НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

ГСТУ СУІБ 2.0/ISO/IEC 27002:2010

ГАЛУЗЕВИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

МЕТОДИ ЗАХИСТУ

ЗВІД ПРАВИЛ ДЛЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

(ISO/IEC 27002:2005, MOD)

Видання офіційне

Київ

НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

2010

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. наук, Т.Тищенко

ВНЕСЕНО Національним банком України

УЗГОДЖЕНО

2 ЗАТВЕРДЖЕНО І ВВЕДЕНО В ДІЮ Постановою Правління Національного банку України від_____ № _____

3 Цей стандарт відповідає ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою).

Ступінь відповідності – модифікований (MOD)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

5 ЗАРЕЄСТРОВАНО „Українським науково-дослідним і навчальним центром проблем стандартизації, сертифікації та якості” (УкрНДНЦ) від_____ № ____

З М І С Т

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є прийнятий зі змінами ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою).

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. Технічні відхили і додаткову інформацію було долучено безпосередньо до пунктів, яких вони стосуються, їх позначено подвійною рамкою та заголовком „Національний відхил”, „Національне пояснення” або „Національна примітка”. 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”, „Національний вступ”, – оформлено згідно з вимогами національної стандартизації України;

- у розділі „Нормативні посилання” наведено українською мовою „Національне пояснення”, виділене в тексті рамкою.

0 Вступ

0.1 Що таке інформаційна безпека?

Інформація є активом, який подібно іншим важливим діловим активам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов'язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов'язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та вразливостей (див. також OECD Guidelines for the Security of Information Systems and Networks).

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ.

Рекомендації Організації економічного співробітництва та розвитку щодо безпеки інформаційних систем та мереж.

Інформація може існувати у багатьох формах. Вона може бути надрукована або написана на папері, збережена в електронному вигляді, переслана поштою або з використанням електронних засобів, показана на плівці або сповіщена у бесіді. Незалежно від набутого виду інформації або засобів, за допомогою яких вона поширюється або зберігається, вона повинна завжди бути відповідно захищена.

Інформаційна безпека - це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес ризику і максимізації рентабельності інвестицій і бізнес можливостей.

Інформаційна безпека досягається впровадженням відповідного набору контролів, який охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції. Ці контролі необхідно розробити, впровадити, моніторити, переглядати та, за необхідності, вдосконалювати для гарантування того, що певні безпека та бізнес-цілі організації будуть досягнуті. Це треба виконувати узгоджено з іншими процесами управління бізнесом.

Національна примітка.

Питання щодо інформаційної безпеки визначаються Законами України:

Про інформацію;
Про захист інформації в інформаційно-телекомуникаційних системах;
Про електронний документ і електронний документообіг;
Про електронний цифровий підпис.

Питання інформаційної безпеки для банківської діяльності визначаються Законами України:

Про Національний банк України;
Про банки і банківську діяльність;
Про платіжні системи та переказ коштів в Україні;

та нормативними документами Національного банку України.

0.2 Навіщо потрібна інформаційна безпека?

Інформація та допоміжні процеси, системи і мережі є важливими бізнес-активами. Визначення, досягнення, підтримка та вдосконалення інформаційної безпеки може бути суттєвим для підтримки конкурентоспроможності, готівкового обігу, рентабельності, відповідності законодавству та комерційної репутації.

Організації та їхні інформаційні системи й мережі натрапляють на загрози безпеці від широкого кола джерел, охоплюючи комп'ютерне шахрайство, шпіонаж, саботаж, вандалізм, пожежу або повінь. Причини порушень типу зловмисних кодів, комп'ютерного хакерства і атак типу відмови в обслуговуванні стали більш поширеними і значно досконалішими.

Інформаційна безпека є важливою як для державного і приватного секторів бізнесу, так і для захисту критичних інфраструктур. В обох секторах інформаційна безпека буде працювати як фактор сприяння, наприклад, в електронному урядуванні або електронному бізнесі, або для уникнення чи зменшення відповідних ризиків. Взаємозв'язок загальнодоступних і приватних мереж та спільне використання інформаційних ресурсів збільшують труднощі в досягненні контролю доступу. Тенденція до розподіленого оброблення даних може також послабити ефективність централізованого, фахового контролю.

Багато інформаційних систем не проектувалися як безпечні. Безпека, яка може бути досягнута за допомогою технічних засобів, є обмеженою і має підтримуватись відповідним управлінням та процедурами. Визначення, які контролі треба застосовувати на місці, вимагає ретельного планування та уваги до подробиць. Управління інформаційною безпекою вимагає щонайменше участі всього персоналу організації. Воно може також вимагати співучасті від акціонерів, постачальників, третіх сторін, користувачів або інших зовнішніх сторін. Рекомендації фахівців із сторонніх організацій також можуть стати в нагоді.

0.3 Як розробити вимоги безпеки

Важливо, щоб організація ідентифікувала свої вимоги безпеки. Є три основні джерела формування вимог безпеки.

1. Одне джерело отримують з оцінки ризиків для організації, беручи до уваги загальну бізнес-стратегію організації та цілі. Під час оцінювання ризику ідентифікують загрози активам і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу.

2. Іншим джерелом є правові вимоги, ті, що діють на підставі закону, нормативні та контрактні вимоги, які організація, її торгові партнери, підрядники та постачальники послуг повинні задовольняти, а також їх соціально-культурне середовище.

3. Ще одним джерелом є власний набір принципів, цілей та бізнес-вимог щодо оброблення інформації, який організація розробила для підтримки свого функціонування.

0.4 Оцінка ризиків безпеки

Вимоги безпеки ідентифікуються систематичною оцінкою ризиків безпеки. Витрати на контролі повинні бути збалансовані з бізнес-втратами, які можуть бути наслідком порушень безпеки.

Результати оцінки ризику допомагатимуть спрямовувати і визначити

відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки і впровадження контролів, вибраних для захисту від цих ризиків.

Оцінка ризиків повинна періодично повторюватися для врахування будь-яких змін, які можуть вплинути на результати оцінки ризику.

Більше інформації щодо оцінки ризиків безпеки можна знайти в розділі 4.1 „Оцінка ризиків безпеки”.

0.5 Вибір контролів

Як тільки вимоги безпеки та ризики ідентифіковано і рішення щодо оброблення ризиків прийнято, повинні бути вибрані та впроваджені відповідні контролі для забезпечення зниження ризиків до прийнятного рівня. Контролі можна вибирати з цього стандарту або інших наборів контролів, або якщо необхідно можна спроектувати нові контролі для задоволення певних потреб. Вибір контролів безпеки залежить від управлінських рішень, основаних на критеріях прийняття ризику, варіантах обробки ризику та загальному підході до управління ризиком, застосовному в організації, і повинен також відповідати усьому чинному національному й міжнародному законодавству та нормативним документам.

Деякі з контролів в цьому стандарті можуть розглядатися як настановні принципи щодо управління інформаційною безпекою, які можуть бути застосовані для більшості організацій. Вони пояснюються більш детально нижче під заголовком „Відправна точка інформаційної безпеки”.

Більше інформації щодо вибору контролів та інших варіантів обробки ризику можна знайти в розділі 4.2 „Обробка ризиків безпеки”.

0.6 Відправна точка інформаційної безпеки

Низку контролів можна розглядати як хорошу відправну точку для впровадження інформаційної безпеки. Вони або базуються на основних законодавчих вимогах, або розглядаються як звичайна практика інформаційної безпеки.

Контролі, які вважаються суттєвими для організації з законодавчої точки зору, містять, залежно від застосовного законодавства:

a) захист даних та конфіденційність персональної інформації (див. 15.1.4);
b) захист записів організації (див. 15.1.3);
c) права інтелектуальної власності (див. 15.1.2).

Контролі, які вважаються звичайною практикою інформаційної безпеки, містять:

a) документ політики інформаційної безпеки (див. 5.1.1);
b) розподіл відповідальностей щодо інформаційної безпеки (див. 6.1.3);
c) поінформованість, освіта і навчання з інформаційної безпеки (див. 8.2.2);
d) правильне оброблення інформації у прикладних програмах (див. 12.2);
e) управління технічною вразливістю (див. 12.6);
f) управління безперервністю бізнесу (див. 14);

g) управління інцидентами інформаційної безпеки та вдосконаленнями (див. 13.2).

Ці контролі застосовують у більшості організацій та у більшості середовищ.

Треба відзначити, що, хоча всі контролі в цьому стандарті є важливими і повинні бути розглянутими, важливість кожного контролю повинна визначатися з позицій певного ризику, з яким стикається організація. Отже, хоча вищевикладений підхід розглядається як хороша відправна точка, він не замінює вибору контролів, основаного на оцінці ризику.

0.7 Критичні фактори успіху

Досвід показує, що нижченаведені фактори часто є критичними для успішного впровадження інформаційної безпеки в організації:

a) політика інформаційної безпеки, цілі та діяльність, які відображують цілі бізнесу;

b) підхід та основні правила впровадження, підтримання, моніторингу та вдосконалення інформаційної безпеки, сумісні з культурою організації;

c) очевидна підтримка та зобов'язання керівництва усіх рівнів;

d) добре розуміння вимог інформаційної безпеки, оцінки ризику та управління ризиком;

e) ефективне доведення та роз'яснення інформаційної безпеки до всіх керівників, працівників та інших сторін для досягнення поінформованості;

f) розповсюдження настанов щодо політики інформаційної безпеки та стандартів всім керівникам, працівникам та іншим сторонам;

g) забезпечення фінансування діяльності з управління інформаційною безпекою;

h) забезпечення відповідних поінформованості, навчання та освіти;

i) розроблення ефективного процесу управління інцидентами інформаційної безпеки;

j) впровадження системи вимірювань[1], яка використовується для оцінювання продуктивності управління інформаційною безпекою і пропозицій зворотного зв'язку для вдосконалення.

0.8 Розвиток ваших власних настанов

Цей звід правил може розцінюватись як відправна точка для розвитку конкретних певних настанов організації. Не всі контролі та настанови з цього зводу правил можуть бути застосовні. Крім того, можуть бути потрібні додаткові контролі та настанови, не включені до цього стандарту. Під час розроблення документів, які містять додаткові настанови чи контролі, може бути корисним наводити в тих місцях, де це необхідно, перехресні посилання на розділи цього стандарту для полегшення перевірки відповідності аудиторами та бізнес-партнерами.

[1] Треба зазначити, що вимірювання інформаційної безпеки виходять за межі цього стандарту.

ГАЛУЗЕВИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. МЕТОДИ ЗАХИСТУ. **ЗВІД ПРАВИЛ ДЛЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ**

Інформационные технологии. Методы защиты.
Свод правил для управления информационной безопасностью

Information technology. Security techniques.
Code of practice for information security management

1 Галузь застосування

Цей стандарт встановлює настанови та загальні принципи щодо започаткування, впровадження, підтримки та вдосконалення управління інформаційною безпекою в організації. Цілі, окреслені в цьому стандарті, надають основні настанови щодо загальноприйнятих цілей управління інформаційною безпекою.

Цілі контролів та контролі цього стандарту призначені для впровадження з метою задоволення вимог, ідентифікованих оцінкою ризику. Цей стандарт може слугувати практичною настановою для розвитку стандартів безпеки в організації та практики ефективного управління безпекою, і для допомоги в побудові конфіденційності в діяльності організації.

2 Терміни та визначення

Для цілей цього документа використовуються наведені нижче терміни та визначення.

2.1 актив (*asset*)

усе, що має цінність для організації [ISO/IEC 13335-1:2004]

Національна примітка.

До активів слід віднести усе, що повинно враховуватися для забезпечення ефективного управління інформаційною безпекою, включаючи інформацію в електронному та паперовому вигляді, програмне та апаратне забезпечення, персонал тощо.

2.2 контроль (*control*)

засоби управління ризиком, які охоплюють політику, процедури, настанови, практику або організаційні структури, які можуть бути адміністративного, технічного, управлінського або правового характеру

ПРИМІТКА. Контроль також використовується як синонім засобу захисту або контрзаходу.

2.3 настанова (*guideline)*

опис, який пояснює, що треба зробити і як, для досягнення встановлених в політиках цілей

[ISO/IEC 13335-1:2004]

2.4 засоби оброблення інформації (*information processing facilities)*

будь-яка система оброблення інформації, послуга чи інфраструктура/фізичний вузол, де вони розміщені

Національна примітка.

Для банків України засобами оброблення інформації можуть бути власні програмно-технічні комплекси або автоматизовані робочі місця державних/міжнародних платіжних/інформаційних систем.

2.5 інформаційна безпека (*information security*)

Збереження конфіденційності, цілісності та доступності інформації; крім того можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність

Національна примітка.

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

2.6 подія інформаційної безпеки (information security event)

подією інформаційної безпеки є ідентифікований стан системи, служби або мережі, який указує на можливе порушення політики інформаційної безпеки чи відмови засобів захисту або раніше невідому ситуацію, яка може мати відношення до безпеки [ISO/IEC TR 18044:2004]

2.7 інцидент інформаційної безпеки (*information security incident*)

на інцидент інформаційної безпеки вказує одна або серія небажаних або непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації функціонування бізнесу і загрози інформаційній безпеці [ISO/IEC TR 18044:2004]

2.8 політика (*policy*)

загальні наміри та вказівки, затверджені керівництвом

2.9 ризик (*risk)*

комбінація ймовірності події та її наслідку [ISO/IEC Guide 73:2002]

2.10 аналізування ризику (*risk analysis*)

систематичне використання інформації для ідентифікації джерел та кількісного оцінювання ризиків [ISO/IEC Guide 73:2002]

2.11 оцінка ризику (*risk assessment*)

загальний процес аналізування ризику та оцінювання ризику [ISO/IEC Guide 73:2002]

2.12 оцінювання ризику (*risk evaluation*)

процес порівняння кількісно оціненого ризику із заданими критеріями ризику для встановлення його значимості [ISO/IEC Guide 73:2002]

2.13 управління ризиком (*risk management*)

скоординовані дії в організації щодо регулювання та контролю ризику [ISO/IEC Guide 73:2002]

Примітка. Управління ризиком зазвичай містить оцінку ризику, оброблення ризику, прийняття ризику і доведення ризику до відома

2.14 оброблення ризику (*risk treatment*)

процес вибору та впровадження заходів щодо модифікації ризику [ISO/IEC Guide 73:2002]

2.15 третя сторона (*third party*)

особа або орган, визнані як незалежними від залучених сторін, так і зацікавленими в розглядуваній проблемі [ISO/IEC Guide 2:1996]

2.16 загроза (*threat*)

потенційна причина небажаного інциденту, який може призвести до шкоди для системи або організації [ISO/IEC 13335-1:2004]

2.17 вразливість (*vulnerability*)

слабкість активу або групи активів, якою можуть скористатися одна або більше загроз [ISO/IEC 13335-1:2004]

3 Побудова цього стандарту

Цей стандарт містить 11 розділів контролів безпеки, які разом охоплюють загалом 39 основних категорій безпеки, а також один вступний розділ, який вводить оцінювання та оброблення ризику.

3.1 Розділи

Кожний розділ містить певну кількість основних категорій безпеки. Одинадцять розділів (супроводжувані певною кількістю основних категорій безпеки, розміщених в кожному розділі):

a) Політика безпеки (1);

b) Організація інформаційної безпеки (2);

c) Управління активами (2);

d) Безпека людських ресурсів (3);

e) Фізична безпека та безпека інфраструктури (2);

f) Управління взаємодією та функціонуванням (10);

g) Контроль доступу (7);

h) Придбання, розроблення і підтримка інформаційних систем (6);

i) Управління інцидентом інформаційної безпеки (2);

j) Управління безперервністю бізнесу (1);

k) Відповідність (3).

Примітка: Порядок розділів у цьому стандарті не означає їх важливості. Залежно від обставин усі розділи можуть бути важливими, тому кожна організація, яка застосовує цей стандарт, повинна ідентифікувати застосовні розділи, наскільки вони важливі та необхідність їх застосування до конкретного бізнес-процесу. Крім того, усі переліки в цьому стандарті не впорядковано у пріоритетному порядку, якщо це не зазначено.

3.2 Основні категорії безпеки

Кожна основна категорія безпеки містить:

a) ціль контролю, яка визначає, чого треба досягти; та

b) один або більше контролів, які можуть бути застосовані для досягнення цілі контролю.

Описи контролів структуровані нижченаведеним чином:

Контроль

Визначає певне положення щодо контролю для досягнення цілі контролю.

Настанова щодо впровадження

Надає більш детальну інформацію для підтримки впровадження контролю та досягнення цілі контролю. Деякі з цих настанов можуть бути придатними не у всіх випадках і, отже, можуть бути більш прийнятними інші шляхи впровадження контролю.

Додаткова інформація

Надає подальшу інформацію, яка може потребувати розгляду, наприклад, правові міркування та посилання та інші стандарти.

4 Оцінка та оброблення ризиків

4.1 Оцінка ризиків безпеки

Оцінка ризиків повинна ідентифікувати і визначити величини і пріоритети ризиків в залежності від критеріїв прийняття ризику і суттєвих цілей організації. Результати повинні спрямувати й визначити відповідні дії та пріоритети з управління ризиками інформаційної безпеки та з –провадження контролів, вибраних для захисту від цих ризиків. Потреба в проведенні процесу оцінки ризиків та вибору контролів може виникнути -декілька разів, щоб охопити різні підрозділи організації або окремі інформаційні системи.

Оцінка ризиків повинна містити системний підхід до визначення кількісно оціненого ризику (аналізування ризику) та процес порівняння кількісно оцінених ризиків з критеріями ризику для встановлення його значимості (визначення ризику).

Оцінки ризиків повинні також проводитись періодично для урахування змін у вимогах безпеки і ситуації з ризиками, наприклад, щодо активів, загроз, вразливостей, значних впливів, оцінювання ризику, а також коли відбуваються значні зміни. Ці оцінки ризиків треба здійснювати системним способом, який надає можливість отримати порівнювані та відтворювані результати.

Оцінка ризиків інформаційної безпеки задля її ефективності повинна мати чітко визначену галузь застосування і повинна мати взаємозв’язки з оцінками ризиків в інших сферах, якщо необхідно.

Галуззю застосування оцінки ризиків може бути або вся організація, підрозділи організації, окрема інформаційна система, певні компоненти системи або послуги, для яких це є практично здійсненним, прагматичним та корисним. Приклади методології оцінки ризиків обговорюються в ISO/IEC TR 13335-3 (Guidelines for the Management of IT Security: Techniques for the Management of IT Security*).*

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ**.**

ISO/IEC TR 13335-3, Настанови з управління безпекою ІТ: Методи управління безпекою ІТ.

Національна примітка.

Банки України використовують декілька програмно-технічних комплексів автоматизації банківської діяльності, які постійно обмінюються інформацією, тому галуззю застосування оцінки ризиків повинен бути весь банк в цілому.

4.2 Оброблення ризиків безпеки

До початку оброблення ризику, організація повинна встановити критерії прийняття ризиків. Ризики можуть бути прийняті, якщо, наприклад, оцінено, що ризик є невеликим або вартість оброблення ризику є нерентабельною для організації. Такі рішення повинні бути задокументовані.

Для кожного з ризиків, ідентифікованих після оцінки ризику, треба

прийняти рішення щодо оброблення ризиків. Можливі варіанти оброблення ризиків включають:

a) застосування належних контролів для зниження ризиків;

b) свідоме й об’єктивне прийняття ризиків із забезпеченням, що вони чітко задовольняють політику організації та критерії прийняття ризику;

c) уникнення ризиків не дозволяючи дії, які можуть спричинити виникнення ризиків;

d) перенесення пов’язаних ризиків на інші сторони, наприклад, страхувальників або постачальників.

Для ризиків, для яких рішенням щодо оброблення ризику є застосування належних контролів, ці контролі повинні бути обрані та впроваджені таким чином, щоб задовольнити вимоги, ідентифіковані оцінкою ризиків. Контролі повинні забезпечити зниження ризиків до прийнятного рівня, беручи до уваги:

a) вимоги та обмеження національного і міжнародного законодавства та нормативів;

b) цілі організації;

c) функціональні вимоги та обмеження;

d) вартість впровадження та функціонування, пов’язану зі знижуваними ризиками, і збереження її пропорційності вимогам та обмеженням організації;

e) необхідність балансу між інвестиціями у впровадження та функціонування контролів і ймовірною шкодою, до якої можуть призвести відмови політики безпеки.

Контролі можна вибрати з цього стандарту або з інших наборів контролів, або можна спроектувати нові контролі для задоволення певних потреб організації. Необхідно усвідомити, що деякі контролі можуть бути не применимим для кожної інформаційної системи або інфраструктури і можуть бути практично не здійсненими для всіх організацій. Як приклад, 10.1.3 описує, як можуть бути розподілені обов’язки для попередження шахрайства та помилки. Для невеликих організацій може бути неможливим розподілення всіх обов’язків і можуть бути необхідними інші шляхи досягнення тієї ж цілі контролю. Інший приклад, 10.10 описує, як можна здійснювати моніторинг використання системи і збирати докази. Описані контролі, наприклад, реєстрація події, можуть суперечити чинному законодавству, наприклад, захисту конфіденційності клієнтів або робочих місць.

Контролі інформаційної безпеки повинні розглядатися на стадіях визначення вимог до систем і проектів та на етапі проектування. Відмова від цього може призвести до додаткових витрат і менш ефективних рішень і, можливо, у гіршому випадку, до неможливості досягти необхідної безпеки.

Треба мати на увазі, що з жодним набором контролів не можна досягти повної безпеки, і що додаткові дії з управління повинні бути впроваджені для моніторингу, оцінювання та вдосконалення дієвості та ефективності контролів безпеки для підтримки прагнень організації.

5 Політика безпеки

5.1 Політика інформаційної безпеки

Ціль: Забезпечити регулювання та підтримку з боку керівництва інформаційної безпеки згідно з вимогами бізнесу та відповідними законами і нормативами.

Відповідно до цілей бізнесу керівництво повинне встановити чітке регулювання політики і продемонструвати підтримку та зобов'язання щодо інформаційної безпеки виданням політики інформаційної безпеки та її підтримкою в організації.

5.1.1 Документ щодо політики інформаційної безпеки

Контроль

Документ щодо політики інформаційної безпеки повинен бути затверджений керівництвом, виданий та доведений до відома всього найманого персоналу та потрібних зовнішніх сторін.

Настанова щодо впровадження

Документ політики інформаційної безпеки повинен встановити зобов'язання керівництва і викласти підхід організації до управління інформаційною безпекою. Документ політики повинен містити положення стосовно:

a) визначення інформаційної безпеки, її загальних цілей і галузі застосування, а також важливості безпеки як механізму уможливлення розповсюдження інформації (див. вступ);

b) положення щодо намірів і підтримки керівництвом мети та принципів інформаційної безпеки згідно з бізнес-стратегією та цілями;

c) основ встановлення цілей контролю і контролів, охоплюючи структуру оцінки ризику та управління ризиком;

d) короткого пояснення особливо важливих для організації політики безпеки, принципів, стандартів безпеки і вимог щодо відповідності, охоплюючи:

1) відповідність законодавчим, нормативним та контрактним вимогами;

2) вимоги до освіти, навчання та поінформованості персоналу щодо безпеки;

3) управління безперервністю бізнесу;

4) наслідки порушення політики інформаційної безпеки;

e) визначення загальних та спеціальних відповідальностей з управління інформаційною безпекою, включаючи звітування щодо інцидентів інформаційної безпеки;

f) посилань на документацію, яка може підтримувати політику, наприклад, більш детальні політики та процедури для певних інформаційних систем або правила безпеки, які користувачі повинні виконувати.

Національна примітка.

Рекомендується розробити більш детальні політики та процедури або правила безпеки, які користувачі повинні виконувати, як складову частину політики інформаційної безпеки.

Ця політика інформаційної безпеки повинна бути доведена до відома користувачів всієї організації у відповідній, доступній та зрозумілій для читача, якому вона призначена, формі.

Національна примітка.

Рекомендується ознайомлювати з політикою інформаційної безпеки користувачів всієї організації під власноручний підпис.

Додаткова інформація

Політика інформаційної безпеки може бути частиною документа щодо загальної політики. Якщо політика інформаційної безпеки поширюється за межі організації, треба подбати про не розголошення чутливої інформації. Додаткову інформацію можна знайти в ISO/IEC 13335-1:2004.

5.1.2 Перегляд політики інформаційної безпеки

Контроль

Політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її постійної придатності, адекватності та ефективності.

Настанова щодо впровадження

Політика інформаційної безпеки повинна мати власника, який несе затверджену керівництвом відповідальність за розвиток, перегляд і оцінювання політики безпеки. Перегляд повинен охоплювати оцінку можливостей вдосконалення політики інформаційної безпеки організації і підхід до управління інформаційною безпекою в разі змін інфраструктури організації, бізнес обставин, правових умов або технічної інфраструктури.

Перегляд політики інформаційної безпеки повинен враховувати результати переглядів з боку керівництва. Повинні бути визначені процедури перегляду з боку керівництва, охоплюючи графік або періодичність перегляду.

Вхідні дані для перегляду керівництвом повинні містити інформацію щодо:

a) зворотного зв’язку від зацікавлених сторін;

b) результатів незалежних переглядів (див. 6.1.8);

c) статусу запобіжних та коригувальних дій (див. 6.1.8 та 15.2.1);

d) результатів попередніх переглядів з боку керівництва;

e) продуктивності процесів та відповідності політиці інформаційної безпеки;

f) змін, які можуть вплинути на підхід організації до управління інформаційною безпекою, охоплюючи зміни в інфраструктурі організації, бізнес-обставинах, доступності ресурсів, контрактних, нормативних і правових умовах або в технічній інфраструктурі;

g) тенденцій щодо загроз та вразливостей;

h) зареєстрованих інцидентів інформаційної безпеки (див. 13.1);

і) рекомендацій, наданих відповідними повноважними організаціями (див. 6.1.6).

Національна примітка.

В якості рекомендацій, наданих відповідними повноважними організаціями, банки України повинні використовувати нормативні документи та рекомендації Національного банку України.

Вихідні дані перегляду з боку керівництва повинні містити будь-які рішення та дії стосовно:

a) вдосконалення підходу організації до управління інформаційною безпекою та її процесами;

b) вдосконалення цілей контролів та контролів;

c) вдосконалення розподілу ресурсів та/або відповідальностей.

Повинна підтримуватися реєстрація переглядів з боку керівництва.

Переглянута політика повинна бути затверджена керівництвом.

6 Організація інформаційної безпеки

6.1 Внутрішня організація

Ціль: Управляти інформаційною безпекою в організації.

Повинна бути встановлена структура управління для започаткування та контролю впровадження інформаційної безпеки в організації.

Керівництво повинно затвердити політику інформаційної безпеки, призначити ролі щодо безпеки і координувати та переглядати впровадження безпеки в організації.

За необхідності, в організації повинне бути створене джерело рекомендацій фахівців з інформаційної безпеки і забезпечений доступ до нього. Треба розвинути контакти з зовнішніми фахівцями або групами, включаючи відповідні повноважні організації, щоб не відставати від промислових тенденцій, здійснювати моніторинг стандартів та методів оцінки і забезпечити можливість обговорення під час оброблення інцидентів інформаційної безпеки. Необхідно заохочувати багатоплановий підхід до інформаційної безпеки.

Національна примітка.

Банки повинні мати групу/підрозділ з фахівців з питань інформаційної безпеки (адміністраторів захисту інформації) для забезпечення впровадження та підтримки системи управління інформаційною безпекою.

6.1.1 Зобов'язання керівництва щодо інформаційної безпеки

Контроль

Керівництво повинно активно підтримувати безпеку в межах організації шляхом чіткого регулювання, підтверджених зобов'язань, чітких призначень та визнання відповідальності за інформаційну безпеку.

Національна примітка.

Керівництво банку повинно затвердити наказом призначення відповідальних за інформаційну безпеку та розподіл повноважень між ними. Усі працівники банку мають власноруч підписати зобов'язання щодо відповідальності за виконання вимог з інформаційної безпеки та інструкцій щодо використання засобів захисту інформації.

Настанова щодо впровадження

Керівництво повинно:

a) забезпечити, щоб задачі інформаційної безпеки були визначені, відповідали вимогам організації і були інтегровані у відповідні процеси;

b) сформулювати, переглядати і затверджувати політику інформаційної безпеки;

c) переглядати ефективність впровадження політики інформаційної безпеки;

d) забезпечити чітке регулювання та явну підтримку з боку керівництва ініціативам щодо безпеки;

e) надавати ресурси, потрібні для інформаційної безпеки;

f) затвердити призначення певних ролей і відповідальностей стосовно інформаційної безпеки в організації;

g) започаткувати плани та програми підтримки поінформованості щодо інформаційної безпеки;

h) забезпечити, щоб впровадження контролів інформаційної безпеки було скоординоване у межах організації (див. 6.1.2).

Керівництво повинно визначити потреби в рекомендаціях внутрішніх та зовнішніх фахівців з інформаційної безпеки і переглядати та координувати результати рекомендацій по всій організації.

Залежно від розміру організації, такі відповідальності може нести спеціальний керівний форум або існуючий керівний орган, наприклад, рада директорів.

Національна примітка.

Банки можуть сформувати спеціальний керівний орган з питань інформаційної безпеки з керівників, відповідальних за окремі бізнес-процеси, для розгляду та виконання відповідних рекомендацій з інформаційної безпеки. Формування такого керівного органу тільки з фахівців з питань інформаційної безпеки є недоцільним, оскільки в такому випадку питання інформаційної безпеки будуть за межами уваги керівників, відповідальних за окремі бізнес процеси, або питання інформаційної безпеки будуть вирішуватися окремо для кожного бізнес процесу, що створить додаткові умови для порушення конфіденційності та несанкціонованого доступу до інформації.

Додаткова інформація

Додаткова інформація міститься в ISO/IEC 13335-1:2004.

6.1.2 Координація інформаційної безпеки

Контроль

Діяльність щодо інформаційної безпеки повинна бути узгодженою між представниками різних підрозділів організації з відповідними ролями та посадовими обов’язками.

Національна примітка.

Банки мають створювати єдину систему інформаційної безпеки для усіх бізнес-процесів та координувати дії різних підрозділів для забезпечення виконання загальних вимог щодо інформаційної безпеки. Для усіх користувачів програмно-технічних комплексів повинні бути визначені відповідні роли, які мають бути зазначені в посадових обов’язках. Крім того, усі працівники банків повинні бути забезпечені інструкціями про порядок дій в разі випадків невідповідності/порушення інформаційної безпеки.

Настанова щодо впровадження

Зазвичай, координація інформаційної безпеки повинна стосуватися співробітництва і координації спільної діяльності менеджерів, користувачів, адміністраторів, розробників прикладних програм, аудиторів і персоналу безпеки, а також фахівців у таких галузях, як страхування, правові питання, людські ресурси, управління ІТ або ризиками.

Національна примітка.

Для координації інформаційної безпеки може бути створена окрема група з перехресними функціями з фахівців різних підрозділів.

Ця діяльність повинна:

a) забезпечити, щоб діяльність з безпеки виконувалася відповідно до політики інформаційної безпеки;

b) визначити, як обробляти невідповідності;

c) затвердити методологію та процеси інформаційної безпеки, наприклад, оцінку ризику, класифікацію інформації;

Національна примітка.

Керівництво банку має забезпечити здійснення класифікації інформації, яка обробляється в бізнес-процесах, та ознайомити усіх працівників банку з цією класифікацією інформації під власноручний підпис.

d) ідентифікувати значні зміни загроз, і також незахищеність від загроз інформації та засобів обробки інформації;

e) оцінити достатність та координувати впровадження контролів інформаційної безпеки;

f) ефективно сприяти в організації освіті, навчанню та поінформованості щодо інформаційної безпеки;

Національна примітка.

Керівництво банку повинне забезпечити навчання працівників з питань інформаційної безпеки. Рекомендується проводити ознайомлення з політикою безпеки та інструкціями з питань забезпечення інформаційної роботи під час прийняття на роботу і в подальшому періодично за необхідністю (наприклад, після перегляду політики безпеки або впровадження нових засобів захисту інформації.

g) виконувати оцінювання інформації, отриманої від моніторингу та перегляду інцидентів інформаційної безпеки, і рекомендувати необхідні дії у відповідь на ідентифіковані інциденти інформаційної безпеки.

Якщо організація не створює окрему групу з перехресними функціями, наприклад, через те, що така група не відповідає розміру організації, вищеописані дії повинні здійснюватися іншим придатним керівним органом або окремим керівником.

6.1.3 Розподіл відповідальностей за інформаційну безпеку

Контроль

Усі відповідальності за інформаційну безпеку треба чітко визначити.

Настанова щодо впровадження

Розподіл відповідальностей за інформаційну безпеку повинен виконуватися відповідно до політики інформаційної безпеки (див. розділ 4). Відповідальність за захист окремих активів та за виконання певних процедур безпеки повинна бути чітко ідентифікована. Така відповідальність повинна доповнюватися, за необхідності, більш докладною настановою щодо окремих місць розміщення та засобів обробки інформації. Повинні бути чітко визначені локальні відповідальності щодо захисту активів та виконання певних процедур безпеки, таких як планування безперервності бізнесу.

