 Планування 5.5 Відповідальність, повноваги та інформаційна взаємодія	 4.2 Політика щодо середовища 4.3 Планування
5.2 Управління ресурсами 5.2.1 Надання ресурсів 5.2.2 Навчання,	**6 Управління ресурсами** 6.1 Надання ресурсів 6.2 Людські ресурси 6.2.2 Компетентність,	 4.2.2 Компетентність,

поінформованість і компетентність	поінформованість і навчання 6.3 Інфраструктура 6.4 Виробниче середовище	навчання та поінформованість
6 Внутрішні аудити СУІБ	8.2.2 Внутрішній аудит	4.5.5 Внутрішній аудит
7 Перегляд СУІБ з боку керівництва 7.1 Загальні положення 7.2 Вхідні дані для перегляду 7.3 Вихідні дані перегляду	**5.6 Перегляд з боку керівництва** 5.6.1 Загальні положення 5.6.2 Вхідні дані для перегляду 5.6.3 Вихідні дані перегляду	**4.6 Перегляд з боку керівництва**
8 Вдосконалення СУІБ 8.1 Постійне вдосконалення	**8.5 Вдосконалення** 8.5.1 Постійне вдосконалення	
8.2 Коригувальні дії	8.5.3 Коригувальні дії	4.5.3 Невідповідність, коригувальні дії та запобіжні дії
8.3 Запобіжні дії	8.5.3 Запобіжні дії	
Додаток А. Цілі контролів і контролі **Додаток В. Принципи OECD і цей стандарт** **Додаток С. Відповідність між ISO 9001:2000, ISO 14001:2004 та цим стандартом**	**Додаток А. Відповідність між ISO 9001:2000 і ISO 14001:2004**	**Додаток А. Настанова щодо використання цього стандарту** **Додаток В. Відповідність між ISO 14001:2004 і ISO 9001:2000**

БІБЛІОГРАФІЯ

Опубліковані стандарти

[1]. ISO 9001:2000, Quality management systems — Requirements

[2]. ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[3]. ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security

[4]. ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards

[5]. ISO 14001:2004, Environmental management systems — Requirements with guidance for use

[6]. ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management

[7]. ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

[8]. ISO/IEC Guide 62:1996, General requirements for bodies operating assessment and certification/registration of quality systems

[9]. ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards

[10]. ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management.

ПОЯСНЕННЯ.

[1]. ISO 9001:2000, Системи управління якістю. Вимоги.

[2]. ISO/IEC 13335-1:2004, Інформаційні технології. Методи захисту. Управління безпекою інформаційних та комунікаційних технологій. Частина 1. Концепції та моделі управління безпекою інформаційних та комунікаційних технологій

[3]. ISO/IEC TR 13335-3:1998, Інформаційні технології. Настанови щодо управління безпекою ІТ. Частина 3. Методи управління безпекою ІТ.

[4]. ISO/IEC TR 13335-4:2000, Інформаційні технології. Настанови щодо управління безпекою ІТ. Частина 4. Вибір засобів захисту.

[5]. ISO 14001:2004, Системи управління навколишнім середовищем. Вимоги з настановою щодо використання.

[6]. ISO/IEC TR 18044:2004, Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки.

[7]. ISO 19011:2002, Настанови щодо аудиту систем управління якістю та/або навколишнім середовищем.

[8]. ISO/IEC Guide 62:1996, Настанова 62:1996. Загальні вимоги до органів, які виконують оцінку та сертифікацію/реєстрацію систем якості.

[9]. ISO/IEC Guide 73:2002, Настанова73:2002. Управління ризиками. Словник. Настанови щодо використання у стандартах.

[10]. ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою.

Інші публікації

[11]. OECD, Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

[12]. NIST SP 800-30, Risk Management Guide for Information Technology Systems

[13]. Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986

ПОЯСНЕННЯ.

[11]. OECD, Настанови щодо безпеки інформаційних систем і мереж. Щодо культури безпеки. Париж. OECD, Липень, 2002. www.oecd.org

[12]. NIST SP 800-30, Остання інформація Національного інституту стандартів і технологій США 800-30. Настановчі принципи з управління ризиками для систем інформаційних технологій.

[13]. Демінг В.І., Поза кризою. Кембридж, Массачусетс. Массачусетський технологічний інститут, Центр сучасних інженерних досліджень, 1986.

Код УКНД 35.040