Особи з визначеними відповідальностями щодо безпеки можуть делегувати задачі безпеки іншим. Незважаючи на це, вони залишаються відповідальними і повинні визначити, чи всі делеговані задачі виконуються правильно.

Повинні бути чітко встановлені сфери відповідальності окремих осіб; зокрема, повинно мати місце наведене нижче:

a) повинні бути ідентифіковані та чітко визначені активи та процедури безпеки, пов'язані з кожною окремою системою;

b) повинна бути призначена особа, відповідальна за кожний актив чи процедуру безпеки і ці відповідальності повинні бути докладно задокументовані (див. також 7.1.2);

c) повинні бути чітко визначені й задокументовані рівні авторизації.

Національна примітка.

Рівні авторизації для доступу до інформаційних активів можуть бути, наприклад, „тільки читати", „читати і записувати", „тільки записувати" тощо.

Додаткова інформація

У багатьох організаціях керівник з інформаційної безпеки призначається повністю відповідальним за розвиток і впровадження безпеки та за підтримку ідентифікації контролів.

Проте, відповідальність за добір ресурсів та впровадження контролів часто залишається за окремими менеджерами. Звичайною практикою є призначення для кожного активу власника, який внаслідок цього стає відповідальним за щоденний захист активу.

6.1.4 Процес авторизації використання засобів оброблення інформації

Контроль

Процес управління авторизацією використання нових засобів оброблення інформації треба визначити та впровадити.

Настанова щодо впровадження

Для процесу авторизації повинні бути розглянуті наведені нижче настанови:

a) нові засоби повинні мати належну авторизацію служби управління користувачами, яка авторизує їх цілі та використання. Авторизацію треба також отримати від керівника, відповідального за підтримку інфраструктури безпеки локальної інформаційної системи для гарантії того, що виконані всі суттєві політики безпеки та вимоги;

b) там, де це необхідно, повинні бути перевірені апаратні засоби та програмне забезпечення, щоб гарантувати їх сумісність з іншими компонентами системи;

c) використання персональних чи приватних засобів обробки інформації, наприклад, портативних, домашніх або кишенькових пристроїв, для обробки бізнес-інформації може спричинити нові вразливості, тому повинні бути ідентифіковані й запроваджені необхідні контролі.

Національна примітка.

Банки мають приділяти особливу увагу питанням інформаційної безпеки при використанні новітніх інформаційних технологій віддаленого доступу до банківської інформації, наприклад, ресурси мережі Інтернет, бездротовий зв'язок тощо).

6.1.5 Угоди щодо конфіденційності

Контроль

Вимоги щодо конфіденційності або угоди щодо нерозголошення, які відображують потреби організації у захисті інформації, повинні бути ідентифіковані та підлягають регулярному перегляду.

Настанова щодо впровадження

Угоди щодо конфіденційності або нерозголошення повинні ураховувати вимоги захисту конфіденційної інформації з використанням існуючих правових норм. Для ідентифікації вимог до угод щодо конфіденційності або нерозголошення треба розглянути наведені нижче елементи:

a) визначення інформації, яка повинна бути захищена (наприклад, конфіденційна інформація);

Національна примітка.

Банки мають чітко визначити перелік відомостей з грифом «банківська таємниця» та інформації з іншими грифами конфіденційності в разі необхідності (наприклад, комерційна таємниця, персональні дані клієнтів тощо).

b) очікувана тривалість угоди, охоплюючи випадки, коли конфіденційність повинна підтримуватися необмежено;

c) необхідні дії після припинення угоди;

d) відповідальності та дії сторін, що підписали угоду, для запобігання неавторизованому розголошенню інформації (типу „необхідно знати”);

e) право власності на інформацію, секрети виробництва та інтелектуальна власність і як вони співвідносяться з захистом конфіденційної інформації;

f) дозволене використання конфіденційної інформації і права сторони, яка підписала угоду, користуватися інформацією;

g) право аудиту і моніторингу діяльності, пов’язаної з конфіденційною інформацією;

h) процес сповіщення та звітування щодо неавторизованого розголошення або порушень конфіденційної інформації;

i) терміни повернення або руйнування інформації у разі припинення угоди; та

j) очікувані дії, яких треба вжити у разі порушення угоди.

Виходячи з вимог безпеки організації, може виникнути необхідність включати в угоду щодо конфіденційності або нерозголошення також інші елементи.

Угоди щодо конфіденційності та нерозголошення повинні відповідати усім існуючим законам та нормам для юрисдикції, де вони використовуються, (див. також 15.1.1).

Вимоги до угод щодо конфіденційності та нерозголошення повинні переглядатись періодично, і у випадках змін, які впливають на ці вимоги.

Додаткова інформація

Угоди щодо конфіденційності та нерозголошення захищають інформацію організації та інформують сторони, які підписали угоди, про їх відповідальність

щодо захисту, використання та розголошення інформації лише у відповідальний та авторизований спосіб.

В організації може виникнути необхідність використовувати різні форми угод щодо конфіденційності та нерозголошення за різних обставин.

6.1.6 Контакти з повноважними органами

Контроль

Повинні підтримуватись належні контакти з відповідними повноважними органами.

Настанова щодо впровадження

В організації повинні бути наявні процедури, які визначають, коли і з якими повноважними органами (наприклад, органами забезпечення правопорядку, пожежної охорони, наглядовими органами) треба контактувати і як своєчасно звітувати про ідентифіковані інциденти інформаційної безпеки, якщо очікується, що цим можуть бути порушені закони.

Національна примітка.

Банки мають сповіщати Національний банк України про ідентифіковані інциденти інформаційної безпеки, які трапляються в платіжних системах з метою нормативного визначення додаткових вимог для запобіганню створення умов виникнення інцидентів інформаційної безпеки в подальшому.

Організації, на яку здійснений напад з Інтернету, можуть знадобитись зовнішні треті сторони (наприклад, Інтернет-провайдер або оператор телекомунікацій) для виконання дій проти джерела нападу.

Національна примітка.

Банки мають сповіщати правоохоронні органи України про ідентифіковані спроби шахрайств з електронними платіжними документами, які призвели до фінансових втрат.

Додаткова інформація

Підтримування таких контактів може бути вимогою щодо підтримки управління інцидентом інформаційної безпеки (Розділ 13.2) або безперервності бізнесу та процесу планування дій в надзвичайних ситуаціях (Розділ 14). Контакти з регулятивними органами також є корисними для передбачення та підготовки до наступних змін до законів та нормативів, яких повинна дотримуватися організація. Контакти з іншими повноважними органами стосуються підприємств комунального обслуговування, аварійних ситуацій, а також здоров’я та безпеки, наприклад, відділів пожежної охорони (у зв’язку з безперервністю бізнесу), операторів телекомунікацій (у зв’язку з маршрутизацією та доступністю ліній), постачальників води (у зв’язку з охолоджувальними засобами обслуговування обладнання).

6.1.7 Контакти з групами фахівців з певної проблематики

Контроль

Повинні підтримуватись належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об’єднаннями.

Настанова щодо впровадження

Членство у групах фахівців з певної проблематики або форумах повинно розглядатись як засіб для:

a) вдосконалення знань щодо найкращих практик та поінформованості щодо суттєвої та найсучаснішої інформації з безпеки;

b) забезпечення того, що розуміння інформаційної безпеки є сучасним та повним;

c) отримання ранніх попереджень із застереженнями, повідомленнями про небезпеку, та кодів оперативного виправлення (patches), які стосуються атак і вразливостей;

d) одержання доступу до рекомендацій фахівців з інформаційної безпеки;

e) спільного користування та обміну інформацією щодо нових технологій, продуктів, загроз або вразливостей;

Національна примітка.

Керівництво банків має забезпечити участь фахівців з інформаційної безпеки в відповідних конференціях, семінарах тощо для підвищення рівня їх кваліфікації та знайомства з тенденціями розвитку інформаційних технологій і захисту інформації.

f) забезпечення можливість обговорення під час роботи з інцидентами інформаційної безпеки (див. також 13.2.1).

Додаткова інформація

Для вдосконалення співпраці та координації у питаннях безпеки можуть укладатися угоди щодо спільного використання інформації. Такі угоди повинні ідентифікувати вимоги щодо захисту чутливої інформації.

6.1.8 Незалежний перегляд інформаційної безпеки

Контроль

Підхід організації до управління інформаційною безпекою та її впровадження (тобто, цілі контролів, контролі, політики, процеси та процедури інформаційної безпеки) підлягають незалежному перегляду в заплановані терміни або за виникнення значних змін у впровадженій безпеці.

Настанова щодо впровадження

Незалежний перегляд повинен ініціюватися керівництвом. Такий незалежний перегляд необхідний для забезпечення подальшої придатності, адекватності та ефективності підходу організації до управління інформаційною безпекою. Перегляд повинен охоплювати оцінку можливостей вдосконалення та необхідності змін у підході до безпеки, охоплюючи політику та цілі контролів.

Такий перегляд повинен виконуватися особами, незалежними від переглядуваної області, наприклад, внутрішнім аудитором, незалежним керівництвом або організацією третьої сторони, яка спеціалізується на таких переглядах. Особи, які здійснюють такий перегляд, повинні мати відповідні навички та досвід.

Результати незалежного перегляду повинні реєструватися та звітуватися керівництву, яке ініціювало перегляд. Ці записи повинні зберігатися та

підтримуватися.

Якщо незалежний перегляд виявив, що підхід організації та впровадження управління інформаційною безпекою є неадекватним або невідповідним напряму інформаційної безпеки, встановленому в документі щодо політики інформаційної безпеки (див. 5.1.1), керівництво повинне розглянути коригувальні заходи.

Додаткова інформація

Область, яка підлягає регулярному перегляду керівництвом (див. 15.2.1), може також бути переглянута незалежно. Методи перегляду можуть охоплювати опитування керівництва, перевірку записів або перегляд документів політики безпеки. ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing може також надати корисні настанови щодо проведення незалежного перегляду, охоплюючи розроблення та впровадження програми перегляду. Підрозділ 15.3 визначає суттєві контролі незалежного перегляду функціонуючих інформаційних систем і використання механізмів системного аудиту.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ.

ISO 19011:2002, Рекомендації з аудиту систем управління якістю та/або довкіллям

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.

Безпека інформації і засобів оброблення інформації, які належать організації, не повинна знижуватись через введення в експлуатацію продуктів або послуг зовнішньої сторони.

Будь-який доступ до засобів оброблення інформації організації, а також оброблення та передавання інформації зовнішнім сторонам повинні бути контрольованими.

Якщо є бізнес-потреба в роботі з зовнішніми сторонами, яка може вимагати доступу до інформації або засобів оброблення інформації організації, або в отриманні від зовнішньої сторони чи наданні їй продукту та послуги, повинна виконуватись оцінка ризику для визначення вимог контролю та наслідків щодо безпеки. Контролі повинні бути погоджені та визначені в угоді з зовнішньою стороною.

6.2.1 Ідентифікація ризиків, пов'язаних з зовнішніми сторонами

Контроль

Ризики для інформації організації та її засобів оброблення інформації бізнес-процесів, до яких залучені зовнішні сторони, повинні бути ідентифіковані і належні контролі повинні бути впроваджені до надання доступу.

Настанова щодо впровадження

Там, де необхідно дозволити зовнішній стороні доступ до засобів оброблення інформації або інформації організації, повинна виконуватися оцінка ризику (див. також розділ 4) для ідентифікації будь-яких вимог до певних контролів. Ідентифікація ризиків, які стосуються доступу зовнішніх сторін, повинна брати до уваги нижченаведені питання:

a) засоби оброблення інформації, доступу до яких потребує зовнішня сторона;

b) вид доступу, який зовнішня сторона буде мати до інформації та засобів оброблення інформації, наприклад:

1) фізичний доступ, наприклад, до офісів, комп'ютерних кімнат, картотек;
2) логічний доступ, наприклад, до баз даних, інформаційних систем організації;
3) наявність зв'язку між мережею організації та мережею(ами) зовнішньої сторони, наприклад, постійний зв'язок, віддалений доступ;
4) чи здійснюється доступ в організації чи поза її межами;

c) цінність та чутливість залученої інформації та її критичність для функціонування бізнесу;

d) контролі, необхідні для захисту інформації, яку не призначено для доступу зовнішніх сторін;

e) персонал зовнішньої сторони, залучений до оброблення інформації організації;

f) як організація чи персонал, які авторизовані на доступ, можуть бути ідентифіковані, авторизація верифікована, і як часто це потребує повторного підтвердження;

g) різні засоби та контролі, які використовуються зовнішньою стороною під час зберігання, оброблення, доведення до відома, спільного використання та обміну інформації;

h) вплив відсутності доступу за потребою зовнішньої сторони, і введення чи одержання зовнішньою стороною неточної або недостовірної інформації;

i) практика і процедури поводження з інцидентами інформаційної безпеки та потенційними ушкодженнями, а також терміни та умови відновлення доступу зовнішньої сторони у випадку інциденту інформаційної безпеки;

j) правові та нормативні вимоги, інші контрактні зобов'язання суттєві для зовнішньої сторони, які треба взяти до уваги;

k) як можуть вплинути відповідні заходи на інтереси будь-яких інших зацікавлених сторін.

Доступ зовнішніх сторін до інформації організації не повинен надаватися доки не впроваджено відповідні контролі та, де це можливо, не підписано контракт, який визначає терміни та умови підключення або доступу та робочі

заходи. Як правило, всі вимоги безпеки, які є наслідком роботи з зовнішніми сторонами або внутрішніми контролями, повинні бути відображені в угоді з зовнішньою стороною (див. також 6.2.2 та 6.2.3).

Повинно бути гарантовано, що зовнішня сторона поінформована щодо своїх зобов'язань і приймає обов'язки та відповідальність, пов'язані з доступом, обробленням, доведенням до відома або управлінням інформацією організації та засобами оброблення інформації.

Національна примітка.

Під час виконання робіт з зовнішніми сторонами банки повинні впевнитися, що працівники зовнішньої сторони, які безпосередньо виконують дії за визначеною угодою, обізнані в питаннях безпеки поводження з інформацією банку, до якої вони можуть мати доступ.

Додаткова інформація

Інформація може бути піддана ризику зовнішніми сторонами з невідповідним управлінням безпекою. Для адміністрування доступу зовнішньої сторони до засобів оброблення інформації контролі повинні бути ідентифіковані та застосовані. Наприклад, якщо є певна потреба конфіденційності інформації, можуть бути використані угоди щодо нерозголошення.

Організації можуть наражатися на ризики, пов'язані з міжорганізаційні процесами, управлінням та зв'язками, якщо має місце високий ступінь аутсорсингу або якщо залучено декілька зовнішніх сторін.

Контролі 6.2.2 та 6.2.3 стосуються різних угод із зовнішніми сторонами, наприклад, включаючи:

a) постачальників послуг, таких як Інтернет-провайдери, постачальники мережевих послуг, телефонні послуги, послуги обслуговування та підтримки;

b) послуги безпеки, якими управляють;

c) клієнтів;

d) аутсорсинг засобів і/або функцій, наприклад, ІТ систем, послуг збору даних, функцій центру телефонного обслуговування;

e) консультантів з управління та бізнесу, аудиторів;

f) розробників та постачальників, наприклад, програмного забезпечення та ІТ систем;

g) послуги з прибирання, харчування та інші аутсорсингові послуги підтримки;

h) тимчасовий персонал, працюючих студентів та інших тимчасових короткострокових працівників.

Такі угоди можуть допомогти знизити ризики, пов'язані з зовнішніми сторонами.

6.2.2 Врахування безпеки під час роботи з клієнтами

Контроль

Перш ніж надавати клієнтам доступ до інформації або активів організації, повинні бути враховані всі ідентифіковані вимоги безпеки.

Настанова щодо впровадження

Повинні бути розглянуті наведені нижче умови для врахування безпеки до надання клієнтам доступу до будь-яких активів організації (залежно від типу та ступеня наданого доступу можуть застосовуватися не всі з них):

a) захист активу, включаючи:
   1) процедури захисту активів організації, охоплюючи інформацію та програмне забезпечення, та управління відомими вразливими;
   2) процедури, які визначають, чи мала місце будь-яка компрометація активів, наприклад, втрата або модифікація даних;
   3) цілісність;
   4) обмеження щодо копіювання та розголошення інформації;
b) опис продукції або послуги, які повинні надаватися;
c) різні причини, вимоги та переваги щодо доступу клієнта;
d) політика контролю доступу, яка охоплює:
   1) дозволені методи доступу, а також контроль та використання унікальних ідентифікаторів, таких як ID (ідентифікатор) користувача та паролі;

Національна примітка.

Банки мають чітко визначити дозволені методи доступу клієнтів для їх віддаленого обслуговування. Рекомендується використовувати процедуру взаємної суворої автентифікації клієнтів з використанням криптографічних ключів. В разі використання для доступу ідентифікатора та паролю повинні бути передбачені контролі складності паролів, довжина паролів повинна бути не менше 6 символів, повинна бути передбачена необхідність заміни паролю, який наданий адміністратором системи, при першому вході клієнта до системи на власний пароль, який не буде відомим адміністратору системи.

   2) процес авторизації доступу та повноважень користувача;
   3) положення про те, що всякий нечітко авторизований доступ - заборонено;
   4) процедуру відкликання прав доступу або переривання зв'язку між системами;
e) заходи щодо звітування, сповіщення та розслідування інформаційних неточностей (наприклад, в персональній додатковій інформації), інцидентів інформаційної безпеки та порушень безпеки;
f) опис кожної послуги, яка повинна бути зроблена доступною;
g) заданий рівень послуг і неприйнятні рівні послуг;
h) право здійснювати моніторинг та відміняти будь-яку діяльність пов'язану з активами організації;
i) відповідні зобов'язання організації та клієнта;
j) відповідальності стосовно правових питань і як забезпечується задоволення правових вимог, наприклад, законодавства щодо захисту даних, особливо беручи до уваги різні національні правові системи, якщо угода охоплює співпрацю з клієнтами в інших країнах (див. також 15.1);
k) права інтелектуальної власності (IPR) та призначення авторського права (див. 15.1.2) і захист будь-якої спільної роботи (див. також 6.1.5).

Додаткова інформація

Вимоги безпеки пов’язані з доступом клієнтів до активів організації, можуть значно відрізнятися залежно від засобів оброблення інформації та інформації, до яких здійснюватиметься доступ. Ці вимоги безпеки можуть бути враховані з угодах з клієнтом, які містять усі ідентифіковані ризики та вимоги безпеки (див. 6.2.1).

Угоди з зовнішніми сторонами можуть також включати інші сторони. Угоди, які надають доступ зовнішній стороні, повинні містити дозвіл на призначення інших прийнятних сторін і умови їх доступу та залучення.

6.2.3 Врахування безпеки в угодах з третьою стороною

Контроль

Угоди з третіми сторонами щодо доступу, оброблення, передавання або управління інформацією організації або засобами оброблення інформації, або щодо до додавання продуктів чи послуг до засобів оброблення інформації повинні охоплювати усі відповідні вимоги безпеки.

Настанова щодо впровадження

Угода повинна забезпечувати відсутність непорозумінь між організацією та третьою стороною. Організації повинні задовольнити свої інтереси щодо відшкодування збитків третьою стороною.

Щоб задовольнити визначені вимоги безпеки, треба розглянути внесення до угод наведених нижче умов (див. 6.2.1):

a) політики інформаційної безпеки;

b) контролів для забезпечення захисту активів, включаючи:

1) процедури захисту активів організації, включаючи інформацію, програмне забезпечення та апаратні засоби;
2) будь-які необхідні контролі та механізми фізичного захисту;
3) контролі для забезпечення захисту від зловмисного програмного забезпечення (див. 10.4.1);
4) процедури для визначення, чи мала місце якась компрометація активів, наприклад, втрата або модифікація інформації, програмного забезпечення та апаратних засобів;
5) контролі для забезпечення повернення чи знищення інформації та активів по закінченні або в погоджений момент часу протягом дії угоди;
6) конфіденційність, цілісність, доступність та будь-які інші відповідні властивості (див. 2.1.5) активів;
7) обмеження щодо копіювання та розголошення інформації та використання угод щодо конфіденційності (див. 6.1.5);

c) навчання користувача та адміністратора щодо методів, процедур та безпеки;

d) забезпечення поінформованості користувача щодо проблем та відповідальностей з інформаційної безпеки;

e) умов щодо переміщення персоналу, за необхідності;

f) відповідальності стосовно інсталяції та підтримки апаратних засобів та

програмного забезпечення;

g) чіткої структури звітування та погоджених форматів звітування;

h) чіткого та визначеного процесу управління змінами;

i) політики контролю доступу, яка охоплює:

1) різні причини, вимоги та переваги, які роблять доступ третіх осіб необхідним;
2) дозволені методи доступу, контроль та використання унікальних ідентифікаторів, таких як ID користувача та паролі;
3) процес авторизації доступу користувача та повноважень;
4) вимогу щодо підтримки переліку осіб, яким надано право використання доступних послуг, і які права та повноваження цих осіб стосовно такого використання;
5) положення про те, що всякий нечітко авторизований доступ є забороненим;
6) процес відкликання прав доступу або переривання зв'язку між системами;

j)заходів щодо звітування, сповіщення та розслідування інцидентів інформаційної безпеки та порушень безпеки, а також порушень вимог, встановлених в угоді;

k) опису продукту або послуги, які повинні надаватися, та опис інформації, яка повинна бути доступною, разом з її класифікацією щодо безпеки (див. 7.2.1);

l) заданого рівня послуги і неприйнятні рівні послуги;

m) визначення критеріїв продуктивності, які можуть бути верифіковані, їх моніторинг та звітування;

n) права здійснювати моніторинг та відміняти будь-яку діяльність, яка стосується активів організації;

o) права здійснювати аудит відповідальностей, визначених в угоді, мати такі аудити, які виконуються третьою стороною, та перелічувати права аудиторів, що відповідають законодавству;

p) встановлення процесу ескалації для розв'язання проблеми;

q) вимоги безперервності послуги, в тому числі заходи щодо доступності та надійності відповідно до бізнес-пріоритетів організації;

r) відповідних зобов'язань сторін угоди;

s) відповідальностей стосовно правових питань і способу забезпечення виконання правових вимог, наприклад, законодавства щодо захисту даних, особливо беручи до уваги різні національні правові системи, якщо угода охоплює співпрацю з клієнтами в інших країнах (див. також 15.1));

t) права інтелектуальної власності (IPR), визнання авторського права (див. 15.1.2) і захисту будь-якої спільної роботи (див. також 6.1.5);

u) залучення третьої сторони як субконтрактора і контролі безпеки, які ці субконтрактори повинні запровадити;

v) умов перегляду/припинення угод:

1) наявність на місці плану дій в надзвичайних ситуаціях, якщо якась із сторін бажає припинити відносини до закінчення угоди;

2) перегляд угод за умови зміни вимог безпеки організації;
3) поточне документування переліків активів, ліцензій, угод або прав, які їх стосуються.

Додаткова інформація

Для різних організацій та різних типів третіх сторін угоди можуть значно відрізнятися. Тому треба звернути увагу на охоплення угодою всіх ідентифікованих ризиків і вимог безпеки (див. також 6.2.1). Якщо необхідно, у плані управління безпекою можуть бути розширені необхідні контролі та процедури.

Якщо управління безпекою здійснюється на умовах аутсорсингу, угода повинна враховувати, яким чином третя сторона гарантуватиме, що відповідна безпека, визначена оцінкою ризику, буде підтримуватися, і яким чином буде пристосовуватися безпека, щоб ідентифікувати та розглядати зміни ризиків.

Різниця між аутсорсингом та іншими формами постачання послуг третьою стороною включає питання відповідальності, планування перехідного періоду і потенційного порушення функціонування протягом цього періоду, заходи з планування дій в аварійних ситуаціях і належні перегляди, збирання та управління інформацією щодо інцидентів безпеки. Тому важливо, щоб організація планувала та управляла переходом до аутсорсингових заходів і мала на місцях відповідні процеси для управління змінами та переукладанням/припиненням угод.

Щоб уникнути будь-якої затримки у розміщенні замінюваних послуг, в угоді повинні бути розглянуті процедури для продовження обробки у випадку, коли третя сторона стає нездатною постачати свої послуги.

Угоди з зовнішніми сторонами можуть також залучати інші сторони. Угоди, які надають доступ зовнішній стороні, повинні містити дозвіл на призначення інших припустимих сторін і умови їх доступу та залучення.

Взагалі, угоди спочатку розробляються організацією. За деяких обставин можуть бути випадки, коли угода може розроблятися і примусово надаватися організації третьою стороною. Організація повинна забезпечити, щоб вимоги третьої сторони, передбачені в примусово наданих угодах, надмірно не впливали на її власну безпеку.

7 Управління активами

7.1 Відповідальність за активи

Ціль: Досягти та підтримувати належний захист активів організації.

Усі активи повинні бути враховані та мати призначеного власника.

Для всіх активів повинні бути ідентифіковані їх власники і повинна бути встановлена відповідальність за підтримування належних контролів. Впровадження певних контролів може делегуватися власником, якщо це прийнятно, проте відповідальним за належний захист активів залишається власник.

7.1.1 Інвентаризація активів

Контроль

Усі активи необхідно чітко ідентифікувати та скласти і підтримувати інвентарний опис усіх важливих активів.

Настанова щодо впровадження

Організація повинна ідентифікувати всі активи і задокументувати важливість цих активів. Інвентарний опис активів повинен містити всю інформацію, необхідну для відновлення після лиха, в тому числі, тип активу, формат, розташування, резервну та ліцензійну інформацію та бізнес-цінність. Інвентарний опис не повинен зайве дублювати інші описи, проте треба гарантувати узгодженість їх змісту.

Крім того, для кожного з активів повинні бути погоджені та задокументовані власник активу (див. 7.1.2) та класифікація інформації (див. 7.2). Базуючись на важливості активу, його бізнес-цінності та класифікації стосовно безпеки, повинні бути ідентифіковані рівні захисту пропорційні цінності активу (більше інформації щодо того, як оцінювати активи, щоб відобразити їх важливість, можна знайти в ISO/IEC TR 13335-3).

Додаткова інформація

Існує багато типів активів, у тому числі:

a) інформація: бази даних та файли даних, контракти та угоди, системна документація, дослідницька інформація, настанови для користувачів, навчальний матеріал, процедури функціонування або підтримки, плани безперервності бізнесу, заходи щодо його відновлення, журнали аудиту та архівна інформація;

b) програмні активи: прикладне програмне забезпечення, системне програмне забезпечення, засоби розробки та утиліти;

c) фізичні активи: комп'ютерне обладнання, телекомунікаційне обладнання, замінювані носії та інше обладнання;

d) послуги: обчислювальні та телекомунікаційні послуги, комунальні послуги, наприклад, опалення, освітлення, енергопостачання та кондиціювання повітря;

e) люди та їх кваліфікація, навички та досвід;

f) нематеріальні активи, такі як репутація та імідж організації.

Інвентарні описи активів допомагають забезпечити наявність ефективного захисту активів і також можуть бути потрібними для інших бізнес-цілей, таких як здоров'я та безпека, страхові або фінансові (управління активами) причини. Процес складання інвентарного опису активів є важливою передумовою управління ризиком (див. також розділ 4).

7.1.2 Володіння активами

Контроль

Уся інформація і активи, пов'язані із засобами оброблення інформації, повинні «бути у власності»[2] призначеного підрозділу організації.

Настанова щодо впровадження

Власник активів повинен бути відповідальний за:

a) забезпечення того, що інформація та активи, пов'язані з засобами оброблення інформації, відповідним чином класифіковані;

b) визначення та періодичний перегляд обмежень та класифікації доступу, беручи до уваги застосовну політику контролю доступу.

Володіння може бути призначено щодо:

c) бізнес процесу;
d) визначеного кола діяльності;
e) прикладної програми; або
f) визначеного набору даних.

Додаткова інформація

Повсякденні задачі можуть бути делеговані, наприклад, куратору, який щоденно наглядає за активом, проте відповідальність залишається за власником.

У разі складних інформаційних систем може бути корисним призначити групи активів, які діють разом для надання окремої функції як „послуги". У цьому випадку власник послуги є відповідальним за постачання послуги, в тому числі за функціонування активів, які її надають.

7.1.3 Припустиме використання активів

Контроль

Правила щодо припустимого використання інформації та активів, пов'язаних з засобами оброблення інформації, повинні бути ідентифіковані, задокументовані та впроваджені.

---

[2] Термін «власник» ідентифікує особу або організацію, для якої встановлено затверджену керівництвом відповідальність щодо контролювання виробництва, розвитку, підтримування, використання та безпеки активів. Термін «власник» не означає, що особа дійсно має права власності на актив.

Настанова щодо впровадження

Весь найманий персонал, контрактори та користувачі третьої сторони повинні виконувати правила щодо припустимого використання інформації та активів, пов'язаних з засобами оброблення інформації, в тому числі:

a) правила користування електронною поштою та Інтернетом (див. 10.8);

b) настанови щодо користування мобільними пристроями, особливо при користуванні поза межами службових приміщень організації (див. 11.7.1);

Національна примітка.

Банки повинні розробити та затвердити загальні правила користування службовими персональними комп'ютерами, ноутбуками та іншими засобами комп'ютерної техніки, правіла роботи в мережі банку, правила надання доступу до інформації і програмно-технічних комплексів автоматизації банківської діяльності.

Спеціальні правила або настанови повинні надаватися відповідним керівництвом. Службовці, контрактори та користувачі третьої сторони, які користуються активами організації або мають до них доступ, повинні бути поінформовані щодо існуючих обмежень стосовно їх користування інформацією, активами організації, пов'язаними із засобами оброблення інформації, та її ресурсами. Вони повинні бути відповідальними за використання ними будь-якими ресурсами оброблення інформації та будь-яке таке використання здійснюється під їх відповідальністю.

7.2 Класифікація інформації

Ціль*:* Забезпечити, що інформація має належний рівень захисту.

Інформація повинна бути класифікована для ідентифікації потреби, пріоритетності та очікуваного ступеня захисту під час її оброблення.

Інформація має різні ступені чутливості та критичності. Деякі елементи можуть потребувати додаткового рівня захисту або певного оброблення. Схема класифікації інформації повинна використовуватися для визначення відповідного набору рівнів захисту і зв'язку з потребою в спеціальних заходах поводження з інформацією.

7.2.1 Настанови щодо класифікації

Контроль

Інформація повинна бути класифікована в термінах її цінності, правових вимог, чутливості та критичності для організації.

Національна примітка.

Банки повинні чітко визначити повний перелік інформації, яка відноситься до «банківської таємниці» відповідно до Закону України «Про банки і банківську діяльність».

Настанова щодо впровадження

Класифікація та пов'язані з нею контролі захисту інформації повинні брати до уваги бізнес-потреби для спільного використання або обмеження інформації та бізнес-впливи, пов'язані з такими потребами.

Настанови щодо класифікації повинні містити домовленості щодо первинної класифікації та повторної класифікації через певний час; відповідно до заздалегідь визначеній політиці контролю доступу (див. 11.1.1).

Повинна бути встановлена відповідальність власника активу (див. 7.1.2) за визначення класифікації активу, періодичний її перегляд, забезпечення підтримки її в актуальному стані і на відповідному рівні. Класифікація повинна брати до уваги ефект об'єднання, наведений у 10.7.2.

Треба розглянути кількість класифікаційних категорій і переваг, які будуть отримані від їх використання. Надмірно складні схеми можуть стати громіздкими й неекономічними для використання або виявитися непрактичними. Треба потурбуватися щодо інтерпретації класифікаційних позначок на документах з інших організацій, які можуть мати інші визначення для тих самих або аналогічно названих позначок.

Національна примітка.

Рекомендується використовувати загально визнані категорії та позначки інформації, наприклад, «банківська таємниця» (БТ), «комерційна таємниця» (КТ) тощо.

Додаткова інформація

Рівень захисту може бути оцінений шляхом аналізу конфіденційності, цілісності та доступності та будь-яких інших вимог до розглядуваної інформації.

Інформація часто перестає бути чутливою або критичною після певного періоду часу, наприклад, після того, як інформація стає загальнодоступною. Ці аспекти треба взяти до уваги, оскільки надмірна класифікація може призвести до впровадження непотрібних контролів, наслідком яких будуть додаткові витрати.

Розгляд документів зі схожими вимогами безпеки під час призначення класифікаційних рівнів може допомогти у спрощенні задачі класифікації.

Взагалі, класифікація, яка надана інформації, є коротким шляхом визначення того, як ця інформація повинна оброблятися та захищатися.

7.2.2 Маркування та оброблення інформації

Контроль

Належна множина процедур для маркування та оброблення інформації повинна бути розроблена та впроваджена згідно зі схемою класифікації, прийнятою організацією.

Настанова щодо впровадження

Необхідно, щоб процедури маркування інформації поширювалися на інформаційні активи в матеріальному та електронному вигляді.

Вихідні дані систем, які містять інформацію, класифіковану як чутлива або критична, повинні містити відповідну класифікаційну позначку (на виході). Маркування повинне відображати класифікацію відповідно до правил, встановлених у 7.2.1. Розглядуваними елементами є надруковані звіти, екрани дисплеїв, носії записів (наприклад, стрічки, диски, CD), електронні повідомлення

та обмін файлами.

Для кожного класифікаційного рівня повинні бути визначені процедури поводження з інформацією, охоплюючи безпечну обробку, зберігання, передавання, розкласифікацію (виведення з класифікації) та знищення. Вони повинні містити також процедури для ланцюга охорони та реєстрації будь-якої події, суттєвої для безпеки.

Угоди з іншими організаціями, які охоплюють спільне використання інформації, повинні містити процедури ідентифікації класифікації такої інформації та інтерпретації класифікаційних позначок інших організацій.

Додаткова інформація

Маркування та безпечне оброблення класифікованої інформації є ключовою вимогою угод щодо спільного використання інформації. Фізичні позначки є загальноприйнятою формою маркування. Проте, деякі інформаційні активи, такі як документи в електронному вигляді, не можуть бути фізично позначені і потребують використання електронних засобів маркування. Наприклад, позначка сповіщення може з’являтися на екрані або дисплеї. Там, де позначки зробити неможливо, можуть бути застосовані інші засоби позначення класифікації інформації, наприклад, через процедури або метадані.

8 Безпека людських ресурсів

8.1 Перед наймом[3]

Ціль: Гарантувати, що найманий персонал, контрактори та користувачі третьої сторони розуміють свої відповідальності, придатні до ролей, на які претендують, і зменшити ризик розкрадання, шахрайства чи зловживання обладнанням.

Відповідальності з безпеки повинні бути визначені перед наймом у відповідних посадових інструкціях і в термінах та умовах найму.

Усі кандидати на найм, контрактори та користувачі третьої сторони повинні бути відповідним чином ретельно перевірені, особливо на роботи, пов'язані з чутливою інформацією.

Найманий персонал, контрактори та користувачі третьої сторони, які користуються засобами оброблення інформації, повинні підписати угоду стосовно їх ролей щодо безпеки та відповідальностей.

Національна примітка.

Усі кандидати на найм, контрактори та користувачі третьої сторони, які будуть працювати з конфіденційною інформацією, повинні власноруч підписати зобов'язання про нерозголошення конфіденційної інформації, яка стане ним відома під час виконання службових обов'язків.

8.1.1 Ролі та відповідальності

Контроль

Ролі щодо безпеки та відповідальності найманого персоналу, контракторів та користувачів третьої сторони повинні бути визначені та задокументовані відповідно до політики інформаційної безпеки організації.

Настанова щодо впровадження

Ролі щодо безпеки та відповідальності повинні містити вимоги щодо:

a) впровадження та діяльності згідно з політикою інформаційної безпеки організації (див. 5.1);

b) захисту активів від неавторизованого доступу, розголошення, модифікації, руйнування або втручання;

c) виконання особливих процедур або дій щодо безпеки;

d) гарантування встановленої для особи відповідальності за здійснювані дії;

e) звітування про події безпеки, або можливі події, або інші ризики безпеки для організації.

[3] Пояснення: Слово „найм" означає тут охоплення всіх перелічених нижче різних ситуацій: найм людей (тимчасовий або довготривалий), призначення функціональних ролей, зміну функціональних ролей, укладання контрактів та припинення будь-якої з цих угод.

Ролі щодо безпеки та відповідальності повинні бути встановлені та чітко доведені до відома претендентів на роботу в процесі, що передує найму.

Додаткова інформація

Для документування ролей щодо безпеки та відповідальностей можуть бути використані посадові інструкції. Повинні також бути чітко визначені та доведені до відома ролі щодо безпеки та відповідальності осіб, залучених не через процедуру найму організації, наприклад, найнятих через організацію третьої сторони.

8.1.2 Ретельна перевірка

Контроль

Верифікаційні перевірки біографічних даних щодо всіх кандидатів на найм, контракторів 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 усвідомлюваними ризиками.

Настанова щодо впровадження

Верифікаційні перевірки повинні враховувати все відповідне законодавство щодо приватності, захисту персональних даних та/або найму і повинні там, де це дозволено, містити таке:

a) наявність задовільних характеристик, наприклад, одної бізнесової і одної особової;

b) перевірку (на повноту та точність) резюме претендентів;

c) підтвердження заявленої академічної та професійної кваліфікації;

d) незалежну ідентифікаційну перевірку особи (паспорт або аналогічний документ);

e) більш детальні перевірки, такі як кредитні перевірки або перевірки за кримінальним обліком.

Там, де на посаду чи при початковому призначенні, чи при підвищенні по службі залучають осіб, які матимуть доступ до засобів оброблення інформації, і особливо, якщо вони оброблятимуть чутливу інформацію, наприклад, фінансову або конфіденційну інформацію, організація повинна передбачити також і подальші більш детальні перевірки.

Процедури повинні визначати критерії та обмеження для верифікаційних перевірок, наприклад, хто має право ретельно перевіряти людей і як, коли й чому верифікаційні перевірки проводяться.

Процес ретельної перевірки повинен також проводитися для контракторів і користувачів третьої сторони. Якщо контрактори надаються через агенцію, угода з цією агенцією повинна чітко визначати відповідальність агенції за ретельну перевірку та процедури сповіщення, яких вона повинна дотримуватися, якщо ретельну перевірку не було завершено або якщо результати викликають сумнів або занепокоєння. Аналогічно угода з третьою стороною (див також 6.2.3)

повинна чітко визначати всі відповідальності та процедури сповіщення щодо ретельної перевірки.

Інформація щодо всіх кандидатів, які розглядаються на посади в організації, повинна збиратися та оброблятися згідно з відповідним законодавством, існуючим у відповідній юрисдикції. Залежно від існуючого законодавства кандидати повинні бути наперед поінформовані щодо діяльності з ретельної перевірки.

8.1.3 Терміни та умови найму

Контроль

Як частину своїх зобов'язань за контрактом, найманий персонал, контрактори та користувачі третьої сторони повинні погодити і підписати терміни та умови свого контракту з найму, який повинен встановити взаємні відповідальності щодо інформаційної безпеки.

Настанова щодо впровадження

Терміни та умови найму повинні погоджуватися з політикою безпеки організації, роз'яснювати та встановлювати:

a) що весь найманий персонал, контрактори та користувачі третьої сторони, яким наданий доступ до чутливої інформації, повинні підписати угоду щодо конфіденційності або нерозголошення до надання доступу до засобів оброблення інформації;

b) правову відповідальність та права найманого персоналу, контракторів та будь-яких інших користувачів, наприклад, стосовно законів про авторське право або законодавства про захист даних (див. також 15.1.1 та 15.1.2);

c) відповідальності за класифікацію інформації і управління активами організації, пов'язаними з інформаційними системами та послугами, з якими має справу найманий персонал, контрактор або користувач третьої сторони (див. також 7.2.1 та 10.7.3);

d) відповідальності найманого персоналу, контрактора або користувача третьої сторони за оброблення інформації, отриманої від інших компаній або зовнішніх сторін;

e) відповідальності організації щодо поводження з персональною інформацією, в тому числі персональною інформацією, створеною в результаті або в ході найму в цю організацію (див. також 15.1.4);

f) відповідальності поза межами службових приміщень організації та поза межами звичайного робочого часу, наприклад, у випадку роботи вдома (див. також 9.2.5 та 11.7.1);

g) дії, яких треба вжити, якщо найманий персонал, контрактор або користувач третьої сторони нехтує вимогами безпеки організації (див. також 8.2.3).

Організація повинна забезпечити, що найманий персонал, контрактори та користувачі третьої сторони згодні з термінами та умовами щодо інформаційної безпеки, які відповідають виду та ступеню доступу, який вони матимуть до

активів організації, пов’язаних з інформаційними системами та послугами.

Там, де це потрібно, відповідальність, що міститься в термінах та умовах найму, повинна розповсюджуватися на визначений період після закінчення найму (див. також 8.3).

Додаткова інформація

Можна застосувати кодекс поведінки, щоб охопити відповідальності найманого персоналу, контракторів та користувачів третьої сторони стосовно конфіденційності, захисту даних, етики, належного використання обладнання та засобів організації, а також гідні поваги правила поведінки, очікувані організацією. Контрактори та користувачі третьої сторони можуть бути пов’язані з зовнішньою організацією, від якої можна у свою чергу вимагати вступу в контрактні угоди від імені контрактної особи.

8.2 Протягом найму

Ціль: Впевнитись, що весь найманий персонал, контрактори 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.

Повинні бути визначені відповідальності керівництва для гарантії, що в організації безпека здійснюється протягом всього найму особи.

Для мінімізації можливих ризиків безпеки всьому найманому персоналу, контракторам та користувачам третьої сторони повинен бути забезпечений відповідний рівень поінформованості, освіти та навчання щодо процедур безпеки та коректного використання засобів оброблення інформації. Повинен бути встановлений офіційно оформлений дисциплінарний процес обробки порушень безпеки.

8.2.1 Відповідальності керівництва

Контроль

Керівництво повинне вимагати від найманого персоналу, контракторів та користувачів третьої сторони застосування безпеки згідно з установленими в організації політиками та процедурами.

Настанова щодо впровадження

Відповідальності керівництва повинні охоплювати забезпечення того, щоб найманий персонал, контрактори та користувачі третьої сторони:

a) належним чином ознайомлені зі своїми ролями щодо інформаційної безпеки та відповідальностями перед наданням доступу до чутливої інформації або інформаційних систем;

b) забезпечені настановами для встановлення в організації очікуваної безпеки їх ролей;

c) мотивовані на виконання політики безпеки організації;

Національна примітка.

Мотивація на виконання політики безпеки охоплює: усвідомлення важливості дотримання процедур, інструкцій, настанов тощо, розуміння своїх відповідальностей і наслідків невідповідних дій чи зловживань інформацією або засобами оброблення інформації організації, до яких надано доступ, а також знання дисциплінарного процесу і впевненість, що своєчасні попередження про інциденти інформаційної безпеки чи власні ненавмисні порушення безпеки і виконання передбачених для цих випадків дій призведе до менших втрат для організації та наслідків для особи, що їх спричинила.

d) досягли рівня поінформованості щодо безпеки, який відповідає їх ролям та відповідальностям в організації;

e) задовольняють терміни та умови найму, що охоплюють політику інформаційної безпеки організації та відповідні методи роботи;

f) підтримують належні навички та кваліфікацію на відповідному рівні.

Додаткова інформація

Якщо найманий персонал, контрактори та користувачі третьої сторони не поінформовано щодо їх відповідальностей стосовно безпеки, вони можуть спричинити значну шкоду організації. Мотивований персонал ймовірніше буде більш надійним і спричинятиме менше інцидентів інформаційної безпеки.

Незадовільне управління може викликати у персоналу недооціненння, що призводить до негативних впливів на безпеку організації. Наприклад, незадовільне управління може призвести до нехтування безпекою або потенційного зловживання активами організації.

8.2.2 Поінформованість, освіта і навчання щодо інформаційної безпеки

Контроль

Увесь найманий персонал організації, а там, де це суттєво, і контрактори 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.

Настанова щодо впровадження

Навчання для поінформованості повинно починатися з офіційно оформленої процедури, спроектованої для ознайомлення з політикою безпеки організації та очікуваннями до надання доступу до інформації або послуг.

Національна примітка.

Рекомендується започаткувати офіційну процедуру навчання правилам роботи на комп'ютерах, основам політики безпеки банку, правилам поведінки та поводження з клієнтами тощо для усіх категорій працівників банку.

Продовження навчання повинно охоплювати вимоги безпеки, правові відповідальності та бізнес-контролі, а також навчання коректному використанню засобів оброблення інформації, наприклад, процедурі реєстрації, використанню пакетів програмного забезпечення та інформації щодо дисциплінарного процесу (див. 8.2.3).

Додаткова інформація

Поінформованість з безпеки, освіта та навчання повинні бути суттєвими і відповідати ролі, відповідальності та навичкам особи, повинні охоплювати інформацію щодо відомих загроз, належних каналів звітування щодо інцидентів інформаційної безпеки (див. також 13.1) і того, з ким контактувати для отримання подальших рекомендацій з безпеки.

Навчання для поліпшення поінформованості призначене для того, щоб надати можливість працівникам усвідомити проблеми та інциденти інформаційної безпеки і реагувати згідно з потребами їхніх посадових ролей.

8.2.3 Дисциплінарний процес

Контроль

Повинен існувати офіційно оформлений дисциплінарний процес щодо найманого персоналу, який здійснив порушення безпеки.

Настанова щодо впровадження

Дисциплінарний процес не повинен розпочинатися без попередньої верифікації того, що порушення безпеки сталося (див. також 13.2.3 щодо збирання доказів).

Офіційно оформлений дисциплінарний процес повинен забезпечувати коректний та справедливий розгляд справи найманого персоналу, якого підозрюють у вчиненні порушень безпеки. Повинен існувати офіційно оформлений дисциплінарний процес для диференційованого реагування, яке бере до уваги такі фактори: відповідне законодавство, бізнес контракти, сутність та тяжкість порушення і його вплив на бізнес, чи є це перше або повторне правопорушення, проходив чи ні порушник належне навчання, а також інші необхідні фактори. У серйозних випадках неналежного поводження процес повинен передбачати невідкладне позбавлення обов’язків, прав доступу та повноважень і негайне випроваджування, за необхідності, з місцеперебування.

Додаткова інформація

Дисциплінарний процес повинен також використовуватися як фактор утримування від порушень політики та процедур безпеки, а також будь-яких інших порушень безпеки найманим персоналом, контакторами і користувачами третьої сторони.

8.3 Припинення або зміна умов найму

Ціль: Впевнитись, що весь найманий персонал, контрактори та користувачі третьої сторони залишають організацію чи змінюють умови найму в установленому порядку.

Повинні бути встановлені відповідальності для гарантії, що найманий персонал, контрактори та користувачі третьої сторони покидають організацію під контролем і що завершено повернення всього обладнання та видалення всіх прав

доступу.

Управління зміною відповідальностей та умов найму в організації повинне виконуватися як припинення передбачених відповідальностей або умов найму згідно з цим розділом, а будь-якими новими умовами найму треба управляти як описано в розділі 8.1.

8.3.1 Припинення відповідальностей

Контроль

Повинні бути чітко визначені та встановлені відповідальності за виконання процедур припинення найму або зміни умов найму.

Настанова щодо впровадження

При припиненні відповідальностей повинні доводитися до відому вимоги безпеки, що продовжують діяти, та правова відповідальність, і, за необхідності, відповідальності, що містяться у будь-якій угоді щодо конфіденційності (див. 6.1.5), терміни і умови найму (див. 8.1.3), які продовжуються на визначений період після звільнення найманого персоналу, контрактора або користувача третьої сторони.

Відповідальності та обов'язки, ще чинні після припинення найму, повинні міститися у контрактах найманого персоналу, контрактора або користувача третьої сторони.

Змінами відповідальності або умов найму треба управляти також, як припиненням передбаченої відповідальності або найму, а нові відповідальності або умови найму повинні контролюватися як описано в розділі 8.1.

Додаткова інформація

Зазвичай відділ кадрів є відповідальним за весь процес припинення найму і для управління аспектами безпеки суттєвих процедур співпрацює з безпосереднім керівником особи, що звільняється. У випадку, коли це контрактор, цей процес припинення відповідальності може виконувати агенція, відповідальна за контрактора, а у випадку іншого користувача це може виконувати його організація.

Може виникнути необхідність повідомляти найманий персонал, клієнтів, контракторів або користувачів третіх сторін про зміни, що стосуються персоналу та функціонування.

8.3.2 Повернення активів

Контроль

Увесь найманий персонал, контрактори та користувачі третьої сторони повинні повернути всі активи організації, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди.

Настанова щодо впровадження

Офіційно оформлений процес припинення найму повинен включати

повернення усього раніше виданого програмного забезпечення, корпоративних документів та обладнання. Також треба повернути інші активи організації, такі як мобільні обчислювальні пристрої, кредитні картки, картки доступу, програмне забезпечення, інструкції та інформацію, збережену на електронних носіях.

Якщо найманий персонал, контрактори та користувачі третьої сторони купує обладнання, що належить організації, або використовує своє власне персональне обладнання, треба слідувати процедурам, які забезпечують, що вся суттєва інформація передається організації і надійно видаляється з обладнання (див. також 10.7.1).

У випадках, коли найманий персонал, контрактори та користувачі третьої сторони має відомості, важливі для подальшого функціонування організації, ця інформація повинна бути задокументована і передана організації.

8.3.3 Вилучення прав доступу

Контроль

Після припинення найму, контракту чи угоди будь-якого найманого персоналу, контракторів і користувачів третьої сторони права їх доступу до інформації та засобів оброблення інформації повинні бути вилучені або пристосовані до зміни.

Настанова щодо впровадження

Після припинення найму права доступу особи до активів, пов’язаних з інформаційними системами та послугами, повинні бути переглянуті. Це повинне визначити, чи необхідно видалити права доступу. Зміни умов найму повинні відобразитися у видаленні всіх прав доступу, які не ухвалено для нових умов найму. Права доступу, які повинні бути видалені або адаптовані, стосуються фізичного та логічного доступу, ключів, ідентифікаційних карток, засобів оброблення інформації (див. також 11.2.4), передплати (підписки), видалення з будь-якої документації, яка ідентифікує його як наявного представника організації. Якщо найманий персонал, контрактор або користувач третьої сторони, що звільняються, знають паролі облікових записів, які залишаються активними, вони повинні бути змінені після припинення або зміни умов найму, договору або угоди.

Права доступу до інформаційних активів та засобів оброблення інформації повинні бути скорочені або видалені до припинення або зміни умов найму залежно від оцінювання таких факторів ризику:

a) чи було припинення або зміна умов найму ініційовано найманим персоналом, контрактором або користувачем третьої сторони чи керівництвом і причини припинення найму;

b) поточні обов’язки найманого персоналу, контрактора або користувача третьої сторони;

c) цінність активів, які залишаються доступними.

Додаткова інформація

За деяких обставин права доступу можуть розподілятися таким чином, щоб бути доступними більшій кількості людей, ніж звільнюваний найманий персонал, контрактор або користувач третьої сторони, наприклад, групові ідентифікатори. За таких обставин звільнювані особи повинні бути видалені з усіх списків групового доступу, і повинні бути вжиті заходи, щоб рекомендувати іншому найманому персоналу, контракторам або користувачам третьої сторони, яких це стосується, далі не використовувати інформацією спільно із звільнюваною особою.

У випадках припинення найму, ініційованого керівництвом, ображений найманий персонал, контрактор або користувач третьої сторони можуть навмисно зіпсувати інформацію або пошкодити засоби оброблення інформації. У випадку відставки людей вони можуть зробити спробу зібрати інформацію для майбутнього використання.

9 Фізична безпека та безпека інфраструктури

9.1 Зони безпеки

Ціль*:* Запобігти неавторизованому фізичному доступу, ушкодженню та вторгненню до службових приміщень організації та втручанню в її інформацію.

Засоби оброблення критичної або чутливої інформації повинні бути розміщені в зонах безпеки, захищених визначеними периметрами безпеки, з належними бар'єрами безпеки та контролями прибуття. Вони повинні бути фізично захищені від неавторизованого доступу, ушкодження та втручання.

Наданий захист повинен бути пропорційним ідентифікованим ризикам.

9.1.1 Периметр фізичної безпеки

Контроль

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).

Національна примітка.

Банки повинні виконувати усі вимоги нормативно-правових актів Національного банку України з питань технічного захисту інформації для приміщень банків, де обробляються електронні банківські документи.

Настанова щодо впровадження

Щодо периметрів фізичної безпеки треба розглянути та впровадити там, де належно, такі настанови:

a) периметри безпеки повинні бути чітко визначені, а розміщення та міцність кожного з периметрів повинні залежати від вимог безпеки щодо активів в межах цього периметра та результатів оцінки ризику;

b) периметри будівлі або приміщень, які містять засоби оброблення інформації, повинні бути фізично надійними (тобто там не повинно бути проміжків у периметрі або зон, де легко може статись зламування); зовнішні стіни приміщень повинні бути міцної конструкції і всі зовнішні двері повинні бути відповідним чином захищені від неавторизованого доступу контрольними механізмами, наприклад, засувами, тривожною сигналізацією, замками тощо; двері та вікна повинні бути замкнені, коли залишаються без нагляду, також треба передбачити зовнішній захист для вікон, особливо на рівні землі;

c) повинні бути наявною зона чергування або інші засоби контролю фізичного доступу до приміщень або будівлі; доступ до приміщень або будівель повинен дозволятися лише авторизованому персоналу;

d) щоб запобігти неавторизованому фізичному доступу та псуванню інфраструктури там, де це потрібно, повинні бути побудовані фізичні бар'єри;

e) усі пожежні двері у периметрі безпеки повинні бути обладнані тривожною сигналізацією, треба здійснювати їх моніторинг та тестувати разом зі стінами, щоб встановити потрібний рівень опору згідно з відповідними регіональними, національними та міжнародними стандартами; вони повинні

безвідмовно функціонувати згідно з місцевими правилами пожежної безпеки;

f) згідно з національними, регіональними або міжнародними стандартами повинні бути встановлені придатні системи виявлення порушників, їх треба регулярно тестувати щодо охоплення цими системами всіх зовнішніх дверей та доступних вікон; незайняті зони повинні постійно бути під охороною тривожної сигналізації; також необхідно забезпечувати наданий захист для інших зон, наприклад, кімнат з комп'ютерами та засобами комунікацій;

g) засоби оброблення інформації, якими управляє організація, повинні бути фізично відокремлені від засобів, якими управляють треті сторони.

Додаткова інформація

Фізичної захищеності можна досягти створенням одного чи більше фізичних бар'єрів навколо службових приміщень та засобів оброблення інформації організації. Використання численних бар'єрів надає додатковий захист, за якого відмова одного бар'єра не означає негайної компрометації безпеки.

Зоною безпеки може бути офіс, що замикається, або декілька кімнат, оточених суцільним внутрішнім бар'єром фізичної безпеки. Для контролю фізичного доступу між зонами з різними вимогами безпеки всередині периметру безпеки можуть бути потрібні додаткові бар'єри та периметри.

Особливої уваги щодо безпеки фізичного доступу потребують будівлі, де розташовані різні організації.

9.1.2 Контролі фізичного прибуття

Контроль

Зони безпеки повинні бути захищені належними контролями прибуття, щоб забезпечити, що доступ дозволений тільки авторизованому персоналу

Настанова щодо впровадження

Треба розглянути наведені нижче настанови:

a) треба записувати дату та час прибуття та відбуття відвідувачів та наглядати за всіма відвідувачами, якщо тільки надання їм доступу не було попередньо затверджено; треба надавати їм доступ лише для певних авторизованих цілей і видавати інструкції щодо вимог безпеки зони та процедур на випадок надзвичайних обставин;

b) доступ до зон, де зберігають або обробляють чутливу інформацію, треба контролювати та обмежити лише авторизованим персоналом; для авторизації та підтвердження всіх доступів треба використовувати контролі автентифікації, наприклад, картки контролю доступу плюс ПІН (персональний ідентифікаційний номер); треба підтримувати безпеку журналів аудиту всіх доступів;

c) треба вимагати, щоб весь найманий персонал, контрактори та користувачі третьої сторони, а також усі відвідувачі носили певну видиму ідентифікацію і негайно сповіщали персонал служби безпеки, якщо вони зустрічають відвідувачів без супроводу та будь-кого без видимої ідентифікації;

d) персоналу служби підтримки третьої сторони, лише за потреби, повинен бути наданий обмежений доступ до зон безпеки або засобів оброблення чутливої інформації; треба здійснювати авторизацію та моніторинг цього доступу;

e) права доступу до зон безпеки треба регулярно переглядати та актуалізувати, а в разі необхідності відміняти (див. 8.3.3).

9.1.3 Убезпечення офісів, кімнат і обладнання

Контроль

Повинна бути розроблена і застосована фізична безпека офісів, кімнат і обладнання.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо безпеки офісів, кімнат та обладнання:

a) треба враховувати суттєві нормативи та стандарти охорони здоров'я та безпеки;

b) основні засоби повинні бути розташовані таким чином, щоб уникнути публічного доступу;

c) за можливості, будівлі повинні не привертати увагу і мінімально позначати своє призначення, без видимих ознак всередині або ззовні будівлі, що ідентифікують наявність діяльності з оброблення інформації;

d) довідники та внутрішні телефонні книжки, які ідентифікують розміщення засобів оброблення чутливої інформації, не повинні бути легко доступними для широкого загалу.

9.1.4 Захист від зовнішніх та інфраструктурних загроз

Контроль

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.

Настанова щодо впровадження

Треба розглянути будь-які загрози безпеці з боку сусідніх службових приміщень, наприклад, пожежа в сусідній будівлі, вода, що протікає з даху чи просочується з поверхів підземного рівня, або вибух на вулиці.

Щоб уникнути пошкоджень внаслідок пожежі, повені, землетрусу, вибуху, акцій громадської непокори та інших форм стихійного або спричиненого людьми лиха треба розглянути наведені нижче настанови:

a) небезпечні або займисті матеріали повинні зберігатися на безпечній відстані від зони безпеки. Оптові запаси, такі як канцелярське приладдя, не повинні зберігатися в межах зони безпеки;

b) обладнання відновлення та носії резервних копій повинні бути розміщені на безпечній відстані, щоб уникнути ушкодження від лиха, яке впливає на основне приміщення;

Національна примітка.

Банки мають забезпечувати виконання вимог нормативно-правових актів Національного банку України щодо забезпечення безперервного функціонування інформаційних систем банків України.

c) треба надати і придатним чином розмістити належне протипожежне обладнання.

9.1.5 Робота в зонах безпеки

Контроль

Повинні бути розроблені та застосовані фізичний захист і настанови щодо роботи в зонах безпеки.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови:

a) про існування зон безпеки або діяльність у них персонал повинен бути поінформований лише в межах необхідних для його роботи;

b) треба уникати роботи в зонах безпеки без нагляду як з причин безпеки, так і з метою запобігання можливій зловмисній діяльності;

c) незайняті зони безпеки повинні бути фізично замкнені і періодично перевірятися;

d) використання фото-, відео-, аудіо- та іншого обладнання для запису, як, наприклад, камер в мобільних телефонах, не повинно дозволятися, доки воно не авторизоване.

Заходи щодо роботи в зонах безпеки охоплюють як контролі щодо найманого персоналу, контракторів і користувачів третьої сторони, які працюють в зонах безпеки, так і щодо іншої діяльності третьої сторони, яка там здійснюється.

9.1.6 Зони загального доступу, доставки та відвантаження

Контроль

Щоб уникнути неавторизованого доступу, точки доступу, наприклад, зони доставки та відвантаження, а також інші точки, через які особи, доступ яких не авторизовано, можуть увійти до службових приміщень, повинні бути контрольовані і, за можливості, ізольовані від засобів оброблення інформації.

Настанова щодо впровадження

Треба розглянути наведені нижче рекомендації:

a) доступ до зон постачання та завантаження іззовні будинку повинен бути обмежений ідентифікованим і авторизованим персоналом;

b) зони постачання та завантаження повинні бути спроектовані таким чином, щоб поставки могли бути розвантажені без отримання персоналом доставляння доступу до інших частин будівлі;

c) зовнішні двері зони постачання та завантаження повинні бути замкнені, коли відчинені внутрішні двері;

d) матеріали, що надходять, повинні обстежуватися на потенційні загрози

(див. 9.2.1d) до того, як вони будуть переміщені з зони постачання та завантаження до місця використання;

e) матеріали, що надходять, повинні реєструватися згідно з процедурою управління активом (див. також 7.1.1) на вході до приміщення;

f) партії товару, що надходять і відсилаються, повинні бути, за можливості, фізично розподілені.

9.2 Безпека обладнання

Ціль: Запобігти втратам, ушкодженню, крадіжці або компрометації активів та перериванню діяльності організації.

Обладнання повинне бути захищене від фізичних та екологічних загроз.

Для зменшення ризику неавторизованого доступу до інформації та для захисту від втрати та ушкодження обладнання повинне бути захищене (охоплюючи те, що використовується зовні, і те майно, що переміщується). При цьому треба також розглянути розміщення та вилучення обладнання. Для захисту від фізичних загроз і для охорони засобів життєзабезпечення, таких як електроживлення та кабельна інфраструктура, можуть бути потрібними спеціальні контролі.

9.2.1 Розміщення та захист обладнання

Контроль

Обладнання повинне бути розміщене чи захищене таким чином, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого неавторизованого доступу.

Настанова щодо впровадження

Для захисту обладнання треба розглянути наведені нижче настанови:

a) обладнання повинне бути розміщене так, щоб мінімізувати непотрібний доступ до робочих зон;

b) засоби оброблення інформації, що обробляють чутливі дані, повинні бути розташовані під обмеженим кутом огляду для зниження ризику спостереження інформації неавторизованими особами під час її використання, та забезпечити безпеку засобів зберігання для уникнення неавторизованого доступу;

c) елементи, що потребують спеціального захисту, повинні бути ізольовані, для зменшення загального рівня необхідного захисту;

d) повинні бути узгоджені контролі для мінімізації ризику потенційних фізичних загроз, наприклад, крадіжки, вогню, вибухів, диму, води (або відмови постачання води), пилу, вібрації, хімічних впливів, завад електроживлення, комунікаційних завад, електромагнітного випромінювання та вандалізму;

e) повинні бути розроблені настанови щодо приймання їжі та напоїв, а також паління поблизу засобів оброблення інформації;

f) треба здійснювати моніторинг умов довкілля таких, як температура та вологість, які можуть негативно вплинути на функціонування засобів оброблення інформації;

g) для всіх будівель треба застосовувати захист від блискавки, а до всіх вхідних ліній енергопостачання та комунікацій повинні бути вбудовані фільтри захисту від блискавки;

h) для обладнання в промисловому оточенні повинне бути розглянуте застосування спеціальних методів захисту, таких як оболонки на клавіатуру;

i) треба захистити обладнання оброблення чутливої інформації для мінімізації ризику витоку інформації внаслідок випромінювання.

9.2.2 Допоміжні комунальні служби

Контроль

Обладнання повинне бути захищене від аварійних відключень живлення та інших порушень, внаслідок аварій в засобів життєзабезпечення.

Настанова щодо впровадження

Усі засоби життєзабезпечення, такі як електрика, водопостачання, водовідведення, опалення/вентиляція та кондиціювання повітря, повинні бути достатніми для систем, які вони підтримують. Засоби життєзабезпечення повинні регулярно оглядатися і, за необхідності, тестуватися для забезпечення їх належного функціонування і для зниження всілякого ризику від їх несправності або відмови. Повинне бути надане придатне електроживлення, яке відповідає специфікаціям виробника обладнання.

Для обладнання, що підтримує критичні бізнес-операції, рекомендовані джерела безперебійного живлення (UPS) для забезпечення правильного закриття або подальшу їх роботу. Плани дій в аварійних обставинах стосовно живлення повинні охоплювати дії, які треба вжити при відмові UPS. Якщо потрібно, щоб робота продовжувалась у разі тривалої відмови живлення, треба передбачити резервний генератор. Для забезпечення роботи генератора протягом тривалого часу повинен бути наявним відповідний запас пального. Обладнання UPS та генератори повинні регулярно перевірятися, щоб забезпечити, що вони мають необхідну потужність і протестовані згідно з рекомендаціями виробника. Крім того, треба розглянути використання різних джерел живлення або, якщо приміщення є великим, окрему підстанцію живлення.

Для сприяння швидкому вимкненню живлення в разі аварійних дій поблизу аварійних виходів з приміщень з обладнанням повинні бути розміщені аварійні вимикачі. На випадок відмови основного живлення повинне бути передбачене аварійне освітлення.

Водопостачання повинне бути стабільним і достатнім для забезпечення кондиціювання повітря, зволожувального обладнання та систем пожежогасіння (де вони використовуються). Несправності у системі водопостачання можуть ушкодити обладнання або не дати можливості ефективно працювати пожежогасінню. Якщо потрібно, для виявлення несправностей засобів життєзабезпечення повинна бути оцінена й інстальована сигнальна система.

Телекомунікаційне обладнання повинне бути підключене до постачальника

послуги щонайменше двома маршрутами, щоб запобігти видаленню голосових послуг при відмові одного каналу зв'язку. Голосові послуги повинні відповідати місцевим правовим вимогам щодо аварійного зв'язку.

Національна примітка.

Банки мають забезпечити резервування каналів зв'язку не тільки для голосових послуг, а також для забезпечення безперервних послуг передавання інформації.

Додаткова інформація

Варіантом досягнення безперервності електроживлення є використання різних джерел живлення, щоб уникнути відмови живлення в одній точці.

9.2.3 Безпека кабельних мереж

Контроль

Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних послуг, повинні бути захищені від перехоплювання чи ушкоджень.

Настанова щодо впровадження

Повинні бути розглянуті наведені нижче настанови щодо безпеки кабельної мережі:

a) силові й телекомунікаційні лінії у засобах оброблення інформації повинні, де можливо, бути заземлені або забезпечені відповідним альтернативним захистом;

b) кабельна мережа повинна бути захищена від неавторизованого перехоплення або ушкодження, наприклад, використанням кабелепроводу або уникненням маршрутів через загальнодоступні зони;

c) силові кабелі повинні бути відокремлені від телекомунікаційних кабелів, щоб запобігти взаємному впливу;

d) для мінімізації помилок неправильного поводження, такого як випадкова комутація неправильних мережних кабелів, треба використовувати чітко ідентифіковані кабелі та марковане обладнання;

e) для зниження можливості помилок треба використовувати задокументований список комутацій;

f) для чутливих або критичних систем додаткові контролі для розгляду охоплюють:

1) інсталяцію захищеного кабелепроводу та кімнат або шаф, які замикаються, у точках вимірювання та приєднання зовнішнього провідника;

2) використання альтернативних засобів маршрутизації та/або передавання, які забезпечують належну безпеку;

3) використання оптоволоконних кабелів;

4) використання електромагнітного екранування для захисту кабелів;

5) введення технічних засобів та фізичних обстежень щодо неавторизованих пристроїв, приєднаних до кабелів;

6) контрольований доступ до комутаційних панелей та кабельних приміщень.

9.2.4 Обслуговування обладнання

Контроль

Обладнання повинне правильно обслуговуватися, щоб забезпечити його постійну доступність та цілісність.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо обслуговування обладнання:

a) обслуговування обладнання повинне виконуватися відповідно до рекомендованих постачальником специфікацій та періодів обслуговування;

b) ремонт та обслуговування обладнання повинен здійснювати лише авторизований обслуговуючий персонал;

c) повинні зберігатися записи стосовно всіх очікуваних або фактичних несправностей та усього запобіжного та коригувального обслуговування;

d) планування обслуговування обладнання повинне передбачати впровадження належних контролів, беручи до уваги, чи здійснюється таке обслуговування внутрішнім персоналом організації, чи зовнішнім; якщо необхідно, чутлива інформація повинна бути вивантажена з обладнання або обслуговуючий персонал повинен бути достатньо проінструктований;

e) повинні задовольнятися усі вимоги, накладені страхуванням.

9.2.5 Безпека обладнання поза службовими приміщеннями

Контроль

До обладнання поза службовими приміщеннями повинен бути застосовний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації.

Настанова щодо впровадження

Незалежно від власника, використання будь-якого обладнання оброблення інформації поза приміщеннями організації повинне бути авторизоване керівництвом.

Для захисту обладнання поза організацією треба розглянути наведені нижче настанови:

a) обладнання та носії, винесені з службових приміщень організації, не повинні залишатися без нагляду у загальнодоступних місцях; портативні комп’ютери при переїздах треба переносити як ручний багаж і, за можливості, приховувати;

b) завжди треба дотримуватися інструкцій виробника щодо захисту обладнання, наприклад, захисту від впливу сильних електромагнітних полів;

c) контролі для надомного обладнання повинні визначатися оцінкою ризику і застосовуватися, за необхідності, належним чином, наприклад, шафи для документів, що замикаються, політика чистого стола, контролі доступу до комп’ютерів і безпечні комунікації з офісом (див. також ISO/IEC 18028 Безпека мереж);

d) для захисту обладнання поза організацією повинен бути наявний відповідний обсяг страхового покриття.

Ризики безпеки, наприклад, ушкодження, крадіжки або підслуховування, можуть суттєво відрізнятися залежно від місцезнаходження, їх треба брати до уваги при визначенні найбільш придатних контролів.

Додаткова інформація

Обладнання збереження та оброблення інформації охоплює всі види персональних комп'ютерів, органайзерів, мобільних телефонів, смарт-карт, паперу тощо, які тримають для роботи вдома або виносять із звичайного місця роботи.

Більше інформації щодо інших аспектів захисту мобільного обладнання можна знайти в 11.7.1.

9.2.6 Безпечне вилучення або повторне використання обладнання

Контроль

Всі елементи обладнання, які містять носії пам'яті, повинні бути перевірені, щоб забезпечити, що будь-які чутливі дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення.

Настанова щодо впровадження

Пристрої, які містять чутливу інформацію, повинні бути фізично зруйновані або інформація повинна бути зруйнована, видалена або перезаписана з використанням методів, які роблять початкову інформацію невідновлюваною, а не використання стандартних функцій видалення або форматування.

Додаткова інформація

Ушкодженні пристрої, що містять чутливі дані, можуть потребувати оцінки ризику для визначення, чи краще фізично зруйнувати елементи, чи надіслати в ремонт або списати.

Через недбале видалення або повторне використання обладнання інформація може бути скомпрометована (див. також 10.7.2).

9.2.7 Переміщення майна

Контроль

Обладнання, інформація чи програмне забезпечення не повинні виноситись назовні без попередньої авторизації цих дій.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови:

a) обладнання, інформація або програмне забезпечення не повинні виноситись назовні без попередньої авторизації цих дій;

b) найманий персонал, контрактори та користувачі третіх сторін, уповноважені дозволяти переміщення активів назовні, повинні бути чітко

ідентифіковані;

c) повинні бути встановлені обмеження на термін переміщення обладнання, треба перевірити відповідність йому при поверненні обладнання;

d) там, де це необхідно і передбачено, обладнання повинне бути зареєстроване як таке, що переміщується, і зареєстроване після повернення.

Додаткова інформація

Вибіркові перевірки, вжиті для виявлення неавторизованого переміщення майна, можуть також виконуватися для виявлення неавторизованих пристроїв записування, зброї тощо і запобігання внесенню їх в організацію. Такі вибіркові перевірки повинні виконуватися відповідно до законодавства та нормативів. Особи повинні бути поінформовані щодо проведення вибіркових перевірок, і перевірки повинні виконуватися лише за дозволом, якого вимагає законодавство та нормативи.

10 Управління комунікаціями та функціонуванням

10.1 Процедури функціонування та відповідальності

Ціль: Забезпечити коректне та безпечне функціонування засобів оброблення інформації.

Повинні бути встановлені відповідальності та процедури управління і функціонування усіх засобів оброблення інформації. Це охоплює розроблення належних процедур функціонування.

Там, де це потрібно, повинен бути запроваджений розподіл обов'язків для зменшення ризику навмисного або викликаного недбалістю зловживання системою.

10.1.1 Задокументовані процедури функціонування

Контроль

Процедури функціонування повинні бути задокументовані, підтримувані та зроблені доступними для всіх користувачів, що їх потребують.

Настанова щодо впровадження

Повинні бути підготовлені задокументовані процедури щодо безпеки і діяльності системи, пов'язаної з засобами оброблення інформації та комунікаціями, такі як процедури запуску і завершення роботи комп'ютера, резервного копіювання, обслуговування обладнання, поводження з носіями, управління комп'ютерними приміщеннями і обробленням пошти.

Процедури функціонування повинні визначати докладні інструкції для виконання кожної роботи, охоплюючи:

a) оброблення та поводження з інформацією;

b) резервне копіювання;

c) вимоги диспетчеризації, охоплюючи взаємозалежність з іншими системами, час самого раннього початку і самого пізнього завершення роботи;

d) інструкції щодо поводження з помилками або іншими надзвичайними обставинами, які можуть виникнути протягом виконання роботи, охоплюючи обмеження на використання системних утиліт (див. 11.5.4);

e) підтримка контактів у випадку неочікуваних технічних проблем або проблем функціонування;

f) певні інструкції щодо поводження з вихідними даними і носіями, такі як використання певного паперу або управління конфіденційними вихідними даними, охоплюючи процедури безпечного вилучення вихідних даних із завдань, що відмовили (див. 10.7.2 та 10.7.3);

g) процедури перезапуску та відновлення системи для використання у разі відмови системи;

h) управління журналом аудиту та інформацією реєстраційного журналу системи (див. 10.10).

Процедури функціонування та задокументовані процедури щодо діяльності системи повинні розглядатися як авторизовані керівництвом офіційно оформлені

документи і зміни. Там, де це технічно можливо, інформаційні системи повинні управлятися однаковим чином, із використанням однакових процедур, інструментів і утиліт.

10.1.2 Управління змінами

Контроль

Зміни у засобах оброблення інформації та системах повинні бути контрольованими.

Настанова щодо впровадження

Операційні системи та прикладне програмне забезпечення повинні підлягати жорсткому контролю управляння змінами.

Зокрема, треба розглянути наведені нижче елементи:

a) ідентифікація та реєстрація значних змін;
b) планування та тестування змін;
c) оцінка потенційних впливів, охоплюючи впливи таких змін на безпеку;
d) процедура офіційного оформлення затвердження запропонованих змін;
e) доведення до відому всіх відповідних осіб подробиць зміни;
f) процедури нейтралізації несправностей, охоплюючи процедури та відповідальності щодо припинення та відновлення після невдалих змін та непередбачуваних подій.

Повинні бути наявні офіційно оформлені відповідальності керівництва та процедури для забезпечення задовільного контролю всіх змін, що стосуються обладнання, програмного забезпечення або процедур. Після проведення змін журнал реєстрації аудиту, який містить усю суттєву інформацію, повинен тривало зберігатися.

Національна примітка.

Банки мають розробити докладні процедури внесення змін до програмного забезпечення систем автоматизації банківської діяльності, які обов'язково повинні включати процедури тестування програмного забезпечення на тестовому комп'ютерному обладнанні. Забороняється вносити зміни до програмно-технічних комплексів, які працюють у промислової експлуатації, без попереднього тестування.

Додаткова інформація

Звичайною причиною відмов систем або безпеки є невідповідний контроль змін у засобах оброблення інформації та системах. Зміни операційного середовища, особливо при переводі системи від етапу розроблення до етапу промислової експлуатації, можуть вплинути на надійність прикладних програм (див. також 12.5.1).

Зміни до систем, які працюють в промислової експлуатації, повинні здійснюватися лише тоді, коли є дійсна бізнес-причина їх робити, наприклад, збільшення ризику системи. Оновлення систем на пізніші версії операційних систем або прикладних програм не завжди відповідає бізнес-інтересам, оскільки це може внести більше вразливостей та нестабільності, ніж поточна версія. Може також виникнути потреба у додатковому навчанні, витратах на ліцензії, підтримку, витратах на обслуговування і адміністрування та нове апаратне

забезпечення, особливо під час міграції.

10.1.3 Розподілення обов'язків

Контроль

Обов'язки та сфери відповідальності повинні бути розподілені для зменшення можливості неавторизованої або ненавмисної модифікації активів організації чи зловживання ними.

Настанова щодо впровадження

Розподілення обов'язків є методом зменшення ризику випадкового або навмисного зловживання системою. Треба потурбуватися, щоб жодна окрема особа не могла мати доступ, модифікувати або використовувати активи без авторизації або виявлення цього. Ініціювання події повинно бути відокремлене від її авторизації. При проектуванні контролів повинна бути розглянута можливість змови.

Невеликі організації можуть вважати, що досягти розподілення обов'язків важко, проте цей принцип повинен застосовуватися наскільки це можливо й практично. Кожного разу, коли важко здійснити розподілення, треба розглянути інші контролі, такі як моніторинг діяльності, журнал аудиту і нагляд керівництва. Важливо, щоб аудит безпеки залишався незалежним.

10.1.4 Відокремлення засобів розробки, тестування та функціонування

Контроль

Засоби розроблення, тестування та функціонування повинні бути відокремлені для зменшення ризиків неавторизованого доступу до системи, яка працює в промислової експлуатації, або її неавторизованої зміни.

Настанова щодо впровадження

Треба ідентифікувати рівень відокремлення середовищ: функціонування, тестування та розроблення, необхідний для запобігання операційним проблемам, і впровадити належні контролі.

Треба розглянути наведені нижче елементи:

a) повинні бути визначені й задокументовані правила переведення програмного забезпечення з етапу розроблення до етапу промислової експлуатації;

b) програмне забезпечення, яке розробляється та працює в промислової експлуатації, забезпечення повинні запускатися на різних системах або комп'ютерних процесорах і в різних доменах або директоріях;

c) компілятори, редактори та інші інструменти розробляння або системні утиліти не повинні бути доступними з систем, які працюють в промислової експлуатації, коли це не потрібно;

d) середовище тестування системи повинне емулювати середовище системи, яка працює в промислової експлуатації, настільки близько, наскільки це можливо;

e) для зниження ризику помилки користувачі повинні використовувати

різні користувацькі профілі для систем, які працюють в промислової експлуатації, та тестових систем, меню повинні виводити на екран належні ідентифікаційні повідомлення;

f) чутливі дані не повинні копіюватися в середовище тестової системи (див. 12.4.2).

Додаткова інформація

Діяльність з розроблення та тестування може спричинити серйозні проблеми, наприклад, небажану модифікацію файлів або середовища системи, або відмову системи. У цьому разі є потреба підтримувати відоме та стабільне середовища, в якому здійснювати змістовне тестування і запобігати неналежному доступу розробника.

Там, де персонал, який займається розробленням та тестуванням, має доступ до системи, яка працює в промислової експлуатації, та її інформації, він може внести неавторизований та непротестований код або змінити операційні дані. В деяких системах такою можливістю можуть зловживати для вчинення шахрайства або внесення непротестованого чи зловмисного коду, який може спричинити серйозні проблеми функціонування.

Розробники та тестувачі також ставлять під загрозу конфіденційність операційної інформації. Діяльність з розроблення та тестування може спричинити ненавмисні зміни у програмному забезпеченні або інформації, якщо спільно використовується те ж саме комп'ютерне середовище. Тому бажаним є відокремлення засобів розроблення, тестування та функціонування для зменшення ризику випадкової зміни або неавторизованого доступу до операційного програмного забезпечення та бізнес-даних (див. також 12.4.2 стосовно захисту даних тестування).

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.

Організація повинна перевірити запровадження угод, здійснювати моніторинг відповідності цими угодами і управляти змінами, щоб забезпечити, що надані послуги задовольняють усім вимогам, погодженим з третьою стороною.

10.2.1 Надання послуг

Контроль

Треба забезпечити, що контролі безпеки, визначення послуг та рівень їх надання, які містить угода щодо надання послуг третьою стороною, впроваджені, функціонують та підтримуються третьою стороною.

Настанова щодо впровадження

Надання послуг третьою стороною повинне включати погоджені заходи безпеки, визначення послуги та аспекти управління послугою. У випадку аутсорсингових заходів організація повинна планувати необхідне переміщення

(інформації, засобів оброблення інформації і всього іншого, що потребує переміщення) і повинна забезпечити підтримання безпеки протягом усього періоду переміщення.

Організація повинна забезпечити, що третя сторона підтримує достатні характеристики послуги разом із планами щодо забезпечення функціонування, розробленими для забезпечення того, щоб погоджені рівні безперервності послуги підтримувалися після основних відмов послуги або лих (див. 14.1).

10.2.2 Моніторинг та перегляд послуг третьої сторони

Контроль

Послуги, звіти та записи, надавані третьою стороною, повинні підлягати регулярному моніторингу і перегляду та повинні проводитись регулярні аудити.

Настанова щодо впровадження

Моніторинг та перегляд послуг третьої сторони повинні забезпечувати, що дотримуються терміни й умови інформаційної безпеки угод і що управління інцидентами інформаційної безпеки та проблемами здійснюється належним чином. Це повинне охоплювати взаємодію та процес управління послугою між організацією та третьою стороною щодо:

a) моніторингу рівнів продуктивності послуги для перевірки дотримання угоди;

b) перегляду звітів стосовно послуги, наданих третьою стороною, та проведення регулярних нарад щодо виконання робіт згідно з вимогами угоди;

c) надання інформації про інциденти інформаційної безпеки та перегляд цієї інформації третьою стороною і організацією згідно з угодою й будь-якими настановами та процедурами, що її підтримують;

d) перегляду журналів аудиту третьої сторони та записів про події безпеки, проблеми функціонування та відмови, відстежування недоліків та порушень, пов’язаних з надаваною послугою;

e) вирішення та управління всіма ідентифікованими проблемами.

Відповідальність щодо управління взаємодією з третьою стороною повинна бути покладена на особу або групу управління послугою. Крім того, організація повинна забезпечити, що третя сторона встановила відповідальності щодо перевірки відповідності та примусового застосування вимог угод. Для моніторингу цих вимог угоди (див. 6.2.3) повинні бути наявними достатні технічні навички та ресурси, особливо повинні задовольнятися вимоги інформаційної безпеки. Якщо помічено недоліки в наданні послуги, треба вжити належні дії.

Організація повинна підтримувати достатній загальний контроль та спостережність всіх аспектів безпеки щодо чутливої або критичної інформації або засобів оброблення інформації, які доступні, обробляються або управляються третьою стороною. Організація повинна забезпечити збереження спостережності діяльності з безпеки, такої як управління змінами, ідентифікація вразливостей та звітування/реагування щодо інциденту безпеки відповідно до визначеного процесу, формату та структури звітування.

Додаткова інформація

У випадку аутсорсингу організації необхідно усвідомлювати, що кінцева відповідальність за інформацію, яку обробляє аутсорсингова сторона, залишається за цією організацією.

Національна примітка.

Банки, які складають угоди щодо надання аусорсингових послуг третьою стороною, повинні звернути особливу увагу на забезпечення захисту інформації, яка відноситься до банківської таємниці, не допускати ознайомлення третьої сторони з персональними даними та даними про фінансові операції і діяльність клієнтів та іншою чутливою інформацією.

10.2.3 Управління змінами у послугах третьої сторони

Контроль

Зміни у наданні послуг, охоплюючи підтримування і вдосконалювання існуючих політик інформаційної безпеки, процедур і контролів, повинні управлятися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків.

Настанова щодо впровадження

Процес управління змінами до послуг третьої сторони потребує урахування наведеного нижче:

a) зміни, зроблені організацією для впровадження:
   1) покращень поточних пропонованих послуг;
   2) розроблення будь-яких нових прикладних програм і систем;
   3) модифікації або оновлення політик та процедур організації;
   4) нових контролів для розв'язання інцидентів безпеки та вдосконалення безпеки;
b) зміни у послугах третьої сторони, щоб впровадити:
   1) зміни та покращення у мережах;
   2) використання нових технологій;
   3) погодження нових продуктів або новіших версій/варіантів реалізації;
   4) нові інструменти та середовище розробки;
   5) зміни фізичного розташування засобів надання послуги;
   6) зміну виробників.

10.3 Планування та приймання системи

Ціль: Мінімізувати ризик відмови систем.

Для надання потрібної продуктивність системи обов'язковими є перспективне планування та підготовка, щоб забезпечити доступність необхідної потужності та ресурсів.

Для зниження ризику перевантаження системи треба спроектувати вимоги щодо майбутньої пропускної здатності.

Операційні вимоги до нових систем повинні бути розроблені, задокументовані і протестовані до їх прийняття й використання.

10.3.1 Управління потужністю

Контроль

Щоб забезпечити потрібну продуктивність системи, треба здійснювати моніторинг та регулювати використання ресурсів і проектувати вимоги до майбутньої потужності.

Настанова щодо впровадження

Для кожної нової або виконуваної діяльності повинні бути ідентифіковані вимоги до потужності. Для забезпечення і, за необхідності, поліпшення доступності та ефективності систем повинні застосовуватися настройка та моніторинг систем. Для вчасного виявлення проблем повинні бути наявними контролі виявлення. Проектування майбутніх вимог до потужності повинне брати до уваги нові вимоги бізнесу та систем і поточні та прогнозовані тенденції щодо можливостей оброблення інформації організації.

Особливу увагу треба звернути на будь-які ресурси, які потребують довгого часу для закупівлі або великих витрат; тому керівники повинні здійснювати моніторинг використання основних ресурсів системи. Вони повинні ідентифікувати тенденції використання, особливо стосовно бізнесових прикладних програм і інструментів управління інформаційними системами.

Керівники повинні використовувати цю інформацію для ідентифікації та уникнення потенційних вузьких місць та залежності від основного персоналу, який може становити загрозу для безпеки системи або послуг, й планувати належні заходи.

Національна примітка.

Банки мають планувати потужності відповідної комп'ютерної та телекомунікаційної техніки з урахуванням майбутнього зростання кількості операцій та дій, які планується виконувати з використанням програмно-технічного комплексу враховуючі потреби бізнесу.

10.3.2 Приймання системи

Контроль

Повинні бути розроблені критерії приймання нових інформаційних систем, модернізацій та нових версій і виконані придатні тести систем протягом розроблення і перед прийманням.

Настанова щодо впровадження

Керівники повинні забезпечити, щоб вимоги та критерії приймання нових систем були чітко визначені, погоджені, задокументовані та протестовані. Нові інформаційні системи, модернізації та нові версії повинні впроваджуватися в промислову експлуатацію тільки після отримання офіційно оформленого акту приймання. До надання офіційно оформленого акту приймання повинні бути розглянуті наведені нижче елементи:

a) вимоги до продуктивності та потужності комп'ютерної техніки;
b) процедури відновлення після помилок і перезапуску, а також плани дій

в аварійних обставинах;

c) підготовка і тестування стандартних операційних процедур за визначеними стандартами;

d) наявність погодженого набору контролів безпеки;

e) ефективні ручні процедури;

f) заходи щодо безперервності бізнесу (див. 14.1);

g) доказ того, що інсталяція нової системи не буде несприятливо впливати на існуючі системи, особливо у пікові часи обробляння, наприклад, у кінці місяця;

h) доказ того, що було розглянуто вплив нової системи на загальну безпеку організації;

i) навчання щодо функціонування або використання нових систем;

j) зручність використання, як вона впливає на продуктивність користувача і уникнення помилок людини.

Національна примітка.

Банкам рекомендується залучати майбутніх операторів та користувачів нової системи на стадії розроблення для проектування найбільш зручного інтерфейсу, який не буде створювати умов для ненавмисних помилок.

Для більшості нових розробок оператори та користувачі повинні отримувати консультації на всіх етапах процесу розроблення для забезпечення ефективності функціонування запропонованого системного проекту. Повинні виконуватися належні тести для підтвердження, що всі критерії приймання були повністю задоволені.

Додаткова інформація

Приймання може складатися з офіційно оформлених процедур сертифікації та акредитації для верифікації того, що всі вимоги безпеки належним чином ураховано.

10.4 Захист від зловмисного та мобільного коду

Ціль: Захистити цілісність програмного забезпечення та інформації.

Необхідна обачність, щоб запобігти і виявити внесення зловмисного коду та неавторизованого мобільного коду.

Програмне забезпечення та засоби оброблення інформації є вразливими до внесення зловмисного коду, такого як комп'ютерні віруси, мережеві „черв'яки", троянські коні та логічні бомби. Користувачі повинні бути поінформовані щодо небезпеки зловмисного коду. Керівники повинні, де необхідно, ввести контролі для запобігання, виявлення та видалення зловмисного коду та контролювати мобільний код.

10.4.1 Контролі від зловмисного коду

Контроль

Повинні бути впроваджені контролі виявлення, запобігання та відновлення для захисту від зловмисного коду і належні процедури поінформовування користувачів.

Настанова щодо впровадження

Захист від зловмисного коду повинен базуватися на виявленні зловмисного коду і виправленні програмного забезпечення, поінформовуванні щодо безпеки, належному доступі до системи та контролях управління змінами. Треба розглянути наведені нижче настанови:

a) розроблення офіційно оформленої політики, яка не допускає використання неавторизованого програмного забезпечення (див. 15.1.2);

b) розроблення офіційної оформленої політики захисту від ризиків, пов'язаних з отриманням файлів і програмного забезпечення від або через зовнішні мережі чи на будь-якому іншому носієві, із зазначенням того, які саме заходи захисту треба вжити;

c) проведення регулярних переглядів програмного забезпечення та вмісту даних систем, які підтримують критичні бізнес-процеси; наявність будь-яких непогоджених файлів або неавторизованих поправок повинна розслідуватись з офіційним оформленням;

d) інсталяцію та регулярне оновлення програмного забезпечення виявлення та знищення зловмисного коду для сканування комп'ютерів та носіїв у якості превентивного контролю або у звичайному порядку; виконувані перевірки повинні включати:

1) перевірку на зловмисний код будь-яких файлів на електронному або оптичному носії та файлів, одержаних через мережі, до застосування;
2) перевірку завантажуваних та приєднаних до електронної пошти файлів на зловмисний код до застосування; ця перевірка повинна виконуватися у різних місцях, наприклад, на серверах електронної пошти, настільних комп'ютерах та на вході в мережу організації;
3) перевірку веб-сторінок на зловмисний код;

e) визначення управлінських процедур і відповідальностей щодо захисту систем від зловмисного коду, навчання використанню систем, звітування та відновлення після атак зловмисного коду (див. 13.1 та 13.2);

f) підготовка відповідних планів безперервності бізнесу для відновлення після атак зловмисного коду, включаючи усі необхідні резервні копіювання даних і програмного забезпечення та заходи з відновлення (див. розділ 14);

g) впровадження процедур для регулярного збирання інформації, таких як підписка на списки розсилання та/або перевірка веб-сайтів, які надають інформацію щодо нових зловмисних кодів;

h) впровадження процедур для верифікації інформації, пов'язаної з зловмисним кодом, і гарантування, що попереджувальні бюлетені є точними та інформативними; керівники повинні гарантувати, що для визначення різниці між містифікацією та справжнім зловмисним кодом використовуються компетентні джерела, наприклад, журнали з гарною репутацією, достовірні Інтернет-сайти або постачальники, які надають програмне забезпечення, що захищає від зловмисного коду; усі користувачі повинні бути поінформовані щодо проблеми містифікацій і що робити при їх отриманні.

Додаткова інформація

Використання двох або більше програмних продуктів, які захищають середовище оброблення інформації від зловмисного коду і отримані від різних виробників, може покращити ефективність захисту від зловмисного коду.

Щоб забезпечити захист на сучасному рівні, може бути інстальоване програмне забезпечення захисту від зловмисного коду для надання автоматичних оновлень баз даних та засобів сканування. Крім того, це програмне забезпечення може бути інстальоване на кожний комп'ютер для виконання автоматичних перевірок.

Треба потурбуватись щодо захисту проти внесення зловмисного коду під час виконання процедур обслуговування і аварійних дій, які можуть обходити звичайні контролі захисту від зловмисного коду.

Національна примітка.

Банки мають визначити усі можливі джерела появи зловмисного коду та забезпечити надійний захист на усіх ділянках обробки інформації.

10.4.2 Контролі від мобільного коду

Контроль

Там, де використання мобільного коду авторизоване (дозволено), конфігурація повинна гарантувати, що авторизований мобільний код функціонує згідно з чітко визначеною політикою безпеки, та треба запобігти виконанню неавторизованого мобільного коду.

Настанова щодо впровадження

Треба розглянути наведені нижче дії для захисту від неавторизованих дій з виконання мобільного коду:

a) виконання мобільного коду в логічно ізольованому середовищі ;

b) блокування будь-якого використання мобільного коду;

c) блокування отримання мобільного коду;

d) активація технічних заходів, наявних у певній системі, для забезпечення того, що здійснюється управління мобільним кодом;

e) контроль ресурсів, до яких можливий доступ мобільного коду;

f) криптографічні контролі для однозначної автентифікації мобільного коду.

Додаткова інформація

Мобільний код - це код програмного забезпечення, який передається з одного комп'ютера на інший і далі виконується автоматично, та реалізує певну функцію з невеликою участю користувача або без неї. Мобільний код пов'язаний з великою кількістю послуг зв'язувального програмного забезпечення.

Крім того, для забезпечення того, що мобільний код не містить зловмисного коду, необхідним є контроль мобільного коду для уникнення неавторизованого використання або порушення системи, мережі або ресурсів прикладних програм, а також інших порушень інформаційної безпеки.

10.5 Резервне копіювання

Ціль: Підтримувати цілісність і доступність інформації та засобів оброблення інформації

Повинні бути розроблені стандартні процедури впровадження погодженої політики й стратегії резервного копіювання (див. також 14.1), щоб отримувати резервні копії даних і повторювати їх періодичне відновлення.

10.5.1 Резервне копіювання інформації

Контроль

Згідно з погодженою політикою резервного копіювання треба регулярно робити і тестувати резервні копії інформації та програмного забезпечення.

Настанова щодо впровадження

Повинні бути надані відповідні засоби резервного копіювання для забезпечення, що вся суттєва інформація і програмне забезпечення можуть бути відновлені після лиха або відмови носія.

Для резервного копіювання інформації треба розглянути наведені нижче елементи:

a) повинен бути визначений необхідний рівень резервного копіювання інформації;

b) повинні бути зроблені точні й повні записи щодо резервних копій і задокументовані процедури поновлення з резервних копій;

c) обсяг (наприклад, повне або диференційоване резервне копіювання) та частота резервних копіювань повинні відображати бізнес-вимоги організації, вимоги безпеки щодо залученої інформації та критичність інформації для безперервного функціонування організації;

d) резервні копії повинні зберігатися у віддаленому місці, на достатній відстані, щоб уникнути будь-якого ушкодження від лиха в основному приміщенні;

e) резервним копіям інформації треба надати належний рівень фізичного та інфраструктурного захисту (див. розділ 9), який не суперечить стандартам, що застосовуються в основному приміщенні, контролі, що застосовуються до носіїв в основному приміщенні, повинні поширюватися на місцеперебування резервних копій;

f) носії резервних копій повинні регулярно тестуватися, щоб забезпечити, що їм, за необхідності, можна довіряти у випадку аварійних дій;

g) процедури відновлення повинні регулярно перевірятися та тестуватися, щоб забезпечити, що вони ефективні і що вони можуть бути завершені у проміжок часу, виділений для відновлення операційними процедурами;

h) у ситуаціях, коли важливою є конфіденційність, резервні копії повинні бути захищені засобами шифрування.

Заходи резервного копіювання для окремих систем повинні регулярно тестуватися, для гарантування того, що вони задовольняють вимоги планів безперервності бізнесу (див. розділ 14). Для критичних систем заходи резервного

копіювання повинні охоплювати всю системну інформацію, прикладні програми та дані, необхідні для відновлення системи в цілому у випадку лиха.

Треба визначити період тривалого зберігання суттєвої бізнес-інформації, а також усі вимоги до архівних копій, які повинні постійно зберігатися (див. 15.1.3).

Національна примітка.

Для банків України вимоги до архівних копій та строків їх зберігання визначаються нормативно-правовими актами Національного банку України.

Додаткова інформація

Заходи резервного копіювання можуть бути автоматизовані для спрощення процесу резервного копіювання та поновлення з резервних копій. Такі автоматизовані рішення повинні ретельно тестуватися до впровадження та через певні проміжки часу.

10.6 Управління безпекою мережі

Ціль: Забезпечити захист інформації в мережах та захист інфраструктури, що їх підтримує.

Управління безпекою мереж, які можуть поширюватися за межі організації, потребує ретельного розгляду потоку даних, правових питань, моніторингу та захисту.

Додаткові контролі також можуть потребуватися для захисту чутливої інформації, яка проходить через загальнодоступні мережі.

10.6.1 Контролі мережі

Контроль

Треба відповідним чином управляти і контролювати мережі, щоб вони були захищеними від загроз і підтримувалася безпека систем та прикладних програм, які використовують мережу, охоплюючи інформацію, що передається.

Настанова щодо впровадження

Керівники мереж повинні впровадити контролі, щоб гарантувати безпеку інформації в мережах та захист підключених послуг від неавторизованого доступу. Зокрема, треба розглянути наведені нижче елементи:

a) відповідальність за функціонування мереж повинна бути, за можливості, відокремлена від функціонування комп'ютерів (див. 10.1.3);

b) повинні бути встановлені відповідальності та процедури управління віддаленим обладнанням, охоплюючи обладнання в користувацьких зонах;

c) треба розробити певні контролі для захисту конфіденційності та цілісності даних, що проходять через загальнодоступні мережі або через безпроводні мережі, та для захисту підключених систем і прикладних програм (див. 11.4 та 12.3); певні контролі можуть також бути необхідними для підтримання доступності послуг мережі та підключених комп'ютерів;

d) для уможливлення запису суттєвих для безпеки дій треба застосувати належні реєстрацію та моніторинг;

e) дії керівництва повинні бути ретельно скоординовані як для оптимізації обслуговування організації, так і для забезпечення того, що контролі несуперечливо застосовуються по всій інфраструктурі оброблення інформації.

Додаткова інформація

Додаткову інформацію щодо безпеки мережі можна знайти в ISO/IEC 18028, Information technology –Security techniques – IT network security.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ**.**
ISO/IEC 18028, Інформаційні технології - Методи безпеки - Безпека мережі ІТ.

10.6.2 Безпека послуг мережі

Контроль

Характеристики безпеки, рівні послуг, а також вимоги управління всіма послугами мережі повинні бути ідентифіковані і міститися у будь-якій угоді щодо послуг мережі, як для послуг, що надаються організацією, так і для аутсорсингових.

Настанова щодо впровадження

Треба визначити і регулярно здійснювати моніторинг здатності постачальника послуг мережі управляти погодженими послугами у безпечний спосіб, при цьому повинне бути погоджене право проведення аудиту.

Повинні бути ідентифіковані заходи безпеки, необхідні для окремих послуг, такі як характеристики безпеки, рівні обслуговування та вимоги щодо управління. Організація повинна забезпечити, що постачальники послуг мережі впровадили ці заходи.

Додаткова інформація

Послуги мережі охоплюють надання підключень, приватні послуги мережі та мережі з доданою вартістю, а також рішення щодо управління безпекою мережі, такі як міжмережеві екрани та системи виявлення вторгнення. Ці послуги можуть різнитися від простої смуги пропускання без управління до складних пропозицій з доданою вартістю.

Характеристиками безпеки послуг мережі можуть бути:

a) технології, застосовані для безпеки послуг мережі, такі як автентифікація, шифрування та контролі мережних підключень;

b) технічні параметри, потрібні для безпечного підключення до послуг мережі відповідно до правил безпеки та підключень мережі;

c) процедури використання послуг мережі для обмеження доступу до послуг мережі або прикладних програм, якщо це необхідно.

10.7 Поводження з носіями

Ціль*:* Запобігти неавторизованому розголошенню, модифікації, вилученню або знищенню активів та перериванню бізнес-діяльності.

Носії повинні бути контрольовані та фізично захищені.

Для захисту від неавторизованого розголошення, модифікації, видалення та знищення документів, комп'ютерних носіїв (наприклад, стрічок, дисків), вхідних/вихідних даних та системної документації повинні бути розроблені належні процедури функціонування.

10.7.1 Управління замінюваними носіями

Контроль

Повинні бути наявними процедури управління замінюваними носіями.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо управління замінюваними носіями:

a) інформація, якщо вона більше непотрібна, що міститься на будь-яких носіях багаторазового використання, які повинні бути видалені з організації, має бути зроблена невідновлюваною;

b) там, де необхідно і доцільно, повинна бути обов'язковою авторизація носіїв, які видаляються з організації, і записи про такі видалення повинні зберігатися для підтримки журналу аудиту;

c) усі носії повинні зберігатися в надійному, безпечному середовищі згідно з специфікаціями виробника;

d) збережена на носії інформація, яка повинна бути доступною довше за термін служби носія (згідно з специфікаціями виробника), повинна також зберігатися десь в іншому місці, щоб уникнути втрати інформації через псування носія;

Національна примітка.
Відповідно до нормативно-правових актів Національного банку України банки мають не рідше одного разу на рік перевіряти можливість читання архівних копій, які зберігаються на двох носіях різних типів і в разі необхідності відновлювати записи даних.

e) треба розглянути реєстрацію замінюваних носіїв для обмеження можливості втрати даних;

f) треба задіювати дисководи замінюваних носіїв лише тоді, коли для цього є бізнес-причина.

Усі процедури та рівні авторизованого доступу повинні бути чітко задокументовані.

Додаткова інформація

До замінюваних носіїв відносяться стрічки, диски, флеш диски, замінювані жорсткі диски, CD, DVD, а також друковані носії.

10.7.2 Вилучення носіїв

Контроль

Коли носії більше не потрібні, вони повинні безпечно і надійно вилучатися із застосуванням офіційно оформлених процедур.

Національна примітка.
Для усіх замінюваних носіїв інформації з грифом "банківська таємниця", повинні бути

використані процедури подвійного форматування або інші процедури, які унеможливлюють відновлення інформації, в тому числі для жорстких дисків комп'ютерів та серверів, в разі вилучення їх з промислової експлуатації або ремонту. В разі непрацездатності замінюваних носіїв інформації з грифом "банківська таємниця" вони підлягають фізичному руйнуванню.

Настанова щодо впровадження

Офіційні оформлені процедури безпечного вилучення носіїв повинні мінімізувати ризик витоку чутливої інформації до неавторизованих осіб. Процедури безпечного вилучення носіїв, які містять чутливу інформацію, повинні бути сумірними з чутливістю інформації. Треба розглянути наведені нижче елементи:

a) носії, що містять чутливу інформацію, повинні зберігатися та вилучатися безпечно і надійно, наприклад, шляхом спалення чи розрізання, або стирання даних перед використанням іншою прикладною програмою в організації;

b) повинні бути наявні процедури ідентифікації елементів, які можуть потребувати безпечного вилучення;

c) може бути легше вжити заходів щодо безпечного накопичення та вилучення усіх носіїв, ніж намагатися виділити чутливі елементи;

d) багато організацій пропонує послуги з накопичення та вилучення паперів, обладнання та носіїв; треба подбати про вибір придатного контрактора з відповідними контролями та досвідом;

e) вилучення чутливих елементів треба, по можливості, реєструвати для підтримки журналу аудиту.

При накопичуванні носіїв для вилучення треба розглянути ефект об'єднання, внаслідок якого велика кількість нечутливої інформації може стати чутливою.

Додаткова інформація

Чутлива інформація може бути розголошена через необережне вилучення носіїв (див. також 9.2.6 стосовно інформації щодо вилучення обладнання).

10.7.3 Процедури поводження з інформацією

Контроль

Для захисту інформації від неавторизованого розголошення або зловживання повинні бути розроблені процедури поводження з інформацією та її збереження.

Національна примітка.

Відповідно до нормативно-правових актів Національного банку України банки мають чітко визначити перелік інформації з грифом "банківська таємниця" та іншої конфіденційної інформації та впровадити внутрішні процедури поводження з такою інформацією.

Настанова щодо впровадження

Повинні бути розроблені процедури поводження, оброблення, збереження та доведення до відома інформації, які не суперечать її класифікації (див. 7.2). Треба розглянути наведені нижче елементи:

a) поводження з усіма носіями та їх позначення відповідно до зазначеного

рівня класифікації;

b) обмеження доступу для запобігання доступу неавторизованого персоналу;

c) підтримування офіційно оформленого реєстру авторизованих одержувачів даних;

d) забезпечення, що вхідні дані є повними, що оброблення завершено належним чином і застосовано підтвердження вихідних даних;

e) захист підкачаних даних, які очікують виведення, на рівні, що не суперечить їх чутливості;

f) зберігання носіїв відповідно до специфікацій виробника;

g) зведення поширення даних до мінімуму;

h) чітке маркування всіх копій носіїв до уваги авторизованого одержувача;

i) перегляд через регулярні інтервали списків розповсюдження та списків авторизованих одержувачів.

Додаткова інформація

Ці процедури застосовують до інформації у документах, комп'ютерних системах, мережах, при мобільному обчисленні, мобільних комунікаціях, у пошті, голосовій пошті, взагалі в мовних комунікаціях, мультимедіа, засобах поштового обслуговування, при використанні факсимільних апаратів та в будь-яких інших чутливих елементах, наприклад, бланкових чеках, рахунках-фактурах.

10.7.4 Безпека системної документації

Контроль

Системна документація повинна бути захищена від неавторизованого доступу.

Настанова щодо впровадження

Для убезпечення системної документації треба розглянути наведені нижче елементи:

a) системна документація повинна безпечно зберігатися;

b) список доступу до системної документації повинен бути зведений до мінімуму і затверджений власником прикладної програми;

c) системна документація, яка зберігається в загальнодоступній мережі або постачається через загальнодоступну мережу, повинна бути захищена належним чином.

Додаткова інформація

Системна документація повинна містити номенклатуру чутливої інформації, наприклад, описи процесів прикладних програм, процедури, структури даних, процеси авторизації.

10.8 Обмін інформацією

Ціль: Підтримувати безпеку інформації і програмного забезпечення, якими обмінюються в організації та з зовнішнім об'єктом.

Обмін інформацією і програмним забезпеченням між організаціями повинен базуватися на офіційно оформленій політиці обміну, виконуватися згідно з угодами щодо обміну і відповідати всьому застосовному законодавству (див. розділ 15).

Повинні бути розроблені процедури та стандарти для захисту інформації та фізичних носіїв, які містять інформацію під час передавання.

10.8.1 Політики та процедури обміну інформацією

Контроль

Повинні бути наявними офіційно оформлені політики, процедури та контролі обміну для захисту обміну інформацією з використанням всіх видів засобів комунікації.

Настанова щодо впровадження

Процедури та контролі, яких треба дотримуватися при використанні електронних засобів комунікації для обміну інформацією, повинні стосуватися наведених нижче елементів:

a) процедури, спроектовані для захисту обмінюваної інформації від перехоплення, копіювання, модифікації, неправильної маршрутизації та знищення;

b) процедури виявлення та захисту від зловмисного коду, який може бути переданий шляхом використання електронних комунікацій (див 10.4.1);

c) процедури захисту передаваної чутливої електронної інформації у формі приєднаних файлів;

d) політику або настанови, що визначають придатне використання електронних засобів комунікації (див. 7.1.3);

e) процедури використання безпроводної комунікації, беручи до уваги її особливі ризики;

f) відповідальності найманого персоналу, контракторів та будь-яких інших користувачів щодо неприпустимості компрометації організації, наприклад, через наклеп, кривдження, запозичення прав, переадресування ланцюгових листів, неавторизовані закупівлі тощо;

g) застосування криптографічних методів, наприклад, для захисту конфіденційності, цілісності та автентичності інформації (див. розділ 12.3);

h) настанови щодо тривалого зберігання та вилучення згідно з національними й місцевими законодавством та нормами всієї бізнес-кореспонденції, охоплюючи повідомлення;

i)неприпустимість залишення чутливої або критичної інформації на друкувальних засобах, наприклад, копіювальних пристроях, принтерах та факсимільних апаратах, оскільки до них може мати доступ неавторизований персонал;

j)контролі та обмеження пов’язані з переадресацією засобів комунікації, наприклад, автоматичне переадресування електронних повідомлень на зовнішні адреси пошти;

k) нагадування персоналу, що він повинен вжити належних запобіжних

заходів, наприклад, не розкривати чутливу інформацію, щоб уникнути при телефонній розмові підслуховування або перехоплення:

1) людьми у безпосередній близькості, особливо при користуванні мобільними телефонами;

2) прослуховуванням телефонних розмов та іншими формами підслуховування через фізичний доступ до телефонної слухавки або телефонної лінії, або при використанні скануючих приймачів;

3) людьми на стороні одержувача;

l)неприпустимість залишення на автовідповідачі повідомлень, які містять чутливу інформацію, оскільки вони можуть бути відтворені неавторизованими особами, зберігатися у спільних системах або зберігатися некоректно через неправильне набирання номера;

m) нагадування персоналу про проблеми використання факсимільних апаратів, а саме:

1) неавторизований доступ до вбудованої пам’яті для повідомлень з метою відновлення повідомлень;

2) навмисне або випадкове програмування апаратів для надсилання повідомлень на певні номери;

3) надсилання документів та повідомлень на неправильний номер або через неправильне набирання номера, або використання збереженого неправильного номера;

n) нагадування персоналу, щоб не записував демографічні дані, такі як адреса електронної пошти або інша персональна інформація, у будь-якому програмному забезпеченні, щоб уникнути їх збирання для неавторизованого використання;

o) нагадування персоналу, що сучасні факсимільні апарати та фотокопіювальні пристрої мають кеш-сторінки і зберігають сторінки, якщо сталася відмова через відсутність паперу чи при передачі, ці сторінки можуть бути надруковані після усунення відмови.

Крім того, персоналу треба нагадувати, що вони не повинні вести конфіденційні розмови у громадських місцях чи відкритих офісах, чи місцях для нарад, де стіни не є звуконепроникними.

Засоби обміну інформацією повинні узгоджуватися з усіма діючими правовими вимогами (див. розділ 15).

Додаткова інформація

Обмін інформацією може здійснюватися з використанням багатьох різних видів засобів комунікації, включаючи електронну пошту, голос, факсимільні апарати та відео.

Обмін програмним забезпеченням може здійснюватись через багато різних видів носіїв, включаючи завантаження з Інтернету та придбання у виробників, які продають серійні продукти.

Треба розглянути вимоги до контролів і наслідки - бізнесові, правові та щодо безпеки, пов’язані з електронним обміном даними, електронною комерцією та електронною комунікацією.

Інформація може бути скомпрометована внаслідок відсутності поінформованості, політики чи процедур щодо використання засобів обміну інформацією, наприклад, через підслуховування розмови по мобільному телефону у громадському місці, неправильне надсилання повідомлення електронною поштою, підслуховування автовідповідача, неавторизований доступ до систем набору номера голосової пошти або факсові повідомлення, випадково надіслані на помилкове факсимільне обладнання.

Функціонування бізнесу може порушуватися та інформація може бути скомпрометована в разі відмови, перевантаження або зупинки засобів комунікації (див. 10.3 та розділ 14). Інформація може бути скомпрометована в разі доступу неавторизованих користувачів (див. розділ 11).

10.8.2 Угоди щодо обміну

Контроль

Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо обміну інформацією та програмним забезпеченням.

Настанова щодо впровадження

Угоди щодо обміну повинні розглядати наведені нижче умови безпеки:

a) відповідальності керівництва з контролю та сповіщення щодо передавання, відсилання та приймання;

b) процедури сповіщення відправника щодо передавання, відсилання та приймання;

c) процедури забезпечення простежуваності та неспростовності;

d) мінімальні вимоги технічних стандартів щодо пакетування та передавання;

e) угоди щодо умовного депонування документів;

f) стандарти ідентифікації кур’єра;

g) відповідальності та зобов’язання у випадку інциденту інформаційної безпеки, наприклад, втрати даних;

h) використання погодженої системи позначень для чутливої або критичної інформації, яка забезпечує, що позначення є одразу ж зрозумілими і що інформація захищена належним чином;

i)право власності та відповідальності щодо захисту даних, авторського права, ліцензійної відповідності програмного забезпечення та інші подібні міркування (див. також 15.1.2 та 15.1.4);

j)технічні стандарти щодо записування та зчитування інформації та програмного забезпечення;

k) будь-які спеціальні контролі, які можуть знадобитися для захисту чутливих елементів, таких як криптографічні ключі (див. 12.3).

Для захисту інформації та фізичних носіїв в транзиті повинні бути розроблені і підтримуватися політика, процедури та стандарти (див. також 10.8.3), на них треба посилатися в угодах щодо обміну.

Зміст будь-якої угоди, який стосується безпеки, повинен відображати чутливість залученої бізнес-інформації..

Додаткова інформація

Угоди можуть бути електронні або складені вручну і можуть мати форму офіційно оформлених контрактів або умов найму. Стосовно чутливої інформації, особливі механізми, використовувані для обміну такою інформацією, повинні бути несуперечливими для всіх організацій та всіх типів угод.

10.8.3 Фізичні носії під час передавання

Контроль

Носії, що містять інформацію, повинні бути захищені від неавторизованого доступу, зловживання або руйнування під час транспортування поза фізичними межами організації.

Настанова щодо впровадження

Для захисту носіїв інформації, які передаються між різними місцями розташування організацій, треба розглянути наведені нижче настанови:

a) треба використовувати надійний засіб сполучення або кур'єрів;

b) перелік авторизованих кур'єрів повинен бути погоджений керівництвом;

c) повинні бути розроблені процедури перевірки ідентифікації кур'єрів;

d) упаковка повинна бути достатньою для захисту вмісту від будь-якого фізичного ушкодження, яке може виникнути протягом транзиту, і відповідати усім специфікаціям виробника (наприклад, щодо програмного забезпечення), наприклад, захисту від будь-яких факторів довкілля, які можуть знизити ефективність поновлення носія, таких як вплив підвищеної температури, вологості або електромагнітних полів;

e) за необхідності повинні бути погоджені контролі для захисту чутливої інформації від неавторизованого розголошення або модифікації; приклади охоплюють:

1) використання замкнених контейнерів;
2) доставляння ручним способом;
3) упаковку, яка надає докази розпакування (яка показує будь-яку спробу отримати доступ);
4) у надзвичайних випадках розподіл відправлення на більш ніж одну поставку та відсилання різними маршрутами.

Додаткова інформація

Інформація може бути вразливою до неавторизованого доступу, зловживання або руйнування під час фізичного транспортування, наприклад, при відсиланні носіїв поштою або кур'єром.

10.8.4 Електронний обмін повідомленнями

Контроль

Інформація, яка міститься в електронних повідомленнях, повинна бути захищена належним чином.

Настанова щодо впровадження

Міркування безпеки щодо електронного обміну повідомленнями повинні включати:

a) захист повідомлень від неавторизованого доступу, модифікації або відмови в обслуговуванні;

b) забезпечення коректного адресування та передавання повідомлення;

c) загальну надійність та доступність послуги;

d) правові вимоги, наприклад, вимоги до електронних підписів;

e) отримання погодження перед використанням загальнодоступних зовнішніх послуг, таких як засоби оперативного пересилання повідомлень або спільне використання файлів;

f) більш жорсткі рівні автентифікації, яка контролює доступ з загальнодоступних мереж.

Додаткова інформація

Електронний обмін повідомленнями, такий як електронна пошта, електронний обмін даними (*Electronic Data Interchange* - EDI) та засоби оперативного пересилання повідомлень, відіграють все більш важливу роль в бізнес-комунікаціях. Електронний обмін повідомленнями має інші ризики, ніж комунікації, основані на обміні паперами.

10.8.5 Системи бізнес-інформації

Контроль

Повинні бути розроблені і впроваджені політика і процедури захисту інформації, пов’язаної з взаємозв’язком систем бізнес-інформації.

Настанова щодо впровадження

Міркування щодо безпеки та наслідків для бізнесу взаємозв’язків таких засобів повинні включати:

a) відомі вразливості адміністративних та бухгалтерських систем, де інформація спільно використовується різними підрозділами організації;

b) вразливість інформації в комунікаційних системах бізнесу, наприклад, запис телефонних викликів або селекторних нарад, конфіденційність викликів, зберігання факсимільних повідомлень, відкривання поштової кореспонденції, поширення поштової кореспонденції;

c) політику та належні контролі для управління спільним використанням інформації;

d) вилучення категорій чутливої бізнес-інформації та класифікованих документів, якщо система не надає належного рівня захисту (див. 7.2);

e) обмеження доступу до інформації щоденників певних осіб, наприклад, персоналу, який працює з чутливими проектами;

f) категорії персоналу, контракторів або бізнес-партнерів, яким дозволено використовувати систему та місця, звідки може бути доступ до неї;

g) обмеження доступу до певного обладнання певними категоріями користувачів;

h) ідентифікація статусу користувачів, наприклад, найманого персоналу

організації або контракторів у довідниках для надання переваг над іншими користувачами;

i)збереження та резервне копіювання інформації, що міститься в системі (див. 10.5.1)

j)вимоги та заходи нейтралізації несправностей.

Додаткова інформація

Офісні інформаційні системи - це можливість швидкого поширення та спільного використання бізнес-інформації із використанням комбінації: документів, комп'ютерів, мобільних обчислень, мобільних комунікацій, пошти, голосової пошти, мовної комунікації взагалі, мультімедіа, поштових послуг/засобів та факсимільних апаратів.

10.9 Послуги електронної комерції

Ціль: Забезпечити захист послуг електронної комерції та їх безпечне використання.

Повинні бути розглянуті наслідки щодо безпеки, пов'язані з використанням послуг електронної комерції, охоплюючи інтерактивні трансакції та вимоги щодо контролів. Також повинні бути розглянуті цілісність та доступність інформації, опублікованої в електронному вигляді через загальнодоступні системи.

Національний відхил.

Цей розділ не використовується в банках України, оскільки вони не надають послуги електронної комерції.

10.9.1 Електронна комерція

Контроль

Інформація, залучена в електронну комерцію, яка проходить через загальнодоступні мережі, повинна бути захищена від шахрайської діяльності, контрактних суперечок і неавторизованого розголошення та модифікації.

Настанова щодо впровадження

Для електронної комерції міркування щодо безпеки повинні включати наведене нижче:

a) рівень конфіденційності, необхідний кожній стороні у кожній іншій заявленій тотожності, наприклад, через автентифікацію;

b) процес авторизації, пов'язаний з тим, хто може встановлювати ціни, видавати або підписувати основні торгові документи;

c) забезпечення, що торгові партнери повністю інформовані щодо свої авторизацій;

d) визначення вимог та відповідність їм щодо конфіденційності, цілісності, доказів відсилання та одержання основних документів, неспростовність контрактів, наприклад, пов'язаних з тендерами та контрактними процесами;

e) рівень довіри, обов'язковий для цілісності офіційно оголошених цін;

f) конфіденційність будь-яких чутливих даних або інформації;

g) конфіденційність та цілісність всіх замовлених трансакцій, платіжної

інформації, подробиць щодо адрес доставки та підтвердження одержань;

h) ступінь верифікації, який відповідає перевірки інформації платежу, наданої клієнтом;

i) вибір найбільш придатної розрахункової форми платежу для захисту від шахрайства;

j) рівень захисту, потрібний для підтримання конфіденційності та цілісності інформації щодо замовлень;

k) уникнення втрати або дублювання інформації трансакції;

l) зобов'язання, пов'язані з будь-якою недостовірною інформацією;

m) страхові вимоги.

Багато з викладених вище міркувань можна урахувати застосовуючи криптографічні контролі (див. 12.3), беручи до уваги відповідність правовим вимогам (див. 15.1, особливо 15.1.6 щодо криптографічного законодавства).

Заходи щодо електронної комерції між торговими партнерами повинні підтримуватися задокументованою угодою, яку укладають обидві сторони щодо погоджених умов торгівлі, охоплюючи подробиці щодо авторизації (див. b) вище). Можуть знадобитись інші угоди з постачальниками інформаційних послуг та мереж з доданою вартістю.

Відкриті торгові системи повинні опублікувати для клієнтів свої бізнес-умови.

Треба розглянути стійкість до атак хоста(ів), який використовують для електронної комерції та впливи на безпеку будь-яких мережних взаємозв'язків, необхідних для впровадження послуг електронної комерції (див. 11.4.6).

Додаткова інформація

Електронна комерція є вразливою до багатьох мережевих загроз, які можуть призвести до шахрайської діяльності, контрактних суперечок і розголошення або модифікації інформації.

Для зменшення ризиків електронна комерція може скористатися методом безпечної автентифікації, наприклад, використовуючи криптографію відкритих ключів та електронних підписів (див. також 12.3). Також там, де такі послуги потрібні, можна використовувати третю довірчу сторону.

10.9.2 Інтерактивні трансакції

Контроль

Інформація, залучена в інтерактивні трансакції, повинна бути захищена для запобігання неповній передачі, неправильній маршрутизації, неавторизованій зміні повідомлення, неавторизованому розголошенню, неавторизованому дублюванню повідомлення або його повторенню.

Настанова щодо впровадження

Міркування щодо безпеки для інтерактивних трансакцій повинні включати наведене нижче:

a) застосування електронних підписів кожною стороною, залученою в трансакцію;

b) усі аспекти трансакції, тобто, забезпечення того, що:
   1) посвідчення користувачів усіх сторін є дійсними та верифікованими;
   2) трансакція залишається конфіденційною; та
   3) зберігається приватність усіх залучених сторін;

c) комунікаційні канали між усіма залученими сторонами зашифровані;

d) убезпеченні протоколи, використовувані для комунікацій між всіма залученими сторонами;

e) забезпечення, що зберігання подробиць трансакції розміщене поза будь-якою загальнодоступною інфраструктурою, наприклад, на запам'ятовувальній платформі, яка існує у внутрішній (Intranet) мережі організації, та тривало не зберігається і не відображається на носії даних безпосередньо доступному з Інтернету;

f) там, де використовують довірчу повноважну організацію (наприклад, для випуску і підтримки цифрового підпису і/або цифрових сертифікатів), безпека є комплексною та вбудованою в єдиний з кінця-в кінець процес управління сертифікатом/підписом.

Додаткова інформація

Необхідно, щоб обсяг прийнятих контролів відповідав рівню ризику, пов'язаного з кожною формою інтерактивної трансакції.

Трансакції можуть потребувати відповідності законам, правилам та нормативам юрисдикцій, в яких трансакція створена, обробляється, закінчується та/або зберігається.

Існує багато форм трансакцій, які можуть виконуватися в інтерактивному режимі, наприклад, контрактні, фінансові тощо.

10.9.3 Загальнодоступна інформація

Контроль

Цілісність інформації, яка буде зроблена доступною у загальнодоступній системі, повинна бути захищена, щоб запобігти неавторизованій модифікації.

Настанова щодо впровадження

Програмне забезпечення, дані та інша інформація, яка потребує високого рівня цілісності, якщо вона робиться доступною через загальнодоступну систему, повинна бути захищена належними механізмами, наприклад, цифровими підписами (див. 12.3). Загальнодоступна система повинна тестуватися на наявність слабких місць та відмов до того, як інформація буде зроблена доступною.

До того, як інформація буде зроблена доступною, повинен бути виконаний офіційно оформлений процес затвердження. Крім того, всі вхідні дані, надані ззовні системи, повинні бути верифіковані та підтверджені.

Електронні системи публікування, особливо ті, що дозволяють зворотній зв'язок і пряме введення інформації, повинні бути ретельно контрольованими, щоб:

a) інформація отримувалася згідно з законодавством щодо захисту даних

(див. 15.1.4);

b) інформація, що входить і обробляється в системі публікування, повинна оброблятися повністю, точно та своєчасно;

c) чутлива інформація повинна захищатися під час збирання, оброблення та зберігання;

d) доступ до системи публікування не повинен дозволяти ненавмисний доступ до мереж, до яких система підключена.

Додаткова інформація

Інформація у загальнодоступній системі, наприклад, інформація на Веб-сервері, доступному через Інтернет, може потребувати відповідності законам, правилам та нормативам юрисдикцій, в яких система розміщена, де відбувається торгівля або де мешкає(ють) власник(и). Неавторизована модифікація опублікованої інформації може зашкодити репутації організації- публікатора.

10.10 Моніторинг

Ціль: Виявити неавторизовану діяльність з оброблення інформації.

Треба здійснювати моніторинг систем і реєструвати події інформаційної безпеки. Для забезпечення ідентифікації проблем інформаційної системи повинні використовуватися журнали реєстрації оператора і реєстрація несправностей.

Організація повинна задовольняти всі суттєві правові вимоги, застосовні до її діяльності з моніторингу та реєстрації.

Моніторинг системи повинен використовуватися для перевірки ефективності прийнятих контролів і для верифікації її відповідності моделі політики доступу.

10.10.1 Журнал аудиту

Контроль

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.

Настанова щодо впровадження

Журнали аудиту повинні включати, за потреби:

a) ID (ідентифікатор) користувача;

b) дати, час та подробиці основних подій, наприклад, входу в систему та виходу з неї;

c) ідентифікацію термінала або розміщення, за можливості;

d) записи успішних та відхилених спроб доступу до системи;

e) записи успішних та відхилених спроб доступу до даних та іншого ресурсу;

f) зміни конфігурації системи;

g) використання повноважень;

h) використання системних утиліт та прикладних програм;
i) файли, які були доступними, та вид доступу;
j) мережеві адреси та протоколи;
k) тривожні сигнали системи контролю доступу;
l) активацію та де-активацію систем захисту, таких як антивірусні системи та системи виявлення вторгнення.

Додаткова інформація

Журнали аудиту можуть містити інтрузивні (шпигунські) та конфіденційні персональні дані. Треба вжити належні заходи захисту приватності (див. 15.1.4). За можливості, системні адміністратори не повинні мати повноваження стирати або де-активувати журнали реєстрації власної діяльності (див. 10.1.3).

10.10.2 Моніторинг використання системи

Контроль

Повинні бути розроблені процедури моніторингу використання засобів оброблення інформації та результати моніторингу діяльності повинні регулярно переглядатися.

Настанова щодо впровадження

Рівень моніторингу, потрібний для окремих засобів, повинен визначатися оцінкою ризику. Організація повинна відповідати всім суттєвим правовим вимогам, застосовним до її діяльності з моніторингу. Сфери, які повинні бути розглянуті, охоплюють:

a) авторизований доступ, охоплюючи такі подробиці:
   1) ID користувача;
   2) дати та час основних подій;
   3) типи подій;
   4) файли, які були доступними;
   5) використані програми/утиліти;
b) усі привілейовані операції, такі як:
   1) використання привілейованих облікових записів, наприклад, супервізора, кореневого каталогу, адміністратора;
   2) запуск та зупинення системи;
   3) під’єднання/від’єднання пристроїв вводу/виводу;
c) спроби неавторизованого доступу, такі як:
   1) невдала або відхилена діяльність користувача;
   2) невдала або відхилена діяльність, що залучає данні та інші ресурси;
   3) порушення політики доступу та сповіщення для мережевих шлюзів та міжмережевих екранів;
   4) попередження від власних систем виявлення вторгнення;
d) системні попередження або відмови, такі як:
   1) попередження або повідомлення з пульта;
   2) особливі ситуації системного журналу;
   3) сигнали тривоги управління мережею;

4) сигнали тривоги системи контролю доступу;

e) зміни або спроби змінити установки та контролі безпеки системи.

Частота перегляду результатів діяльності з моніторингу повинна залежати від залучених ризиків. Фактори ризику, які треба розглянути, включають:

a) критичність прикладних процесів;

b) цінність, чутливість та критичність залученої інформації;

c) минулий досвід проникнення в систему та зловживання, частота використання вразливостей;

d) ступінь взаємозв'язаності систем (особливо загальнодоступних мереж);

e) де-активацію засобів реєстрації.

Додаткова інформація

Використання процедур моніторингу необхідне для забезпечення того, що користувачі виконують лише ту діяльність, яка була чітко авторизована (дозволена).

Перегляд журналу реєстрації призводить до розуміння загроз, на які наражається система, і способу, в який вони можуть виникнути. Приклади подій, які можуть вимагати подальшого розслідування у разі інцидентів інформаційної безпеки, наведені в 13.1.1.

10.10.3 Захист інформації журналів реєстрації

Контроль

Засоби реєстрування і інформація реєстрації повинні бути захищені від фальсифікації та неавторизованого доступу.

Настанова щодо впровадження

Ціллю контролів повинен бути захист від неавторизованих змін та проблем функціонування за допомогою засобів реєстрування, включаючи:

a) зміни типів записуваних повідомлень;

b) редагування та видалення файлів реєстрації;

c) перевищення місткості пам'яті носія файлів журналів реєстрації, яке призводить до відмови щодо записування подій або до перезаписування минулих записаних подій.

Може потребуватися архівування деяких журналів аудиту, якщо це є частиною політики тривалого збереження записів або вимогами збирання й тривалого зберігання доказів (див. також 13.2.3).

Додаткова інформація

Системний журнал часто містить великий обсяг інформації, більшість якої не стосується моніторингу безпеки. Щоб допомогти виділити значні для цілей моніторингу безпеки події треба розглянути автоматичне копіювання належних типів повідомлень у другий журнал реєстрації та/або використання придатних системних утиліт чи інструментів аудиту для виконання опитування файлу та вдосконалення.

Системні журнали потребують захисту, оскільки, якщо дані можуть бути модифіковані або дані в них знищені, їх існування може створити помилкове

розуміння безпеки.

10.10.4 Журнали реєстрації адміністратора та оператора

Контроль

Діяльність системного адміністратора та системного оператора повинна реєструватися.

Настанова щодо впровадження

Журнали реєстрації повинні містити:

a) час, коли відбулася подія (успіх чи відмова);

b) інформацію щодо події (наприклад, оброблені файли) або відмови (наприклад, помилку, що сталася, і вжиті коригувальні дії);

c) який обліковий запис та якого адміністратора чи оператора залучено;

d) які процеси було залучено.

Журнали реєстрації системного адміністратора та оператора повинні переглядатися на регулярній основі.

Додаткова інформація

Система виявлення вторгнення, якою управляють поза межами контролю системного адміністратора та адміністратора мережі, може використовуватися для моніторингу діяльності системного адміністратора та адміністратора мережі щодо їх відповідності.

10.10.5 Реєстрація несправностей

Контроль

Несправності треба реєструвати, аналізувати та вживати належні дії.

Настанова щодо впровадження

Несправності, про які повідомили користувачі або програми системи, пов’язані з обробленням інформації або комунікаційними системами, повинні бути зареєстровані. Повинні бути визначені чіткі правила поводження зі звітами щодо несправностей включаючи:

a) перегляд журналів реєстрації несправностей для забезпечення, що проблеми з несправностями задовільно розв’язано;

b) перегляд коригувальних заходів для забезпечення, що контролі не скомпрометовано і вжита дія є повністю авторизованою.

Треба забезпечити, щоб була задіяна реєстрація помилок, якщо ця функція системи доступна.

Додаткова інформація

Реєстрація помилок та несправностей може вплинути на продуктивність системи. Ця реєстрація повинна задіюватися компетентним персоналом і рівень реєстрації, потрібний для окремих систем, повинен визначатися оцінкою ризику, беручи до уваги погіршення показників продуктивності.

10.10.6 Синхронізація годинників

Контроль

Годинники всіх суттєвих систем оброблення інформації в організації або домені безпеки повинні бути синхронізовані з джерелом часу погодженої точності.

Настанова щодо впровадження

Якщо комп'ютер або пристрій зв'язку має можливість оперувати годинником істинного часу, цей годинник повинен бути встановлений згідно з погодженим стандартом, наприклад, Загальний скоординований час (Coordinated Universal TIME - UTC) або місцевий стандартний час. Оскільки відомо, що деякі годинники з часом мають відхилення, повинна бути процедура, яка перевіряє й коригує будь-яке значне відхилення.

Для забезпечення того, що позначка часу відображує справжню дату/час, важливою є коректна інтерпретація формату дати/часу. Треба взяти до уваги місцеві особливості (наприклад, перехід на літній час).

Національна примітка.

Банки мають здійснити синхронізацію часу з погодженим стандартом для забезпечення коректної роботи у системах реального часу та забезпечення надання послуг електронного цифрового підпису центрами сертифікації ключів банків.

Додаткова інформація

Правильна установка комп'ютерного годинника важлива для забезпечення точності журналів аудиту, необхідних для розслідування або як доказ в правових або дисциплінарних випадках. Неточні журнали аудитів можуть заважати таким розслідуванням і підірвати довіру до такого доказу. Годинник, зв'язаний з широкомовним розсиланням радіо-часу від національного атомного годинника, може використовуватись як еталонний годинник для систем реєстрації. Часовий мережевий протокол може використовуватися для утримування всіх серверів у режимі синхронізації із еталонним годинником.

11 Контроль доступу

11.1 Бізнес вимоги до контролю доступу

Ціль: Контролювати доступ до інформації.

Доступ до інформації, засобів оброблення інформації та бізнес-процесів повинен контролюватися на основі вимог бізнесу і безпеки.

Правила контролю доступу повинні брати до уваги політику щодо поширення інформації та авторизації.

11.1.1 Політика контролю доступу

Контроль

Політика контролю доступу повинна бути розроблена, задокументована та переглядатися на основі вимог бізнесу та безпеки щодо доступу.

Настанова щодо впровадження

Правила контролю доступу та права кожного користувача чи групи користувачів повинні бути чітко встановлені в політиці контролю доступу. Контролі доступу є як логічними, так і фізичними (див. також розділ 9), і їх треба розглядати разом. Користувачам та постачальникам послуг треба надати чітке положення щодо бізнес-вимог, які повинні задовольняти контролі доступу.

Політика повинна брати до уваги наведене нижче:

a) вимоги безпеки окремих прикладних програм бізнесу;

b) ідентифікацію всієї інформації стосовно прикладних програм бізнесу та ризиків, на які наражається інформація;

c) політику щодо поширення інформації та авторизації, наприклад, потребу знати принципи та рівні безпеки і класифікацію інформації (див. 7.2);

d) несуперечливість контролю доступу та політики класифікації інформації різних систем та мереж;

e) відповідне законодавство й будь-які контрактні зобов’язання стосовно захисту доступу до даних чи послуг (див. 15.1);

f) стандартні профілі доступу користувача для звичайних посадових ролей в організації;

g) управління правами доступу в розподіленій і об’єднаній в мережу інфраструктурі, яка розпізнає усі типи доступних підключень;

h) відокремлення ролей контролю доступу, наприклад, запит доступу, авторизація, адміністрування доступу;

i) вимоги щодо офіційного оформлення авторизації запитів доступу (див. 11.2.1);

j) вимоги щодо періодичного перегляду контролів доступу; (див. 11.2.4);

k) видалення прав доступу (див. 8.3.3).

Додаткова інформація

При визначенні правил контролю доступу треба приділити увагу:

a) розрізненню правил, до виконання яких примушують завжди, і

настанов, які є необов'язковими або залежать від умов;

b) встановленню правил, основаних на передумові „Все взагалі заборонено, доки явно не дозволено", а не на слабкішому правилі „Все взагалі дозволено, доки явно не заборонено";

c) зміні інформаційних позначок (див. 7.2), які створюються автоматично засобами оброблення інформації, й тих, які створюються на розсуд користувача;

d) зміні дозволів для користувачів, які створюються автоматично інформаційною системою, й тих, що створюються адміністратором;

e) правилам, які потребують спеціального затвердження до введення в дію, й тих, що його не потребують.

Правила контролю доступу повинні підтримуватися офіційно оформленими процедурами та чітко визначеними відповідальностями (див., наприклад, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Управління доступом користувача

Ціль: Забезпечити авторизований доступ користувача і запобігти неавторизованому доступу до інформаційних систем.

Повинні бути наявними офіційно оформлені процедури контролю призначення прав доступу до інформаційних систем та послуг.

Процедури повинні охоплювати всі етапи життєвого циклу доступу користувача від первинної реєстрації нових користувачів до кінцевого зняття з реєстрації користувачів, яким більше не потрібний доступ до інформаційних систем та послуг. За потреби, особливу увагу треба приділити необхідності контролю призначення привілейованих прав доступу, які дозволяють користувачам скасовувати контролі системи.

11.2.1 Реєстрація користувача

Контроль

Для надання та відміни доступу до всіх інформаційних систем і послуг повинні бути наявними офіційно оформлені процедури реєстрації та зняття з реєстрації.

Настанова щодо впровадження

Процедура контролю доступу для реєстрації та зняття з реєстрації користувача повинна включати:

a) використання унікальних ідентифікаторів (IDs), які дають змогу користувачам підключатися і нести відповідальність за свої дії; використання групових ідентифікаторів (IDs) повинне бути затвердженим і задокументованим та повинно дозволятися тільки там, де це необхідно з причин, обумовлених бізнесом або функціонуванням;

b) перевірку, що користувача авторизовано власником системи на використання інформаційної системи чи послуги; може бути припустимим окреме затвердження керівництвом прав доступу;

c) перевірку, що рівень наданого доступу відповідає бізнес-цілям (див.

11.1) і не суперечить політиці безпеки організації, наприклад, він не компрометує розподіл обов'язків (див. 10.1.3);

d) надання користувачам письмового положення щодо їх прав доступу;

e) вимогу підписання користувачами положення, яке визначає, що вони розуміють умови доступу;

f) забезпечення, що постачальники послуг не надають доступ до завершення процедур авторизації;

g) підтримка офіційно оформленого запису щодо всіх осіб, зареєстрованих для користування послугою;

h) негайне видалення або блокування прав доступу користувачів, які змінили ролі чи посади або залишили організацію;

i)періодичну перевірку, видалення або блокування зайвих ідентифікаторів (IDs) користувача та облікових записів (див. 11.2.4);

j)забезпечення, що зайві ідентифікатори (IDs) користувача не надаються іншим користувачам.

Додаткова інформація

Треба розглянути встановлення ролей користувача щодо доступу, основаних на бізнес-вимогах, які підсумовують численні права доступу в типові профілі доступу користувачів. На рівні таких ролей запитами доступу й переглядами (див. 11.2.4) легше управляти, ніж на рівні окремих прав.

Треба розглянути розміщення в контрактах персоналу й договорах розділів, які визначають санкції щодо спроб неавторизованого доступу з боку персоналу або агентів послуг (див. також 6.1.5, 8.1.3 та 8.2.3).

11.2.2 Управління повноваженнями

Контроль

Призначення та використання повноважень повинно бути обмеженим та контрольованим.

Настанова щодо впровадження

Призначення повноважень в багатокористувацьких системах, які потребують захисту від неавторизованого доступу, повинне контролюватися за офіційно оформленим процесом авторизації. Треба розглянути наведені нижче кроки:

a) повинні бути ідентифіковані повноваження доступу, пов'язані з кожним продуктом системи, наприклад, операційною системою, системою управління базою даних та кожною прикладною програмою, і користувачі, для яких вони повинні бути призначені;

b) основою для призначення повноважень користувачам повинні бути необхідність використання (потребує-використання) і події (від-події-до-події) згідно з політикою контролю доступу (див. 11.1.1), тобто повноваження призначаються на рівні мінімальних вимог, яких потребує їх функціональна роль, та лише за потреби;

c) повинні підтримуватися процес авторизації та реєстрація всіх

призначених повноважень. Повноваження не повинні надаватися до завершення процесу авторизації;

d) треба сприяти розвитку та використанню системних підпрограм, щоб уникнути необхідності надання користувачам повноважень;

e) треба сприяти розвитку та використанню програм, які не потребують повноважень для запуску;

f) повноваження повинні призначатися ідентифікаторам (IDs) користувача, які відрізняються від тих, що використовують у бізнесі зазвичай.

Додаткова інформація

Невідповідне використання повноважень адміністрування системи (будь-яка властивість або засіб інформаційної системи, які дозволяють користувачеві скасувати системні чи прикладні контролі) може бути головним чинником відмов або порушень систем.

11.2.3 Управління паролем користувача

Контроль

Призначення паролів повинне бути контрольованим за допомогою офіційно оформленого процесу управління.

Настанова щодо впровадження

Процедура повинна містити наведені нижче вимоги:

a) від користувачів треба вимагати підписання положення щодо конфіденційного зберігання особистих паролів і зберігання групових паролів виключно серед членів групи; це підписане положення можна розмістити у термінах та умовах найму (див. 8.1.3);

b) якщо від користувачів вимагають підтримки їх власних паролів, їм треба спочатку надати безпечний тимчасовий пароль (див. 11.3.1), який їх примушують негайно замінити;

c) встановлення процедур верифікації особи користувача до надання нового, заміненого або тимчасового пароля;

d) тимчасові паролі повинні надаватися користувачам у безпечний спосіб; треба уникати залучення третіх сторін або використання незахищених (відкритий текст) повідомлень електронної пошти;

e) тимчасові паролі повинні бути унікальними для особи і не повинні бути такими, про які можна здогадатися;

f) користувачі повинні підтвердити отримання пароля;

g) паролі не повинні ніколи зберігатися в комп’ютерній системі у незахищеному вигляді;

h) використовувані за замовчанням паролі постачальника повинні бути змінені після інсталяції систем або програмного забезпечення.

Додаткова інформація

Паролі є звичайними засобами верифікації особи користувача до надання доступу до інформаційної системи або послуги згідно з авторизацією

користувача. Інші методи ідентифікації та автентифікації користувача, такі як біометрія, наприклад, верифікація відбитку пальця, верифікація підпису та використання апаратних токенів, наприклад, смарт-карток, можливе і повинне розглядатися за потреби.

Національна примітка.

Банкам рекомендується для систем, які обробляють інформацію з грифом "банківська таємниця" використовувати автентифікацію користувачів з використанням апаратних токенів або суворої автентифікації з використанням криптографічних ключів, які зберігаються на апаратних носіях.

11.2.4 Перегляд прав доступу користувача

Контроль

Керівництво повинне переглядати права доступу користувача у встановлені терміни, використовуючи офіційно оформлену процедуру.

Настанова щодо впровадження

Перегляд прав доступу повинен брати до уваги наведені нижче настанови:

a) права доступу користувача повинні переглядатися через суворо дотримувані інтервали часу, наприклад, з періодом 6 місяців, і після будь-яких змін, таких як підвищення або зниження по службі або припинення найму (див. 11.2.1);

b) права доступу користувача повинні переглядатися та перепризначатися при переході з однієї посади на іншу в межах тієї ж організації;

c) авторизація певних привілейованих прав доступу (див. 11.2.2) повинна переглядатися через частіші інтервали, наприклад з періодом 3 місяці;

d) призначення повноважень повинне перевірятися через суворо дотримувані інтервали часу, щоб забезпечити, що не було отримано неавторизовані привілеї;

e) зміни до привілейованих облікових записів повинні реєструватися для періодичного перегляду.

Додаткова інформація

Необхідно регулярно переглядати права доступу користувача для підтримки ефективного контролю доступу до даних та інформаційних послуг.

11.3 Відповідальності користувача

Ціль: Запобігти неавторизованому доступу користувача і компрометації або викраденню інформації та засобів оброблення інформації.

Для ефективної безпеки суттєвою є співпраця авторизованих користувачів.

Користувачі повинні бути поінформовані щодо своїх відповідальностей для підтримки ефективних контролів доступу, особливо тих, що стосуються використання паролів та безпеки обладнання користувача.

Для зниження ризику неавторизованого доступу або ушкодження паперів, носіїв та засобів оброблення інформації треба впровадити політику чистого стола та чистого екрана.

11.3.1 Використання паролів

Контроль

Треба вимагати від користувачів додержання визнаних практик безпеки у виборі та використанні паролів.

Настанова щодо впровадження

Усіх користувачів треба сповістити щодо:

a) збереження конфіденційності паролів;

b) уникнення зберігання запису паролів (наприклад, на папері, у файлі програмного забезпечення або у портативному пристрої) доти, доки вони не будуть зберігатися безпечно і спосіб збереження не буде затверджений;

c) зміни паролів кожного разу, коли є якась ознака можливої компрометації системи або пароля;

d) вибору якісних паролів з обґрунтовано мінімальною довжиною, які:

1) легкі для запам’ятовування;

2) не базуються на чомусь, про що будь-хто інший може легко здогадатися або отримати, використовуючи особисту інформацію, наприклад, імена, телефонні номери, дати народження тощо;

3) не уразливі до словникових атак (тобто не складаються з слів, що містяться в словниках);

4) не мають послідовності однакових тільки цифрових або тільки абеткових символів;

e) зміни паролів через суворо дотримувані інтервали часу або на підставі кількості доступів (паролі для привілейованих облікових записів повинні змінюватись частіше, ніж звичайні паролі) та уникнення повторного використання або циклічного використання старих паролів;

f) зміни тимчасових паролів при першій реєстрації;

g) не включення паролів у будь-які автоматизовані процеси реєстрації, наприклад, збережені за допомогою макроса або функціональної клавіші;

h) спільно не використовувати індивідуальні паролі користувача;

i) не використовувати той самий пароль для бізнес і не бізнес цілей.

Якщо користувачам потрібний доступ до колективних послуг, систем або платформ, і вимагається підтримка різних окремих паролів, їм треба рекомендувати, щоб вони використовували єдиний якісний пароль (див. d) вище) для всіх послуг, щодо яких користувач впевнений, що для збереження цього пароля в кожній послузі, системі чи платформі встановлено належний рівень захисту.

Додаткова інформація

Управління системою служби допомоги, яка має справу із загубленими або забутими паролями, потребує особливої обережності, оскільки це може також бути засобом атаки на систему паролів.

11.3.2 Обладнання користувачів, залишене без нагляду

Контроль

Користувачі повинні забезпечити, що залишене без нагляду обладнання, належним чином захищене.

Настанова щодо впровадження

Усі користувачі повинні бути поінформовані щодо вимог безпеки та процедур захисту залишеного без нагляду обладнання та їх відповідальності за впровадження такого захисту. Користувачам треба рекомендувати:

a) припиняти активні сеанси по закінченні, доки вони не будуть убезпеченні відповідним блокувальним механізмом, наприклад, екранною заставкою, захищеною паролем;

b) завершати роботу головного комп'ютера, серверів та офісних персональних комп'ютерів по закінченні сеансу (тобто не лише вимкнути екран ПК або термінал);

c) персональні комп'ютери або термінали, коли їх не використовують, убезпечувати від неавторизованого використання блокуванням клавіатури або еквівалентним контролем, наприклад, парольним доступом (див. також 11.3.3).

Додаткова інформація

Обладнання, встановлене в користувацьких зонах, наприклад, робочі станції або файлові сервери, може потребувати спеціального захисту від неавторизованого доступу, якщо воно залишається без нагляду на досить тривалий час.

11.3.3 Політика чистого стола та чистого екрана

Контроль

Повинні бути ухвалені політика чистого стола щодо паперів і замінюваних носіїв пам'яті та політика чистого екрану щодо засобів оброблення інформації

Настанова щодо впровадження

Політика чистого стола та чистого екрана повинна брати до уваги класифікацію інформації (див. 7.2), правові та контрактні вимоги (див. 15.1) та відповідні ризики і культурні аспекти організації. Треба розглянути наведені нижче настанови:

a) носії чутливої або критичної інформації, наприклад, папери або на замінювані носії пам'яті, повинні бути замкнені (краще, якщо в сейфі, шафі або інших видах захищених меблів), якщо вони не потрібні, особливо коли залишають офіс пустим;

b) залишати без нагляду комп'ютери й термінали треба завершивши сеанс або захистивши екран і клавіатуру механізмом блокування, який контролюється паролем, токеном або подібним механізмом автентифікації користувача, коли комп'ютери й термінали не використовуються, вони повинні бути захищені блокуванням клавіатури, паролями або іншими контролями;

c) точки отримання та відправлення пошти та залишені без нагляду

факсимільні апарати повинні бути захищені;

d) треба запобігати неавторизованому використанню фотокопіювальної та іншої розмножувальної техніки (наприклад, сканерів, цифрових камер);

e) документи, що містять чутливу або класифіковану інформацію, повинні видалятися з принтерів негайно.

Додаткова інформація

Політика чистого стола/чистого екрана знижує ризики неавторизованого доступу, втрати або ушкодження інформації протягом та після звичайного робочого часу. Сейфи та інші види засобів безпечного зберігання можуть також захищати інформацію, що в них зберігається, від таких лих, як пожежа, землетрус, повінь або вибух.

Розгляньте використання принтерів з функцією пін-коду, тоді лише ініціатори друку зможуть отримати віддруковані матеріали і лише перебуваючи поруч з принтером.

11.4 Контроль доступу до мережі

Ціль: Запобігти неавторизованому доступу до послуг мережі.

Доступ як до внутрішніх, так і до зовнішніх послуг мережі повинен бути контрольованим.

Доступ користувача до мережі та мережевих послуг не повинен компрометувати безпеку мережевих послуг, забезпечивши:

a) наявність відповідних інтерфейсів між мережею організації та мережами, якими володіють інші організації, і загальнодоступними мережами;

b) застосування відповідних механізмів автентифікації користувачів та обладнання;

c) примусовий контроль доступу користувача до інформаційних послуг.

11.4.1 Політика використання послуг мережі

Контроль

Користувачам повинен надаватися доступ тільки до послуг, на використання яких вони були авторизовані.

Настанова щодо впровадження

Повинна бути сформульована політика стосовно використання мереж і послуг мережі. Ця політика повинна охоплювати:

a) мережі та послуги мережі, до яких дозволено доступ;

b) процедури авторизації для визначення, кому дозволено доступ і до яких мереж та мережевих послуг;

c) контролі управління та процедури захисту доступу до мережевих підключень та послуг мережі;

d) засоби, використовувані для доступу до мереж та послуг мережі (наприклад, умови дозволу доступу по телефонних лініях до послуг Інтернет-провайдера або віддаленої системи).

Політика користування послугами мережі не повинна суперечити політиці контролю бізнес-доступу (див. 11.1).

Додаткова інформація

Неавторизовані та незахищені підключення до послуг мережі можуть зашкодити всій організації. Такий контроль є особливо важливим для мережевих підключень до чутливих або критичних прикладних програм бізнесу або до користувачів, розташованих у місцях високого ризику, наприклад загальнодоступних чи зовнішніх зонах, що знаходяться поза межами управління та контролю безпеки організації.

11.4.2 Автентифікація користувача у зовнішніх підключеннях

Контроль

Для контролю доступу віддалених користувачів повинні використовуватися відповідні методи автентифікації.

Настанова щодо впровадження

Віддалені користувачі можуть бути автентифіковані з використанням, наприклад, методів основаних на криптографії, апаратних токенах або протоколі виклик/відповідь. Можливе впровадження таких методів можна знайти у різних рішеннях для приватних віртуальних мереж (VPN). Для забезпечення впевненості у джерелі підключення можуть також використовуватися виділені приватні лінії.

Процедури і контролі зворотного виклику, наприклад, використання модемів зворотного виклику, можуть забезпечити захист від неавторизованих та небажаних підключень до засобів оброблення інформації організації. Цей вид контролю автентифікує користувачів, які намагаються встановити віддалене підключення до мережі організації. При використанні такого контролю організація не повинна використовувати послуги мережі, які включають переадресування виклику, або, якщо використовує, вони (послуги) повинні унеможливлювати використання таких властивостей, щоб уникнути слабких місць, пов’язаних з переадресуванням виклику. Процес зворотного виклику повинен забезпечити, що зі сторони організації відбувалося фактичне роз’єднання. Інакше віддалений користувач може тримати лінію відкритою симулюючи, що верифікація зворотного виклику відбулася. Процедури та контролі зворотного виклику повинні ретельно тестуватися стосовно такої можливості.

Автентифікація вузла може слугувати альтернативним засобом автентифікації груп віддалених користувачів, якщо вони підключені до безпечного, спільно використовуваного комп’ютерного засобу. Для автентифікації вузла можуть використовуватися криптографічні методи, наприклад, основані на сертифікаті комп’ютера. Це є частиною деяких рішень, основаних на VPN.

Додаткові контролі автентифікації повинні бути впроваджені для контролю доступу у безпроводних мережах. Зокрема, особливої обережності потребує вибір контролів для безпроводних мереж через більші можливості невиявленого

перехоплення та включення у мережевий трафік.

Додаткова інформація

Зовнішні підключення надають потенційну можливість неавторизованого доступу до бізнес-інформації, наприклад, доступу методами зворотного виклику. Є різні види методів автентифікації, деякі з них надають більш високий рівень захисту ніж інші, наприклад, методи основані на використанні криптографічних методів, можуть забезпечити надійну автентифікацію. З оцінки ризику важливо визначити потрібний рівень захисту. Це необхідно для належного вибору методу автентифікації.

Засоби автоматичного підключення до віддаленого комп'ютера можуть надати шлях для неавторизованого отримання доступу до прикладних програм бізнесе. Це особливо важливо, якщо підключення використовує мережу, яка перебуває поза контролем управління безпекою організації.

11.4.3 Ідентифікація обладнання в мережах

Контроль

Автоматична ідентифікація обладнання повинна розглядатися як засіб автентифікації підключень з певного місця та певного обладнання.

Настанова щодо впровадження

Ідентифікація обладнання може використовуватись, якщо важливо, щоб підключення могло ініціюватися з певного місця або обладнання. Ідентифікатор у обладнанні або закріплений за ним може застосовуватися для позначення, чи дозволено підключати це обладнання до мережі. Якщо існує більше ніж одна мережа і, особливо, якщо ці мережі мають різну чутливість, такі ідентифікатори повинні чітко позначати, до якої мережі дозволено підключати обладнання. Для підтримки безпеки ідентифікатора обладнання може бути необхідно розглянути фізичний захист обладнання.

Додаткова інформація

Цей контроль може бути доповнений іншими методами автентифікації користувача обладнання (див. 11.4.2). Додатково до автентифікації користувача може застосовуватися ідентифікація обладнання.

11.4.4 Захист порту віддаленої діагностики та конфігурування

Контроль

Фізичний і логічний доступ до портів віддаленої діагностики та конфігурування повинен бути контрольований.

Настанова щодо впровадження

Можливі контролі доступу до портів діагностики та конфігурування включають використання блокування клавіатури і процедури підтримки для контролю фізичного доступу до порту. Прикладом такої процедури підтримки є забезпечення того, що порти діагностики та конфігурування доступні лише за домовленістю між керівником комп'ютерної служби та персоналом підтримки

апаратних засобів/програмного забезпечення, які потребують доступу.

Порти, послуги та аналогічні засоби інстальовані на комп'ютерних або мережевих засобах, які безпосередньо не потрібні для бізнес-діяльності, повинні бути недоступними або видаленими.

Додаткова інформація

Багато комп'ютерних систем, мережевих систем та комунікаційних систем інсталюється із дистанційними засобами діагностики та конфігурування для використання їх інженерами з обслуговування. Якщо вони не захищені, ці порти діагностики надають можливість неавторизованого доступу.

11.4.5 Сегментація у мережах

Контроль

У мережі повинні бути сегментовані групи інформаційних послуг, користувачів, а також інформаційні системи.

Настанова щодо впровадження

Одним з методів контролю безпеки великих мереж є розділення їх на окремі логічні мережеві домени, наприклад, внутрішній мережевий домен організації та зовнішній мережевий домен, кожен з яких захищений визначеним периметром безпеки. У різних логічних доменах мережі може бути застосований диференційований набір контролів для подальшої сегментації безпечної інфраструктури мережі, наприклад, загальнодоступних систем, внутрішніх мереж та критичних активів. Домени повинні визначатися на основі оцінки ризику та різних вимог безпеки у межах кожного домену.

Для контролю доступу та інформаційного потоку між двома доменами такий периметр мережі може бути впроваджений шляхом інсталяції шлюзу безпеки між двома мережами, які повинні бути з'єднані. Цей шлюз повинен бути конфігурований для фільтрування трафіку між цими доменами (див. 11.4.6 та 11.4.7) і для блокування неавторизованого доступу відповідно до політики контролю доступу організації (див. 11.1). Прикладом цього типу шлюзу є те, що зазвичай згадується як міжмережевий екран. Іншим способом сегментації на окремі логічні домени є обмеження доступу до мережі шляхом застосування віртуальних приватних мереж для груп користувачів у межах організації.

Мережі також можуть бути сегментовані з використанням функціональності мережевого пристрою, наприклад, IP комутації. Окремі домени можуть потім запроваджуватися контролюванням мережевого потоку даних з використанням можливостей маршрутизації/комутації, таких як списки контролю доступу.

Критерії для сегментації мереж у домени повинні базуватися на політиці контролю доступу та вимогах доступу (див. 10.1), а також брати до уваги відносну вартість і вплив продуктивності вбудовування придатної мережної маршрутизації або технології шлюзів (див. 11.4.6 та 11.4.7).

Крім того, з метою зниження загального впливу порушення обслуговування сегментація мереж повинна базуватися на цінності та класифікації інформації, яка зберігається або обробляється в мережі, рівнях довіри або бізнес-спеціалізації.

Треба приділити увагу сегментації безпроводних мереж з внутрішніх та приватних мереж. Оскільки периметри безпроводових мереж не є добре визначеними, в таких випадках повинна бути виконана оцінка ризику для ідентифікації контролів (наприклад, жорстка автентифікація, криптографічні методи і вибір частоти) для підтримки сегментації мережі.

Додаткова інформація

Мережі все більше розширюються за межі традиційних границь організації, оскільки формуються бізнес-спільноти, які можуть вимагати з'єднання або спільного використання засобів оброблення інформації та обслуговування мережі. Таке розширення може збільшити ризик неавторизованого доступу до існуючих інформаційних систем, які користуються мережею, причому деякі з них можуть вимагати захисту від користувачів іншої мережі через свою чутливість або критичність.

11.4.6 Контроль підключень до мережі

Контроль

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)

Настанова щодо впровадження

Права доступу користувачів до мережі повинні підтримуватися та оновлюватися згідно з вимогами політики контролю доступу (див. 11.1.1).

Спроможність до підключення користувачів може обмежуватися мережевими шлюзами, які фільтрують трафік за допомогою заздалегідь визначених таблиць або правил. Прикладами прикладних програм, до яких повинні застосовуватися обмеження, є:

a) обмін повідомленнями, наприклад, електронна пошта;
b) передавання файлів;
c) інтерактивний доступ;
d) доступ до прикладних програм.

Треба розглянути співвідношення між правом доступу до мережі з певним часом дня або датами.

Додаткова інформація

Для мереж спільного використання, особливо тих, що поширюються за межі організації, політика контролю доступу може вимагати вбудовування контролів для обмеження спроможності користувачів до підключення.

11.4.7 Контроль маршрутизації в мережі

Контроль

Для мереж повинні бути впроваджені контролі маршрутизації, щоб забезпечити, що підключення комп'ютерів і потоки інформації не порушують

політику контролю доступу прикладних програм бізнесу.

Настанова щодо впровадження

Контролі маршрутизації повинні базуватися на механізмі позитивної перевірки адрес джерела та призначення.

Для підтвердження адрес джерела та призначення у внутрішніх та зовнішніх контрольних точках мережі можуть застосовуватися шлюзи безпеки, якщо використовуються технології прокси-серверів та/або трансляції мережевої адреси. Персонал, який займається впровадженням, повинен бути поінформованим щодо стійкості та недоліків будь-яких застосованих механізмів. Вимоги до контролю маршрутизації в мережі повинні базуватися на політиці контролю доступу (див. 11.1).

Додаткова інформація

Мережі спільного використання, особливо ті, що поширюються за межі організації, можуть потребувати додаткових контролів маршрутизації. Це особливо стосується мереж спільно використовуваних з користувачами третьої сторони (що не належать до організації).

11.5 Контроль доступу до операційної системи

Ціль: Запобігти неавторизованому доступу до операційних систем.

Треба використовувати засоби безпеки для обмеження доступу уповноважених користувачів до операційних систем. Ці засоби повинні допускати таке:

a) автентифікацію авторизованих користувачів відповідно до визначеної політики контролю доступу;
b) реєстрацію успішних та невдалих системних спроб автентифікації;
c) реєстрацію використання певних системних повноважень;
d) видання сигналу тривоги при порушенні політики безпеки системи;
e) надання належних засобів автентифікації;
f) за необхідності, обмеження часу підключення користувачів.

11.5.1 Процедури безпечної реєстрації

Контроль

Доступ до операційної системи повинен контролюватися процедурою безпечної реєстрації.

Настанова щодо впровадження

Процедура реєстрації в операційної системі повинна бути спроектована так, щоб звести до мінімуму можливість неавторизованого доступу. Тому процедура реєстрації повинна розкривати мінімум інформації щодо системи, щоб уникнути надання неавторизованому користувачу непотрібної допомоги. Надійна процедура реєстрації повинна:

a) не виводити на екран ідентифікатори системи або прикладної програми до успішного завершення процесу реєстрації;

b) виводити на екран загальне попередження, що комп'ютер буде доступним тільки авторизованому користувачу;

c) не надавати протягом процедури реєстрації допоміжних повідомлень, які б сприяли неавторизованому користувачу;

d) підтверджувати інформацію реєстрації лише після завершення вводу всіх даних. При виникненні помилки система не повинна показувати, яка частина даних є коректною або некоректною;

e) обмежувати кількість дозволених невдалих спроб реєстрації, наприклад, трьома спробами, і брати до уваги:

1) реєстрацію невдалих та успішних спроб;
2) примусову затримку часу перед тим, як дозволити подальші спроби реєстрації, або, якщо не надано певної авторизації, відхиляти будь-які подальші спроби;
3) роз'єднання підключених каналів передавання даних;
4) надсилання на системний пульт тривожного повідомлення по досягненні максимальної кількості спроб реєстрації;
5) встановлення числа повторень пароля співвідносно з мінімальною довжиною пароля і цінністю системи, яку захищають;

f) обмежувати максимальний та мінімальний час, дозволений для процедури реєстрації. У разі його перевищення система повинна припинити реєстрацію;

g) по завершенні успішної реєстрації виводити на екран наведену нижче інформацію:

1) дату та час попередньої успішної реєстрації;
2) подробиці всіх невдалих спроб реєстрації після останньої успішної реєстрації;

h) не виводити на екран введений пароль або розглянути приховування символів пароля знаками;

i)не передавати паролі відкритим текстом через мережу.

Додаткова інформація

Якщо паролі протягом сеансу реєстрації передаються відкритим текстом через мережу, вони можуть бути перехоплені мережевою програмою спостереження за даними в мережі.

11.5.2 Ідентифікація та автентифікація користувача

Контроль

Всі користувачі повинні мати унікальний ідентифікатор (ID користувача) тільки для свого персонального використання та треба вибрати придатну методику автентифікації для підтвердження заявленої ідентичності користувача.

Настанова щодо впровадження

Цей контроль повинен застосовуватися до всіх категорій користувачів (охоплюючи персонал технічного обслуговування, операторів, адміністраторів мережі, системних програмістів і адміністраторів баз даних).

Для відповідальної особи повинні використовуватися ідентифікатори користувачів (IDs), щоб відстежувати її діяльність. Звичайна діяльність користувача не повинна здійснюватись з привілейованих облікових записів.

У надзвичайних випадках, коли від цього є явні бізнес-переваги, можна застосовувати спільний ідентифікатор користувача (ID) для групи користувачів або для певної роботи. У таких випадках повинне бути задокументоване затвердження від керівництва. Для підтримки відстежуваності можуть бути потрібні додаткові контролі.

Загальні ідентифікатори для індивідуального використання можуть бути дозволені лише, якщо доступні функції або виконувані за допомогою ідентифікатора дії не потребують відстежування (наприклад, доступ тільки на читання) або якщо застосовано інші контролі (наприклад, пароль для загального ідентифікатора видається одночасно тільки одній особі і це реєструється).

Там, де потрібні сувора автентифікація та верифікація особи, повинні використовуватися методи, альтернативні паролю, такі як криптографічні засоби, смарт-картки, токени або біометричні засоби.

Додаткова інформація

Паролі (див. також 11.3.1 та 11.5.3) є найбільш звичайним способом забезпечити ідентифікацію та автентифікацію, основану на таємниці, яку знає лише користувач. Цього ж можна досягти криптографічними засобами або протоколами автентифікації. Суворість ідентифікації та автентифікації користувача повинна відповідати чутливості інформації, до якої потрібний доступ.

Такі об’єкти, як токени з пам’яттю чи смарт-картки, якими володіють користувачі, також можуть використовуватись для ідентифікації та автентифікації. Технології біометричної автентифікації, які використовують унікальні характеристики або атрибути особи, також можна використовувати для автентифікації тотожності особи. Поєднання надійно пов’язаних технологій та механізмів призведе до більш суворої автентифікації.

11.5.3 Система управління паролем

Контроль

Системи для управління паролями повинні бути інтерактивними і забезпечувати якісні паролі.

Настанова щодо впровадження

Система управління паролем повинна:

a) для підтримки відстежуваності змушувати до використання індивідуальних ідентифікаторів користувача (IDs) та паролів;

b) дозволяти користувачам вибирати та змінювати свої власні паролі, а також містити процедуру підтвердження на введення поправок помилкового вводу;

c) змушувати вибирати якісні паролі (див. 11.3.1);

d) змушувати до зміни паролів (див. 11.3.1);

e) примушувати користувачів змінювати тимчасові паролі при першій реєстрації (див. 11.2.3);

f) підтримувати запис попередніх паролів користувача і перешкоджати повторному їх використанню;

g) не виводити паролі на екран при їх введенні;

h) зберігати файли паролів окремо від системних даних прикладних програм;

i) зберігати та передавати паролі в захищеній (наприклад, зашифрованій або хешованій) формі.

Додаткова інформація

Паролі є одним з основних засобів підтвердження повноважень користувача на доступ до комп'ютерних послуг.

Деякі прикладні програми вимагають, щоб паролі користувача призначались незалежною повноважною організацією; у таких випадках пункти b), d) та e) наведеної вище настанови не застосовують. У більшості випадків паролі вибирають та підтримують користувачі. Щодо настанови з використання паролів див. 11.3.1.

11.5.4 Використання системних утиліт

Контроль

Використання програм утиліт, що можуть бути спроможні скасовувати контролі системи та прикладних програм, повинно бути обмежене та суворо контрольоване.

Настанова щодо впровадження

Повинні бути розглянуті наведені нижче настанови щодо використання системних утиліт:

a) для системних утиліт використовувати процедури ідентифікації, автентифікації авторизації;

b) сегментувати системні утиліти з програмного забезпечення прикладних програм;

c) обмежувати використання системних утиліт мінімальною практично застосовною кількістю довірених авторизованих користувачів;

d) авторизувати на спеціальне використання системних утиліт;

e) обмежувати доступність системних утиліт, наприклад, на період авторизованої зміни;

f) реєструвати всі використання системних утиліт;

g) визначати та документувати рівні авторизованого доступу для системних утиліт;

h) видаляти або блокувати всі утиліти та системне програмне забезпечення, основані на непотрібному програмному забезпеченні;

i) не робити системні утиліти доступними для користувачів, які мають доступ до прикладних програм у системах, де вимагається розподіл обов'язків.

Додаткова інформація

Більшість комп'ютерних інсталяцій мають одну або більше системних утиліт, які здатні скасовувати контролі системи та прикладних програм.

11.5.5 Блокування неактивних сеансів

Контроль

Неактивні сеанси повинні бути перервані після визначеного періоду бездіяльності.

Настанова щодо впровадження

Засіб тайм-ауту (лімітування часу неактивності) повинен очистити екран сеансу, а також, можливо пізніше, після визначеного періоду неактивності закрити обидва сеанси - і прикладної програми і мережі. Тривалість тайм-ауту повинна відображати ризики безпеки зони, класифікацію оброблюваної інформації та прикладних використовуваних програм і ризики, пов'язані з користувачами обладнання.

Для деяких систем може бути забезпечена обмежена форма засобу тайм-ауту, яка очищає екран і запобігає неавторизованому доступу, але не закриває сеанс прикладної програми і мережі.

Додаткова інформація

Цей контроль є особливо важливим у місцях високого ризику, які охоплюють загальнодоступні або зовнішні зони за межами управління безпекою організації. Сеанси повинні перериватися, щоб запобігти доступу неавторизованих осіб та відхилити атаки на послуги.

11.5.6 Обмеження часу підключення

Контроль

Для забезпечення додаткового захисту прикладних програм з високим ризиком треба використовувати обмеження часу підключення.

Настанова щодо впровадження

Для чутливих комп'ютерних прикладних програм, особливо з місць високого ризику, які охоплюють загальнодоступні або зовнішні зони за межами управління безпекою організації, повинні розглядатися контролі часу підключення. Приклади таких обмежень включають:

a) використання заздалегідь визначених інтервалів часу, наприклад, для передавання командного файлу, або регулярних короткотривалих інтерактивних сеансів;

b) обмеження часу підключення звичайним робочим часом, якщо відсутні вимоги щодо понаднормового чи продовженого часу роботи;

c) розгляд повторної автентифікації через заплановані проміжки часу.

Додаткова інформація

Обмеження періоду, протягом якого дозволене підключення до

комп'ютерних послуг, зменшує вікно можливостей неавторизованого доступу. Обмеження тривалості активних сеансів запобігає користувачам утримувати сеанси відкритими, щоб уникнути повторної автентифікації.

11.6 Контроль доступу до прикладних програм та інформації

Ціль: Запобігти неавторизованому доступу до інформації, що міститься в прикладних системах.

Для обмеження доступу до та в межах прикладних систем повинні використовуватися засоби безпеки.

Логічний доступ до прикладного програмного забезпечення та інформації повинен обмежуватися лише авторизованими користувачами. Прикладні системи повинні:

a) контролювати доступ користувача до інформації та функцій прикладних систем відповідно до визначеної політики контролю доступу;

b) забезпечити захист від неавторизованого доступу будь-яких утиліт, операційного системного програмного забезпечення та зловмисного програмного забезпечення, яке спроможне скасувати або обійти контролі системи або прикладної програми;

c) не компрометувати інші системи, з якими інформаційні ресурси спільно використовуються.

11.6.1 Обмеження доступу до інформації

Контроль

Доступ користувачів та обслуговуючого персоналу до інформації та функцій прикладних систем повинен бути обмежений відповідно до визначеної політики контролю доступу.

Настанова щодо впровадження

Обмеження доступу повинні базуватися на вимогах конкретної прикладної програми бізнесу. Політика контролю доступу повинна також не суперечити політиці доступу організації (див. розділ 11.1).

Для підтримки вимог обмеження доступу повинне бути розглянуте застосування наведених нижче настанов:

a) надання меню, щоб контролювати доступ до функцій прикладних систем;

b) контроль прав доступу користувачів, наприклад, на зчитування, записування, видалення та виконання;

c) контроль прав доступу інших прикладних програм;

d) забезпечення того, що вихідні дані прикладних систем, які обробляють чутливу інформацію, містять лише ту інформацію, яка стосується використання вихідних даних, і вона надсилається лише до авторизованих терміналів та вузлів;

це має включати періодичні перегляди таких вихідних даних, щоб забезпечити, що надлишкова інформація видаляється.

11.6.2 Ізоляція чутливих систем

Контроль

Чутливі системи повинні мати спеціально призначене (ізольоване) комп'ютерне середовище.

Настанова щодо впровадження

Для ізоляції чутливої системи повинні бути розглянуті наведені нижче пункти:

a) чутливість прикладної системи повинна бути чітко ідентифікована та задокументована власником прикладної програми (див. 7.1.2);

b) якщо чутлива прикладна програма повинна виконуватися в спільно використовуваному середовищі, то прикладні системи, з якими вона буде поділяти ресурси, і відповідні ризики повинні бути ідентифіковані й прийняті власником чутливої прикладної програми.

Додаткова інформація

Деякі прикладні системи є досить чутливими до можливої втрати, вони вимагають спеціальної обробки. Чутливість може означати, що прикладна система:

a) повинна запускатись на спеціально призначеному комп'ютері; або

b) повинна спільно використовувати ресурси лише з довірчими прикладними системами.

Ізоляції можна досягти з використанням фізичних або логічних методів (див. також 11.4.5).

11.7 Мобільні обчислення та дистанційна робота

Ціль: Забезпечити безпеку інформації при використанні мобільних обчислень та засобів дистанційної роботи.

Обов'язковий захист повинен бути співвідносним з ризиками, які спричиняють такі спеціальні способи роботи. При використанні мобільного обчислення повинні бути розглянуті ризики роботи у незахищеному середовищі і застосовано належний захист. У випадку дистанційної роботи організація повинна застосувати захист місця дистанційної роботи і забезпечити застосування придатних заходів щодо цього виду роботи.

11.7.1 Мобільні обчислення та комунікації

Контроль

Для захисту від ризиків використання мобільного обчислення та комунікаційних засобів повинна бути наявною офіційно оформлена політика і повинні бути ухвалені відповідні заходи безпеки.

Настанова щодо впровадження

При використанні мобільних обчислень та комунікаційних засобів, наприклад, ноутбуків, кишенькових комп'ютерів, смарт-карток та мобільних телефонів, особливу увагу треба приділити забезпеченню того, щоб бізнес-інформацію не скомпрометовано. Політика мобільного обчислення повинна брати до уваги ризики роботи з обладнанням мобільного обчислення в незахищеному середовищі.

Політика мобільного обчислення повинна охоплювати вимоги щодо фізичного захисту, контролів доступу, криптографічних методів, резервного копіювання та захисту від вірусів. Ця політика повинна також містити правила та рекомендації щодо підключення мобільних засобів до мереж і настанову щодо використання таких засобів у загальнодоступних місцях.

Треба приділяти увагу використанню засобів мобільного обчислення у загальнодоступних місцях, приміщеннях для нарад та інших незахищених зонах за межами службових приміщень організації. Для уникнення неавторизованого доступу до інформації або розголошення інформації, яка зберігається або обробляється такими засобами, повинен бути наявним захист, наприклад, з використанням криптографічних методів (див. 12.3).

Користувачі засобів мобільного обчислення у загальнодоступних місцях повинні подбати про уникнення ризику підглядання неавторизованими особами. Повинні бути наявними і актуалізованими процедури проти зловмисного програмного забезпечення (див. 10.4).

Резервне копіювання критичної бізнес-інформації повинне здійснюватися регулярно. Повинне бути доступним обладнання, яке уможливлює швидке й легке резервне копіювання інформації. Таким резервним копіям треба надати відповідний захист від, наприклад, крадіжки або втрати інформації.

Треба відповідним чином захистити використання мобільних засобів, підключених до мереж. Віддалений доступ до бізнес-інформації через загальнодоступну мережу з використанням засобів мобільного обчислення повинен мати місце лише після успішної ідентифікації та автентифікації та за наявності відповідних механізмів контролю (див. 11.4).

Засоби мобільного обчислення повинні також бути фізично захищені від крадіжки, особливо, якщо їх залишають, наприклад, в автомобілях та інших видах транспорту, готельних номерах, конференц-центрах та приміщеннях для нарад. Для випадків крадіжки або втрати засобів мобільного обчислення повинні бути встановлені певні процедури, які беруть до уваги правові, страхові та інші вимоги безпеки організації. Обладнання, яке є носієм важливої, чутливої та/або критичної бізнес-інформації, не повинне залишатися без нагляду і, за можливості, повинне бути фізично заблоковане, або треба використовувати спеціальні замки для убезпечення обладнання (див. 9.2.5).

Для персоналу, який використовує мобільне обчислення, повинне бути організоване навчання для підвищення його поінформованості щодо додаткових ризиків внаслідок такого способу роботи, і щодо контролів, які повинні бути впроваджені.

Додаткова інформація

Безпроводові мобільні мережеві підключення подібні до інших видів мережевих підключень, але мають важливі відмінності, які треба розглянути при ідентифікації контролів. Типовими відмінностями є:

a) деякі безпроводні протоколи безпеки є слаборозвиненими і мають відомі недоліки;

b) з інформації, що зберігається на мобільних комп'ютерах, не можна зробити резервну копію через обмежену пропускну спроможність мережі та/або через те, що мобільне обладнання може бути не підключене тоді, коли заплановано резервне копіювання.

11.7.2 Дистанційна робота

Контроль

Повинні бути розроблені та впроваджені політика, плани функціонування та процедури щодо дистанційної роботи.

Настанова щодо впровадження

Організації повинні лише тоді дозволяти дистанційну роботу, якщо вони впевнені, що належні заходи безпеки та контролі наявні і що вони задовольняють політику безпеки організації.

Повинен бути наявним придатний захист місця дистанційної роботи від, наприклад, крадіжки обладнання та інформації, неавторизованого розголошення інформації, неавторизованого віддаленого доступу до внутрішніх систем організації або неправильного використання засобів. Дистанційна робота повинна як дозволятися, так і контролюватися керівництвом, і треба забезпечити наявність придатних заходів для цього виду роботи.

Повинні бути розглянуті наведені нижче питання:

a) існуюча фізична безпека місця дистанційної роботи, беручи до уваги фізичну безпеку будівлі та локальної інфраструктури;

b) пропонована фізична інфраструктура дистанційної роботи;

c) вимоги безпеки комунікацій, беручи до уваги потребу дистанційного доступу до внутрішніх систем організації, чутливість інформації, до якої буде доступ, і шлях по каналах зв'язку та чутливість внутрішньої системи;

d) загроза неавторизованого доступу до інформації або ресурсів інших осіб, які користуються тим же приміщенням, наприклад, родини або друзів;

e) використання домашніх мереж і вимоги або обмеження щодо конфігурації послуг безпроводної мережі;

f) політики та процедури запобігання суперечкам щодо прав на інтелектуальну власність, розроблену на обладнанні, що знаходиться у приватній власності;

g) доступ до обладнання, що знаходиться у приватній власності (для перевірки безпеки комп'ютера або в процесі розслідування), якому може перешкоджати законодавство;

h) угоди щодо ліцензування програмного забезпечення, які є такими, що організації можуть бути відповідальними за ліцензування клієнтського програмного забезпечення на робочих станціях, які знаходиться у приватній власності найманого персоналу, контракторів та користувачів третьої сторони;

і)вимоги щодо антивірусного захисту та міжмережевого екранування.

Настанови та заходи, які треба розглянути, повинні включати:

a) забезпечення відповідним обладнанням та пристроями зберігання для дистанційної роботи там, де не дозволяється використання обладнання, що знаходиться у приватній власності, яке не перебуває під контролем організації;

b) визначення дозволеного виду робіт, годин роботи, класифікація інформації, яку можна обробляти, а також внутрішні системи та послуги, доступ до яких дозволено для дистанційної роботи;

c) забезпечення придатним комунікаційним обладнанням, включаючи методи забезпечення віддаленого доступу;

d) фізичну безпеку;

e) правила та настанови щодо доступу родини та відвідувачів до обладнання та інформації;

f) забезпечення підтримки та обслуговування апаратних засобів та програмного забезпечення;

g) забезпечення страхування;

h) процедури резервного копіювання та безперервності бізнесу;

i) аудит та моніторинг безпеки;

j) скасування повноважень та прав доступу, а також повернення обладнання після припинення дистанційної роботи.

Додаткова інформація

Дистанційна робота використовує комунікаційні технології для надання можливості особі працювати віддалено від фіксованого місця за межами його організації.

12 Придбання, розроблення та підтримка інформаційних систем

12.1 Вимоги безпеки для інформаційних систем

Ціль: Забезпечити, що безпека є невід'ємною частиною інформаційних систем.

Інформаційні системи включають операційні системи, інфраструктуру, прикладні програми бізнесу, серійні продукти, послуги та розроблені користувачем прикладні програми. Проектування та впровадження інформаційної системи, яка підтримує бізнес-процес, може бути ключовим для безпеки. Вимоги безпеки повинні ідентифікуватися та погоджуватися до початку розроблення та впровадження інформаційних систем.

Усі вимоги безпеки повинні бути ідентифіковані на етапі встановлення вимог до проекту, обґрунтовані, погоджені та задокументовані як частина загальної бізнес-справи інформаційної системи.

12.1.1 Аналіз та специфікація вимог безпеки

Контроль

Положення щодо бізнес-вимог до нових інформаційних систем або модернізацій до існуючих інформаційних систем повинні визначати вимоги до контролів безпеки.

Настанова щодо впровадження

Специфікації вимог до контролів повинні стосуватися автоматизованих контролів, вбудовуванних в інформаційну систему, і потреби в підтримуючих ручних контролях. Подібні міркування повинні застосовуватися при оцінюванні розроблених або придбаних пакетів програмного забезпечення для прикладних програм бізнесу.

Вимоги безпеки та контролі повинні відображати цінність для бізнесу охоплюваних інформаційних ресурсів (див. також 7.2) і потенційну шкоду бізнесу, яка може бути наслідком відмови або відсутності безпеки.

Системні вимоги до інформаційної безпеки та процеси запровадження безпеки повинні бути інтегровані на початкових стадіях проектування інформаційної системи. Контролі, внесені на етапі проектування, значно дешевше впроваджувати і підтримувати, ніж ті, що вводяться протягом або після впровадження.

Якщо продукти купують, треба слідувати офіційно оформленій процедурі тестування та придбання. Контракти з постачальником повинні враховувати ідентифіковані вимоги безпеки. Якщо функціональність безпеки пропонованого продукту не задовольняє специфіковані вимоги, то внесений ризик і відповідні контролі повинні бути переглянуті до придбання продукту. Якщо постачається додаткова функціональність та спричиняє ризик безпеки, це треба заборонити або треба переглянути запропоновану структуру контролів для визначення того, чи можуть бути отримані переваги із збільшення функціональності.

Додаткова інформація

Якщо визнано придатним, наприклад, через вартість, керівництво може побажати використовувати незалежно оцінені та сертифіковані продукти. Додаткова інформація щодо критеріїв оцінювання ІТ продуктів безпеки може бути, за потреби, знайдена в ISO/IEC 15408 або інших стандартах з оцінювання чи сертифікації.

ISO/IEC TR 13335-3 надає настанову щодо використання процесів управління ризиком для ідентифікації вимог до контролів безпеки.

12.2 Коректне оброблення в прикладних програмах

Ціль: Запобігти помилкам, втратам, неавторизованій модифікації або зловживанню інформацією в прикладних програмах.

У прикладних програмах, включаючи прикладні програми, розроблені користувачами, повинні бути спроектовані належні контролі для забезпечення правильного оброблення. Ці контролі повинні охоплювати підтвердження вхідних даних, внутрішню обробку та вихідні данні.

Для систем, які обробляють або мають вплив на чутливу, цінну або критичну інформацію, можуть бути потрібними додаткові контролі. Такі контролі повинні бути визначені на основі вимог безпеки та оцінки ризику.

12.2.1 Підтвердження вхідних даних

Контроль

Вхідні дані для прикладних програм повинні бути підтверджені для забезпечення того, що ці дані є коректними та відповідними.

Настанова щодо впровадження

До вхідних даних бізнес-трансакцій, фіксованих даних (наприклад, імен та адрес, кредитних лімітів, посилальних номерів клієнта) та таблиць параметрів (наприклад, цін продажу, курсів обміну валюти, податкових ставок) повинні застосовуватися перевірки. Треба розглянути наведені нижче настанови:

a) введення даних по двох незалежних каналах або інші вхідні перевірки, такі як перевірка меж або обмеження полів визначеними діапазонами вхідних даних, для виявлення нижченаведених помилок:

1) значень за межами діапазону;
2) помилкових символів у полях даних;
3) пропущених або неповних даних;
4) перевищення верхньої та нижньої меж кількості даних;
5) неавторизованих або суперечних контрольних даних;

b) періодичний перегляд вмісту ключових полів або файлів даних для підтвердження їх достовірності та цілісності;

c) перевірка друкованих копій вхідних документів на будь-які неавторизовані зміни (усі зміни до вхідних документів повинні бути авторизовані);

d) процедури реагування на помилки підтвердження;

e) процедури тестування правдоподібності вхідних даних;

f) визначення відповідальностей всього персоналу, задіяного в процесі введення даних;

g) створення журналу реєстрації діяльності, яка стосується процесу введення даних (див. 10.10.1).

Додаткова інформація

Там, де це можливо, можуть бути розглянуті автоматичний аналіз і підтвердження вхідних даних для зниження ризику помилок і запобігання звичайним атакам, включаючи переповнення буфера та вставка кодів.

12.2.2 Контроль внутрішньої обробки

Контроль

Підтверджувальні перевірки повинні бути вбудовані у прикладні програми для виявлення будь-якого викривлення інформації через помилки обробки або навмисні дії.

Настанова щодо впровадження

Проектування та впровадження прикладних програм повинні забезпечити, щоб ризики відмов обробки, які ведуть до втрати цілісності, були мінімальними. Особливі сфери діяльності для розгляду включають:

a) функцій додавання, модифікації та видалення, які використовуються для впровадження змін даних;

b) процедури запобігання запуску програм в неправильній послідовності або після відмови попередньої обробки (див. також 10.1.1);

c) використання належних програм для відновлення після відмов, щоб забезпечити коректну обробку даних;

d) захист проти атак з використанням переповнення буфера (вихід за межі пам’яті або переповнення розрядної сітки)

Повинен бути підготований належний контрольний список, діяльність задокументована і результати повинні безпечно зберігатися. Приклади перевірок, які можуть бути вбудовані, включають наведене нижче:

a) сеансові або пакетні контролі для врегулювання балансу файлів після оновлення трансакцій;

b) балансові контролі для перевірки відкритих балансів порівняно з попередніми завершеними балансами, а саме:

1) контролі від-запуску-до-запуску;
2) контрольна сума оновлення файлу;
3) контролі від-програми-до-програми;

c) підтвердження згенерованих системою вхідних даних (див. 12.2.1);

d) перевірки цілісності, автентичності або будь-яких інших характеристик безпеки даних або програмного забезпечення, яке завантажено або пересилається між центральним та віддаленими комп’ютерами;

e) контрольна сума записів та файлів;

f) перевірки для забезпечення того, що прикладні програми

запускаються у правильний час;

g) перевірки для забезпечення того, що прикладні програми запускаються в правильному порядку і припиняються у випадку відмови і що подальша обробка зупиняється, поки проблема не буде вирішена;

h) створення журналу реєстрації діяльності, яка стосується обробки (див. 10.10.1).

Додаткова інформація

Дані, що були введені коректно, можуть бути ушкоджені через помилки апаратних засобів, помилки обробки або через зловмисні дії. Обов'язкові підтверджувальні перевірки будуть залежати від сутності прикладної програми та впливу на бізнес будь-якого ушкодження даних.

12.2.3 Цілісність повідомлення

Контроль

Повинні бути ідентифіковані вимоги щодо забезпечення автентичності та захисту цілісності повідомлень у прикладних програмах, належні контролі повинні бути ідентифіковані та впроваджені.

Настанова щодо впровадження

Повинна здійснюватися оцінка ризиків безпеки для визначення обов'язковості цілісність повідомлення і для ідентифікації найбільш належного методу впровадження.

Додаткова інформація

Як належні засоби впровадження автентифікації повідомлення можна використовувати криптографічні засоби (див. 12.3).

12.2.4 Підтвердження вихідних даних

Контроль

Вихідні дані прикладної програми повинні бути підтверджені для забезпечення того, що оброблення інформації, яку зберігають, є коректним та відповідним до обставин.

Настанова щодо впровадження

Підтвердження вихідних даних може включати:

a) перевірку правдоподібності для тестування, чи є вихідні дані прийнятними;

b) узгодження контрольних обчислень, щоб забезпечити обробляння всіх даних;

c) надання достатньої інформації для зчитувача або наступної системи обробки, щоб визначити безпомилковість, повноту, точність та класифікацію інформації;

d) процедури реагування на підтверджувальне тестування вихідних даних;

e) визначення відповідальностей всього персоналу, задіяного в процесі одержання вихідних даних;

f) створення журналу реєстрації діяльності, яка стосується процесу підтвердження вихідних даних.

Додаткова інформація

Зазвичай системи та прикладні програми розробляються в припущенні, що якщо ужито належних підтвердження, верифікації та тестування, вихідні дані завжди будуть коректними. Однак, це припущення не завжди є дійсним; наприклад, системи, тестування яких було виконано, можуть продовжувати, за певних обставин, видавати некоректні вихідні дані.

12.3 Криптографічні контролі

Ціль: Захистити конфіденційність, автентичність або цілісність інформації криптографічними засобами.

Повинна бути розроблена політика використання криптографічних контролів. Для підтримки використання криптографічних методів повинне бути наявним управління ключами.

12.3.1 Політика використання криптографічних контролів

Контроль

Повинна бути розроблена і впроваджена політика використання криптографічних контролів для захисту інформації.

Настанова щодо впровадження

При розробленні криптографічної політики треба розглянути викладене нижче:

a) підхід керівництва до використання криптографічних контролів в усій організації, охоплюючи загальні принципи, згідно з якими бізнес-інформація повинна захищатися (див. також 5.1.1);

b) виходячи з оцінки ризику, повинен бути ідентифікований потрібний рівень захисту з урахуванням типу, стійкості та якості необхідного алгоритму шифрування;

c) використання шифрування для захисту чутливої інформації, яка транспортується на мобільних або замінюваних носіях, пристроях або через комунікаційні канали;

d) підхід до управління ключами, включаючи методи, що стосуються захисту криптографічних ключів та відновлення зашифрованої інформації у випадку втрачених, скомпрометованих або ушкоджених ключів;

e) ролі та відповідальності, наприклад, хто є відповідальним за:

1) впровадження політики;

2) управління ключами, включаючи генерацію ключа (див. також 12.3.2);

f) стандарти, які повинні бути прийняті для ефективного впровадження в усій організації (яке рішення використовується для якого бізнес-процесу);

g) вплив застосування зашифрованої інформації на контролі, які залежать від перегляду вмісту (наприклад, виявлення вірусу).

При запроваджені криптографічної політики організації треба розглянути

нормативи та національні обмеження, які можуть застосовуватися до використання криптографічних методів у різних частинах світу, та проблеми транскордонних потоків зашифрованої інформації (див. також 15.1.6).

Криптографічні контролі можуть використовуватися для досягнення різних цілей безпеки, наприклад:

a) конфіденційності: використання шифрування інформації для захисту чутливої або критичної інформації, як збереженої, так і тієї, що передається;

b) цілісності/автентичності: використання цифрових підписів або кодів автентифікації повідомлення для захисту автентичності та цілісності збереженої або тієї, що передається, чутливої або критичної інформації;

c) неспростовності: використання криптографічних методів для отримання доказів виникнення або не виникнення події або дії.

Національна примітка.

Банки мають використовувати криптографічний захист інформації відповідно до нормативно-правових актів Національного банку України.

Додаткова інформація

Прийняття рішення щодо того, чи криптографічне рішення є належним, повинне розглядатися як частина більш широкого процесу оцінки ризику та вибору контролів. Ця оцінка може потім бути використана для визначення, чи криптографічний контроль є належним, якого типу контроль треба застосувати та для яких цілей і бізнес-процесів.

Політика використання криптографічних контролів є необхідною для максимізації переваг та мінімізації ризиків використання криптографічних методів, а також для уникнення неналежного або некоректного використання. При використанні цифрових підписів треба розглянути все суттєве законодавство, особливо законодавство, яке описує умови, за яких цифровий підпис є юридично обов’язковим (див. 15.1).

Треба отримати рекомендації фахівця для ідентифікації належного рівня захисту та визначення придатних специфікацій, які нададуть необхідний захист та підтримають запровадження безпечної системи управління ключами (див. також 12.3.2).

ISO/IEC JTC1 SC27 розробив декілька стандартів стосовно криптографічних контролів. Додаткову інформацію можна також знайти в IEEE P1363 та OECD Guidelines on Cryptography.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ.

Настанова OECD щодо криптографії.

12.3.2 Управління ключами

Контроль

Для підтримки використання в організації криптографічних методів повинно бути наявним управління ключами.

Настанова щодо впровадження

Усі криптографічні ключі повинні бути захищені від модифікації, втрати та

знищення. Крім того, таємні та особисті ключі потребують захисту від неавторизованого розголошення. Обладнання, яке застосовують для генерації, зберігання та архівування ключів, повинне бути фізично захищене.

Система управління ключами повинна базуватися на погодженому наборі стандартів, процедур та методів безпеки щодо:

a) генерації ключів для різних криптографічних систем та різних прикладних програм;

b) генерації та отримання сертифікатів відкритих ключів;

c) розподілу ключів серед призначених користувачів, включаючи те, як ключі повинні бути активовані після отримання;

d) зберігання ключів, включаючи, як авторизовані користувачі отримують доступ до ключів;

e) заміни або оновлення ключів, включаючи правила стосовно того, коли ключі повинні замінюватися і яким чином це треба робити;

f) поводження із скомпрометованими ключами;

g) відкликання ключів, включаючи те, як ключі повинні бути скасовані або деактивовані, наприклад, коли ключі скомпрометовано або коли користувач залишає організацію (у якому випадку ключі повинні також бути архівовані);

h) відновлення ключів, які втрачено або зруйновано, як частина управління безперервністю бізнесу, наприклад для відновлення зашифрованої інформації;

i) архівування ключів, наприклад, для архівованої або резервної скопійованої інформації;

j) знищення ключів;

k) реєстрування та аудит діяльності, пов’язаної з управлінням ключами.

З метою зниження ймовірності компрометації, активація та деактивація даних для ключів повинна бути визначена так, щоб ключі могли застосовуватися лише обмежений період часу. Цей період часу повинен залежати від обставин, за яких використовується криптографічний контроль, та від усвідомлюваного ризику.

Додатково до безпечного управління таємним та особистим ключами також повинна бути розглянута автентичність відкритих ключів. Такий процес автентифікації може виконуватися із використанням сертифікатів відкритих ключів, які, зазвичай, випускаються повноважною організацією з сертифікації, яка повинна бути визнаною організацією з наявними контролями та процедурами придатними для забезпечення необхідного ступеня довіри.

Зміст угод або контрактів щодо рівня послуг зовнішніх постачальників криптографічних послуг, наприклад, повноважної організації з сертифікації, повинен охоплювати питання обов’язків, надійності послуг та часу реагування щодо надання послуг (див. 6.2.3).

Додаткова інформація

Управління криптографічними ключами є суттєвим для ефективного використання криптографічних методів. ISO/IEC 11770 надає додаткову інформацію щодо управління ключами. Двома видами криптографічних методів є:

a) методи таємного ключа, коли дві або більше сторони спільно

використовують один і той же ключ, і цей ключ застосовують як для шифрування, так і дешифрування інформації; цей ключ повинен зберігатися в таємниці, оскільки будь-хто, який має доступ до цього ключа, здатен дешифрувати всю інформацію, зашифровану за допомогою цього ключа, або внести неавторизовану інформацію, застосовуючи цей ключ;

b) методи відкритого ключа, де кожний користувач має пару ключів, відкритий ключ (який може бути відтворений будь-ким) та особистий ключ (який повинен зберігатися в таємниці); методи відкритого ключа можуть застосовуватися для шифрування та для створення цифрових підписів (див. також ISO/IEC 9796 та ISO/IEC 14888).

Є загроза підробки цифрового підпису шляхом заміни відкритого ключа користувача. Ця проблема враховується використанням сертифіката відкритого ключа.

Криптографічні методи можуть також використовуватися для захисту криптографічних ключів. Може потребуватися розгляд процедур для обробки правових запитів на доступ до криптографічних ключів, наприклад, може знадобитись, щоб зашифрована інформація була доступною в незашифрованій формі як доказ у судовій справі.

12.4 Безпека системних файлів

Ціль: Забезпечити безпеку системних файлів.

Доступ до системних файлів та початкового програмного коду повинен бути контрольований, а ІТ проекти та діяльність з обслуговування повинні вестися у безпечний спосіб. Треба потурбуватися щодо уникнення незахищеності чутливих даних у випробувальному середовищі.

12.4.1 Контроль операційного програмного забезпечення

Контроль

Повинні бути наявними процедури контролю інсталяції програмного забезпечення в операційних системах.

Настанова щодо впровадження

Для мінімізації ризику ушкодження операційних систем повинні бути розглянуті наведені нижче настанови щодо контролю змін:

a) оновлення операційного програмного забезпечення, прикладних програм та бібліотек програм повинні здійснюватися лише адміністраторами, які пройшли навчання, після відповідної їх авторизації керівництвом (див. 12.4.3);

b) операційні системи повинні містити лише затверджений виконуваний код, а не розроблений код чи компілятори;

c) прикладні програми та програмне забезпечення операційних систем повинні запроваджуватися лише після всебічного та успішного тестування; тести повинні включати тестування на простоту використання, безпеку, вплив на інші системи та зручність для користувачів і повинні виконуватися на відокремлених системах (див. також 10.1.4); треба забезпечити, що всі відповідні бібліотеки

початкових програм оновлені;

d) для додержання контролю як над усім впровадженим програмним забезпеченням, так і над усією системною документацією повинна використовуватися система контролю конфігурації;

e) стратегія резервного копіювання повинна бути наявна до впровадження змін;

f) для всіх оновлень бібліотек операційних програм повинен підтримуватися журнал аудиту;

g) як захід на випадок непередбачуваних обставин повинні підтримуватися попередні версії прикладного програмного забезпечення;

h) старі версії програмного забезпечення повинні зберігатися в архіві разом з усією необхідною інформацією та параметрами, процедурами, подробицями щодо конфігурації та програмами підтримки, стільки ж часу, скільки в архіві зберігаються дані.

Використовуване в операційних системах програмне забезпечення, яке постачає виробник, повинне обслуговуватися на рівні, який підтримує постачальник. Через певний час виробники програмного забезпечення припиняють підтримувати попередні версії програмного забезпечення. Організація повинна розглянути ризики залежності від непідтримуваного програмного забезпечення.

Будь-яке рішення щодо переходу на нову версію повинне враховувати бізнес-вимоги щодо зміни та безпеку версії, тобто введення нової функціональності безпеки або кількості та серйозності проблем безпеки, які впливають на цю версію. Виправлення програмного забезпечення повинні застосовуватися, якщо вони можуть допомогти усунути або зменшити слабкі місця безпеки (див. також 12.6.1).

Фізичний або логічний доступ повинен надаватися постачальникам лише за необхідності та з метою підтримки і після затвердження керівництвом. Повинен здійснюватися моніторинг діяльність постачальників.

Програмне забезпечення може залежати від постачених ззовні програмного забезпечення та модулів, які треба моніторити і контролювати, щоб уникнути неавторизованих змін, які можуть привнести слабкі місця безпеки.

Додаткова інформація

Операційні системи повинні оновлюватися лише тоді, коли в цьому є необхідність, наприклад, якщо поточна версія операційної системи більше не підтримує бізнес-вимоги. Оновлення не повинно здійснюватися лише тому, що стала доступною нова версія операційної системи. Нові версії операційних систем можуть бути менш безпечні, менш стабільні та менш зрозумілі, ніж поточні системи.

12.4.2 Захист даних для тестування системи

Контроль

Дані для тестування повинні бути ретельно відібрані, захищені та контрольовані.

Настанова щодо впровадження

Треба уникати використання для цілей тестування операційних баз даних, які містять персональну інформацію або будь-яку іншу чутливу інформацію. Якщо персональна або будь-яка інша чутлива інформація використовується для цілей тестування, усі чутливі подробиці та вміст повинні до використання бути видалені або модифіковані до невпізнанності. Для захисту операційних даних при їх використанні для цілей тестування повинні застосовуватися наведені нижче настанови:

a) процедури контролю доступу, які застосовують до операційних прикладних систем, повинні також застосовуватися до тестованих прикладних систем;

b) повинна здійснюватися окремо кожного разу авторизація копіювання операційної інформації для тестованої прикладної системи;

c) операційна інформація повинна видалятися з тестованої прикладної системи негайно після завершення тестування;

d) копіювання та використання операційної інформації повинне реєструватися для формування журналу аудиту.

Додаткова інформація

Системне та приймальне тестування зазвичай потребує значних обсягів тестових даних, найблизькіших до операційних даних, наскільки це можливо.

12.4.3 Контроль доступу до початкових кодів програми

Контроль

Доступ до початкових кодів програми повинен бути обмежений.

Настанова щодо впровадження

Доступ до початкових кодів програми та пов’язаних елементів (таких як проект, специфікації, плани верифікації та плани підтвердження) повинні бути ретельно контрольованими для запобігання внесенню неавторизованої функціональності та уникнення ненавмисних змін. Для початкових кодів програми цього можна досягти за допомогою контрольованого централізованого зберігання такого коду, краще у бібліотеках початкових програм. У такому випадку треба розглянути наведені нижче настанови (див. також 11) для контролю доступу до таких бібліотек початкових програм, щоб зменшити можливість руйнування комп’ютерних програм:

a) за можливості, бібліотеки початкових програм не повинні зберігатися в працюючих системах;

b) управління початковим кодом програми та бібліотекою початкових програм повинне здійснюватися відповідно до розроблених процедур;

c) допоміжний персонал не повинен мати необмежений доступ до бібліотек початкових програм;

d) оновлення бібліотек початкових програм та пов’язаних елементів і надання джерел програм програмістам повинні здійснюватися лише після отримання відповідного дозволу;

e) лістинги програм повинні зберігатися у безпечному середовищі (див.

10.7.4);

f) повинен підтримуватися журнал аудиту всіх доступів до бібліотек початкових програм;

g) підтримування та копіювання бібліотек початкових програм повинне бути об’єктом процедур жорсткого контролю змін (див. 12.5.1).

Додаткова інформація

Початковий код програми є кодом, написаним програмістами, який компілюється (та компонується) для створення виконавчих файлів. Деякі мови програмування формально не розрізняють початковий код та виконавчі файли, оскільки виконавчі файли створюються при їх активації.

Стандарти ISO 10007 та ISO/IEC 12207 надають подальшу інформацію стосовно управління конфігурацією та процесу життєвого циклу програмного забезпечення.

12.5 Безпека у процесах розроблення та підтримки

Ціль: Підтримувати безпеку прикладного програмного забезпечення та інформації.

Середовище проектування та підтримки повинне бути жорстко контрольованим.

Керівники, відповідальні за прикладні системи, повинні також бути відповідальними за безпеку середовища проектування або підтримки. Вони повинні забезпечити, що всі пропоновані зміни системи переглядаються для перевірки того, що вони не компрометують безпеку ні системи, ні операційного середовища.

12.5.1 Процедури контролю змін

Контроль

Впровадження змін повинно бути контрольованим за допомогою офіційно оформлених процедур контролю змін.

Настанова щодо впровадження

Офіційно оформлені процедури контролю змін повинні бути задокументовані та здійснюватися примусово для мінімізації руйнування інформаційних систем. Введення нових систем та більшості змін до існуючих систем повинне слідувати за офіційно оформленим процесом документування, специфікаціями, тестуванням, контролем якості та впровадженням, яким управляють.

Цей процес повинен включати оцінку ризику, аналіз впливу змін і специфікацію необхідних контролів безпеки. Цей процес повинен також забезпечувати, що існуючі процедури безпеки та контролювання не скомпрометовано, що обслуговуючим програмістам надано доступ лише до тих частин системи, які необхідні для їх роботи, і що для будь-яких змін отримано офіційно оформлені угоди та затвердження.

Всюди, де це можливо, процедури контролю змін прикладних програм і функціонування повинні бути об’єднані (див. також 10.1.2). Процедури змін повинні включати:

a) підтримування запису щодо погоджених рівнів авторизованого доступу;

b) забезпечення, що зміни подаються авторизованими користувачами;

c) перегляд контролів та процедур цілісності для забезпечення того, що вони не будуть цими змінами скомпрометовані;

d) ідентифікація усього програмного забезпечення, інформації, компонентів баз даних та апаратних засобів, які потребують корекції;

e) отримання до початку роботи офіційно оформленого затвердження докладних пропозицій;

f) забезпечення, щоб авторизовані користувачі прийняли зміни до їх впровадження;

g) забезпечення, що комплект системної документації оновлюється по завершенні кожної зміни і що стара документація архівується або вилучається;

h) підтримання контролю версій для всіх оновлень програмного забезпечення;

i) підтримання журналу аудиту всіх запитів на зміни;

j) забезпечення, що операційна документація (див. 10.1.1) та користувацькі процедури за необхідності змінюються для того, щоб залишатися належними;

k) забезпечення, що впровадження змін має місце у потрібний час і не порушує залучені бізнес-процеси.

Додаткова інформація

Заміна програмного забезпечення може вплинути на операційне середовище.

Хорошою практикою є тестування нового програмного забезпечення в середовищі, сегментованому як від промислового обладнання, так і від середовища розробки (див. також 10.1.4). Це забезпечує засоби контролю над новим програмним забезпеченням і надає додатковий захист операційній інформації, яка використовується для тестування. Це повинне охоплювати виправлення, пакети оновлення та інші оновлення. Автоматичні оновлення не повинні використовуватися на критичних системах, оскільки деякі оновлення можуть спричинити відмову критичних прикладних програм (див. 12.6).

12.5.2 Технічний перегляд прикладних програм після змін операційної системи

Контроль

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.

Настанова щодо впровадження

Ця процедура повинна включати:

a) перегляд процедур контролювання та цілісності прикладних програм для забезпечення того, що їх не було скомпрометовано змінами операційної системи;

b) забезпечення, що річний план підтримки та бюджет забезпечують перегляди та тестування системи внаслідок змін операційної системи;

c) забезпечення, що сповіщення щодо змін операційної системи надано вчасно для уможливлення проведення до впровадження належного тестування та переглядів;

d) забезпечення, що зроблені належні зміни до плану безперервності бізнесу (див. розділ 14).

На окрему групу або особу треба покласти відповідальність за моніторинг вразливостей та версій виправлень та тимчасових рішень (див. 12.6).

12.5.3 Обмеження на зміни до пакетів програмного забезпечення

Контроль

Модифікації до пакетів програмного забезпечення повинні не заохочуватися, бути обмеженими найнеобхіднішими змінами і всі зміни повинні суворо контролюватися.

Настанова щодо впровадження

Наскільки це можливо і практично застосовно, постачені виробником пакети програмного забезпечення повинні використовуватися без модифікацій. У тих випадках, коли пакети програмного забезпечення потребують модифікації, треба розглянути наведені нижче пункти:

a) ризик компрометації вбудованих контролів та процесів цілісності;

b) чи треба отримати згоду виробника;

c) можливість отримання необхідних змін від виробника як стандартних оновлень програми;

d) вплив того, що організація внаслідок змін стає відповідальною за майбутню підтримку програмного забезпечення.

Якщо зміни необхідні, оригінальне програмне забезпечення повинне бути збережене, а зміни застосовані до чітко визначеної копії. Повинен бути впроваджений процес управління оновленням програмного забезпечення, щоб гарантувати, що найновіші затверджені виправлення та оновлення прикладних програм інстальовані на всьому авторизованому програмному забезпеченні (див. 12.6). Усі зміни повинні бути повністю протестовані та задокументовані, так, щоб вони могли бути повторно застосовані, за необхідності, до майбутніх модернізацій програмного забезпечення. Якщо це потрібно, модифікації повинні бути протестовані та затверджені незалежним органом з оцінювання.

12.5.4 Витік інформації

Контроль

Треба запобігати можливостям витоку інформації.

Настанова щодо впровадження

Для обмеження ризику витоку інформації, наприклад, через використання та

експлуатацію прихованих каналів, треба розглянути наведене нижче:

a) сканування носіїв та комунікацій, що виходять за межі організації, щодо прихованої інформації;

b) маскування та модуляція поведінки систем і комунікацій для зниження ймовірності того, що третя сторона зможе через таку поведінку простежити інформацію;

c) використання систем та програмного забезпечення, які, як вважається, мають високу цілісність, наприклад, застосування продуктів, якість яких визначена (див. ISO/IEC 15408);

d) регулярний моніторинг діяльності персоналу та системи, де це дозволено правовими нормами і нормативами;

e) моніторинг використання ресурсу в комп'ютерних системах.

Додаткова інформація

Приховані канали - це шляхи, не призначені для передавання інформаційних потоків, але які тим не менше можуть існувати в системі або мережі. Наприклад, маніпулювання бітами в пакетах комунікаційного протоколу може використовуватися як прихований метод передавання сигналів. У зв'язку з їх природою запобігання існуванню всіх можливих прихованих каналів буде важким, якщо не неможливим. Проте, експлуатація таких каналів часто здійснюється за допомогою троянського коду (див. також 10.4.1). Отже, вжиття заходів захисту від троянського коду зменшує ризик експлуатації прихованих каналів.

Запобігання неавторизованому доступу до мережі (11.4) так же, як політика та процедури не заохочення зловживання персоналом інформаційними послугами (15.1.5), допоможуть захисту від прихованих каналів.

12.5.5 Аутсорсингове розроблення програмного забезпечення

Контроль

Організація повинна здійснювати нагляд над аутсорсинговим розробленням програмного забезпечення та його моніторинг.

Настанова щодо впровадження

Там, де є аутсорсингове розроблення програмного забезпечення, треба розглянути наведені нижче пункти:

a) ліцензійні угоди, права власності на коди та права інтелектуальної власності (див. 15.1.2);

b) сертифікацію якості й точності виконуваних робіт;

c) заходи умовного депонування документів у випадку відмови третьої сторони;

d) права доступу для аудиту якості та точності виконаних робіт;

e) контрактні вимоги до якості та безпечної функціональності коду;

f) тестування перед інсталяцією для виявлення зловмисних та троянського кодів.

12.6 Управління технічною вразливістю

Ціль: Зменшити ризики в результаті використання публікацій щодо технічних вразливостей.

Управління технічною вразливістю повинне впроваджуватися в ефективний, систематичний та відтворюваний спосіб з вимірюваннями, спрямованими на підтвердження його ефективності. Ці міркування стосуються операційних систем та усіх інших використовуваних прикладних програм.

12.6.1 Контроль технічних вразливостей

Контроль

Треба отримувати своєчасну інформацію щодо технічних вразливостей використовуваних інформаційних систем, оцінювати підвладність організації таким вразливостям і вживати належні заходи, щоб врахувати пов'язаний з цим ризик.

Настанова щодо впровадження

Актуальний та повний інвентарний опис активів (див. 7.1) є передумовою ефективного управління технічною вразливістю. Спеціальна інформація, необхідна для підтримки управління технічною вразливістю, охоплює виробника програмного забезпечення, номери версій, поточний стан розміщення (наприклад, яке програмне забезпечення інстальоване в яких системах) і особу (осіб) в організації, відповідальну(их) за програмне забезпечення.

У відповідь на ідентифікацію потенційних технічних вразливостей повинні вживатися належні та своєчасні дії. Для розроблення ефективного процесу управління технічними вразливостями треба слідувати наведеній нижче настанові:

a) організація повинна визначити та встановити ролі та відповідальності, пов’язані з управлінням технічною вразливістю, включаючи моніторинг вразливості, оцінку ризику вразливості, виправлення, відслідковування активу, та всі необхідні відповідальності щодо координації;

b) інформаційні ресурси, які будуть використовуватися для ідентифікації суттєвих технічних уразливостей і підтримки поінформованості щодо них, повинні бути ідентифіковані для програмного забезпечення та інших технологій (на основі інвентарного опису активів, див. 7.1.1); ці інформаційні ресурси повинні оновлюватися на основі змін в інвентарному описі або якщо знайдено інші нові або корисні ресурси;

c) повинна бути визначена часова шкала реагування на сповіщення щодо потенційно суттєвих технічних вразливостей;

d) як тільки потенційна технічна вразливість ідентифікована, організація повинна ідентифікувати пов’язані ризики і дії, яких треба вжити; така дія може залучати виправлення у вразливих системах та/або застосування інших контролів;

e) залежно від того, наскільки терміново треба врахувати технічну вразливість, вжиті дії повинні здійснюватися відповідно до контролів, пов’язаних з управлінням змінами (див. 12.5.1), або згідно з процедурами відповіді на

інциденти інформаційної безпеки (див. 13.2);

f) якщо доступне виправлення, треба оцінити ризики, пов’язані з інсталяцією виправлення (ризики, викликані уразливістю, повинні бути порівняні з ризиком від інсталяції виправлення);

g) виправлення повинні бути протестовані й оцінені до їх інсталяції, щоб забезпечити, що вони ефективні і не призводять до побічних неприпустимих ефектів; якщо виправлення недоступні, треба розглянути інші контролі, такі як:

1) відключити послуги або можливості, пов’язані з вразливістю;
2) пристосувати або додати контролі доступу, наприклад, міжмережеві екрани на границях мережі (див. 11.4.5);
3) посилити моніторинг для виявлення або запобігання реальним атакам;
4) покращити поінформованість щодо вразливості;

h) для всіх вжитих процедур треба підтримувати журнал аудиту;

i) повинні постійно здійснюватися моніторинг і оцінювання процесу управління технічною вразливістю, щоб забезпечити його результативність та ефективність;

j) системи з високим ризиком повинні враховуватися першими.

Додаткова інформація

Коректне функціонування процесу управління технічною вразливістю в організації є критичним для багатьох організацій і тому треба постійно здійснювати його моніторинг. Точний інвентарний опис необхідний для того, щоб забезпечити, що потенційно суттєві технічні вразливості ідентифіковано.

Управління технічною вразливістю може розглядатися як підфункція управління змінами і, як така, може одержувати ефект від процесів та процедур управління змінами (див. 10.1.2 та 12.5.1).

На виробників часто чиниться тиск, щоб вони випускали виправлення якомога скоріше. Тому виправлення може не враховувати проблему адекватно і може мати негативний побічний ефект. До того ж у деяких випадках, якщо виправлення було застосоване, деінсталювати його може бути нелегко.

Якщо адекватне тестування виправлень неможливе, наприклад, через вартість або недостатність ресурсів, можна розглянути відкладення виправлення доки на основі досвіду, описаного іншими користувачами, будуть оцінені пов’язані ризики.

13 Управління інцидентом інформаційної безпеки

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.

Повинні бути наявними офіційно оформлені процедури звітування про події та ескалації. Весь найманий персонал, контрактори і користувачів третьої сторони повинні бути поінформовані щодо процедур звітування про різні види подій та слабких місць, які можуть впливати на безпеку активів організації. Вони повинні бути зобов'язані якнайшвидше звітувати про будь-які події та слабкі місця інформаційної безпеки у визначену точку контакту.

13.1.1 Звітування про події інформаційної безпеки

Контроль

Щодо подій інформаційної безпеки треба якнайшвидше звітувати через належні канали управління.

Настанова щодо впровадження

Повинна бути розроблена офіційно оформлена процедура звітування про події інформаційної безпеки, а також процедури реагування та ескалації, де встановлено дії, яких треба вжити після отримання звіту про події інформаційної безпеки. Повинна бути встановлена контактна особа для звітування про подій інформаційної безпеки. Треба забезпечити, що ця контактна особа була відома у межах всієї організації, завжди доступна і здатна адекватно і своєчасно відреагувати.

Весь найманий персонал, контрактори і користувачів третьої сторони повинні бути поінформовані щодо своєї відповідальності якнайшвидше звітувати про будь-які події інформаційної безпеки. Вони також повинні бути поінформовані щодо процедури звітування про події інформаційної безпеки і контактну особу. Процедури звітування повинні включати:

a) відповідні процедури зворотного зв'язку для забезпечення того, щоб ті, хто звітував про події інформаційної безпеки, були сповіщені про результати після того, як проблему було оброблено й закрито;

b) форми звітування про подію інформаційної безпеки для підтримування звітування і допомоги особі, що звітує, запам'ятати всі необхідні дії у разі події інформаційної безпеки;

c) правильну поведінку, якої треба дотримуватися у разі події інформаційної безпеки, тобто:

1) негайно записувати усі важливі подробиці (наприклад, тип невідповідності або порушення, збій, який мав місце, повідомлення на екрані, незвичайний режим роботи);

2) не виконувати жодних власних дій, а негайно звітувати контактній особі;

d) посилання на офіційно оформлений дисциплінарний процес поводження

із найманим персоналом, контакторами і користувачами третьої сторони, які здійснили порушення безпеки.

У середовищі високого ризику може бути наданий сигнал щодо змушення[4], яким особа, яку примушують, може позначити такі проблеми. Процедури реагування на сигнал щодо змушення повинні відображати ситуацію високого ризику, яку позначають такі сигнали.

Додаткова інформація

Прикладами подій та інцидентів інформаційної безпеки є:

a) втрата послуги, обладнання або засобів обслуговування;
b) збій або перевантаження системи;
c) людські помилки;
d) невідповідності політиці або настановам;
e) порушення заходів фізичної безпеки;
f) неконтрольовані зміни системи;
g) збій програмного забезпечення або апаратних засобів;
h) порушення доступу.

При належному піклуванні про аспекти конфіденційності, інциденти інформаційної безпеки можна використовувати у навчанні користувачів для поінформованості (див. 8.2.2) як приклади того, що може трапитись, як реагувати на такі інциденти і як уникнути їх у майбутньому. Щоб бути здатними правильно враховувати події та інциденти інформаційної безпеки, може бути необхідним збирати докази якнайшвидше після того, як вони відбулися (див. 13.2.3).

Збої або інша аномальна поведінка системи можуть бути показником атаки на безпеку або фактичного порушення безпеки і тому про них треба завжди звітувати як про подію інформаційної безпеки.

Додаткову інформацію щодо звітування про події інформаційної безпеки та управління інцидентами інформаційної безпеки можна знайти в ISO/IEC TR 18044.

13.1.2 Звітування щодо слабких місць інформаційної безпеки

Контроль

Треба вимагати від усього найманого персоналу, контракторів 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.

Настанова щодо впровадження

Увесь найманий персонал, контрактори та користувачі третьої сторони повинні якнайшвидше звітувати про це або своєму керівництву або безпосередньо своєму провайдеру, щоб запобігти інцидентам інформаційної безпеки. Процес звітування повинен бути якомога простим, доступним та досяжним. Вони повинні бути поінформовані, що вони не повинні за жодних обставин намагатися знайти підтвердження очікуваної слабкого місця.

[4] Сигнал щодо змушення є методом таємного позначення, що дія мала місце „з примусу”.

Додаткова інформація

Найманому персоналу, контракторам та користувачам третьої сторони треба рекомендувати не намагатися знайти підтвердження очікуваної слабкого місця безпеки. Тестування слабких місць може розцінюватися як потенційне зловживання системою і може також нанести ушкодження інформаційній системі або послузі і призвести до правових зобов'язань особи, яка здійснює тестування.

13.2 Управління інцидентами інформаційної безпеки та вдосконаленням

Ціль: Забезпечити застосування до управління інцидентами інформаційної безпеки послідовного та ефективного підходу.

Повинні бути наявними відповідальності та процедури ефективної обробки подій та слабких місць інформаційної безпеки одразу ж після звітування про них. До реагування, моніторингу, оцінювання та загального управління інцидентами інформаційної безпеки повинен застосовуватися процес безперервного вдосконалення.

Там, де потрібні докази, вони повинні бути зібрані, щоб забезпечити відповідність правовим вимогам.

13.2.1 Відповідальності та процедури

Контроль

Повинні бути розроблені відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.

Настанова щодо впровадження

Додатково до звітування про події та слабкі місця інформаційної безпеки (див. також 13.1) для виявлення інцидентів інформаційної безпеки повинні використовуватися моніторинг систем, сигналів і вразливостей (10.10.2). Треба розглянути наведені нижче настанови щодо процедур управління інцидентом інформаційної безпеки:

a) повинні бути розроблені процедури обробки різних видів інцидентів інформаційної безпеки, охоплюючи:
   1) відмови інформаційної системи й втрату послуги;
   2) зловмисний код (див. 10.4.1);
   3) відмову в обслуговуванні;
   4) помилки внаслідок неповних або неточних бізнес-даних;
   5) порушення конфіденційності та цілісності;
   6) зловживання інформаційними системами;

b) додатково до звичайних планів дій в аварійних обставинах (див. 14.1.3) процедури повинні також включати (див. також 13.2.2):
   1) аналіз та ідентифікацію причини інциденту;
   2) локалізацію;
   3) планування та впровадження коригувальних дій для запобігання

рецидивів, за необхідності;

4) зв’язок з тими, хто постраждав від інциденту або залучений до відновлення;
5) звітування про дію тому, хто має належні повноваження;

c) журнали аудиту та аналогічні докази повинні збиратися (див. 13.2.3) і, за необхідності, захищатися для:

1) внутрішнього аналізу проблеми;
2) застосування як судового доказу стосовно потенційного порушення контрактних або нормативних вимог або у разі цивільних або кримінальних позовів, наприклад, порушення законодавства щодо зловживання комп’ютером або захисту даних;
3) ведення переговорів щодо компенсації від постачальників програмного забезпечення та послуг;

d) діяльність з відновлення після порушень безпеки і відмов в коректній роботі системи повинна ретельно контролюватися з офіційним оформленням; процедури повинні забезпечувати, що:

1) лише чітко ідентифікованому та авторизованому персоналу дозволяється доступ до діючих систем та оперативних даних (див. також 6.2 стосовно зовнішнього доступу);
2) усі вжиті аварійні дії були детально задокументовані;
3) аварійні дії звітувалися керівництву і системно переглядалися;
4) цілісність бізнес систем та контролів підтверджувалася з мінімальною затримкою.

Цілі управління інцидентами інформаційної безпеки повинні бути погоджені з керівництвом, і треба забезпечити, що особи, відповідальні за управління інцидентами інформаційної безпеки, розуміють пріоритети організації щодо обробки інцидентів інформаційної безпеки.

Додаткова інформація

Інциденти інформаційної безпеки можуть виходити за межі організації та державні кордони. Щоб реагувати на такі інциденти існує зростаюча потреба координувати дії у відповідь і спільно використовувати інформацію щодо цих інцидентів з належними зовнішніми організаціями.

13.2.2 Вивчення інцидентів інформаційної безпеки

Контроль

Повинні бути наявними механізми, які дозволяють визначати кількість і здійснювати моніторинг типів, обсягів та вартості інцидентів інформаційної безпеки.

Настанова щодо впровадження

Інформація, отримана від оцінювання інцидентів інформаційної безпеки, повинна використовуватися для ідентифікації інцидентів, які повторюються або мають великий вплив.

Додаткова інформація

Оцінювання інцидентів інформаційної безпеки може вказати на потребу в удосконалених або додаткових контролях для обмеження частоти, ушкодження та вартості майбутніх інцидентів або може бути взяте до уваги в процесі перегляду політики безпеки (див. 5.1.2).

13.2.3 Збирання доказів

Контроль

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.

Настанова щодо впровадження

Повинні бути розроблені і виконуватися внутрішні процедури збирання й надання доказів для дисциплінарних цілей, здійснюваних організацією.

У загальному випадку правила щодо доказів охоплюють:

a) припустимість доказу: може чи ні доказ бути використаний у суді;

b) вагомість доказу: якість та повнота доказу.

Щоб досягти припустимості доказу, організація повинна забезпечити, що її інформаційні системи задовольняють будь-який опублікований стандарт або звід правил щодо отримання доказів, які можуть бути прийняті до розгляду судом.

Вагомість доказу, що надається, повинна задовольняти будь-які застосовні вимоги. Щоб досягти вагомості доказу, повинні бути продемонстровані в доказової виді якість та повнота контролів, використовуваних для правильного та несуперечливого захисту доказу (тобто, доказ процесу контролю) протягом періоду зберігання та оброблення доказу. Взагалі, така доказовість може бути встановлена за таких умов:

a) для паперових документів: оригінал надійно зберігають з реєстрацією особи, яка знайшла документ, того, де цей документ було знайдено, коли цей документ було знайдено і хто був свідком знаходження; будь-яке розслідування повинне пересвідчитися, що оригінали не підроблені;

b) для інформації на комп'ютерних носіях: щоб забезпечити доступність інформації повинні братися дзеркальні відображення або копії (залежно від застосовних вимог) будь-якого замінюваного носія, інформації з жорстких дисків або пам'яті; повинен зберігатися журнал всіх дій протягом процесу копіювання і процес повинен бути засвідчений; оригінальний носій та журнал реєстрації (якщо це неможливо, то хоча б одне дзеркальне відображення або копія) повинні бути надійно збережені і недоторкані.

Будь-які судові роботи повинні виконуватися лише з копіями доказових матеріалів. Цілісність усіх доказових матеріалів повинна бути захищена. Копіювання доказового матеріалу повинне здійснюватися під наглядом персоналу, який заслуговує довіри, та повинна бути зареєстрована інформація: коли і де виконувався процес копіювання, хто здійснював копіювання і які інструменти та програми були використані.

Додаткова інформація

Коли подію інформаційної безпеки виявлено вперше, може не бути очевидним, чи дійсно ця подія призведе до судових дій. Тому існує небезпека, що необхідний доказ буде зруйнований навмисно або випадково до усвідомлення серйозності інциденту. Тому бажано завчасно в будь-яку правову діяльність залучити адвоката або поліцію і отримати рекомендації щодо необхідного доказу.

Докази можуть виходити за межі організації та/або юрисдикції. У таких випадках треба забезпечити, щоб організація мала право збирати необхідну інформацію як доказ. Щоб максимально збільшити можливості визнання за межами відповідної юрисдикції, повинні також бути розглянуті вимоги різних юрисдикцій.

14 Управління безперервністю бізнесу

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.

Процес управління безперервністю бізнесу повинен запроваджуватися для мінімізації впливу на організацію та відновлення втрати інформаційних активів (які можуть спричинятися, наприклад, природними лихами, нещасними випадками, відмовами обладнання, а також навмисними діями) до прийнятного рівня шляхом поєднання превентивних та відновлювальних контролів. Цей процес повинен ідентифікувати критичні бізнес-процеси та інтегрувати вимоги управління інформаційною безпекою щодо безперервності бізнесу з іншими вимогами безперервності, які стосуються таких аспектів, як функціонування, кадрове забезпечення, матеріали, транспорт і засоби обслуговування.

Наслідки катастроф, відмов безпеки, втрати обслуговування та доступності обслуговування повинні бути предметом аналізу впливів на бізнес. Плани безперервності бізнесу повинні бути розроблені та впроваджені для забезпечення своєчасного відновлення суттєвого функціонування. Інформаційна безпека повинна бути невід'ємною частиною загального процесу безперервності бізнесу та інших процесів управління організації.

Додатково до загального процесу оцінки ризиків управління безперервністю бізнесу повинне включати контролі для ідентифікації та зменшення ризиків, обмеження наслідків ушкоджуючих інцидентів і забезпечувати, що інформація, необхідна для бізнес-процесів, легко доступна.

14.1.1 Залучення інформаційної безпеки в процес управління безперервністю бізнесу

Контроль

Для безперервності бізнесу в усій організації треба розробити та підтримувати процес, що управляється, який враховує вимоги інформаційної безпеки, необхідні для безперервності бізнесу в організації.

Настанова щодо впровадження

Процедура повинна зводити разом наведені нижче ключові елементи управління безперервністю бізнесу:

a) розуміння ризиків, з якими організація зустрічається, з точки зору ймовірності та впливу у часі, охоплюючи ідентифікацію та пріоритизацію (див. 14.1.2);

b) ідентифікація всіх активів, залучених у критичні бізнес-процеси (див. 7.1.1);

c) розуміння впливу, який переривання, спричинені інцидентами інформаційної безпеки, ймовірно, матимуть на бізнес (важливо віднайти рішення, які оброблятимуть як інциденти, що спричиняють менші впливи, так і серйозні

інциденти, котрі можуть загрожувати життєздатності організації), і встановлення цілей бізнесу щодо засобів обробки інформації;

d) розгляд придбання відповідної страховки, яка може як складати частину загального процесу безперервності бізнесу, так і бути частиною управління операційним ризиком;

e) ідентифікація та розгляд впровадження додаткових превентивних та послаблюючих контролів;

f) ідентифікація достатніх фінансових, організаційних, технічних та інфраструктурних ресурсів для урахування ідентифікованих вимог інформаційної безпеки;

g) забезпечення безпеки персоналу та захист засобів оброблення інформації і майна організації;

h) формулювання та документування планів безперервності бізнесу, які враховують вимоги інформаційної безпеки відповідно до погодженої стратегії безперервності бізнесу (див. 14.1.3);

i) регулярне тестування та оновлення наявних планів та процесів (див. 14.1.5);

j) забезпечення того, що управління безперервністю бізнесу вбудоване в процеси та структуру організації; відповідальність за процес управління безперервністю бізнесу повинна бути призначена на відповідному рівні в межах організації (див. 6.1.1).

14.1.2 Безперервність бізнесу та оцінка ризику

Контроль

Події, що можуть спричинити переривання в бізнес-процесах, повинні бути ідентифіковані разом з імовірністю та впливом таких переривань і їх наслідків для інформаційної безпеки.

Настанова щодо впровадження

Аспекти інформаційної безпеки щодо безперервності бізнесу повинні базуватися на ідентифікації подій (або послідовності подій), які можуть спричинити переривання бізнес-процесів організації, наприклад, відмова обладнання, людські помилки, крадіжка, пожежа, природні лиха та терористичні акти. Це має супроводжуватися оцінкою ризику для визначення ймовірності та впливу таких переривань з точки зору часу, шкали ушкоджень та періоду відновлення.

Оцінка ризику безперервності бізнесу повинна виконуватись з повним залученням власників бізнес-ресурсів та процесів. Ця оцінка повинна розглядати всі бізнес-процеси і не обмежуватись лише засобами оброблення інформації, а охоплювати результати, характерні для інформаційної безпеки. Важливо поєднати різні аспекти ризику для отримання повної картини вимог безперервності бізнесу організації. Оцінка повинна ідентифікувати, кількісно оцінювати і пріоритизувати ризики залежно від суттєвих для організації критеріїв та цілей, включаючи критичні ресурси, впливи порушень, припустимий час непрацездатності системи та пріоритети відновлення.

Залежно від результатів оцінки ризику повинна бути розроблена стратегія безперервності бізнесу для визначення загального підходу до безперервності бізнесу. Після створення цієї стратегії керівництво повинне її погодити, і повинний бути створений та погоджений план впровадження цієї стратегії.

14.1.3 Розроблення та впровадження планів безперервності бізнесу, які охоплюють інформаційну безпеку

Контроль

Повинні бути розроблені та впроваджені плани для підтримки або поновлення операцій і забезпечення доступності інформації на потрібному рівні та в потрібні проміжки часу після переривання чи відмови критичних бізнес-процесів.

Настанова щодо впровадження

Процес планування безперервності бізнесу повинен розглядати наведене нижче:

a) ідентифікацію та погодження всіх відповідальностей та процедур безперервності бізнесу;

b) ідентифікацію припустимих втрат інформації та обслуговування;

c) впровадження процедур, які уможливлюють відновлення та поновлення функціонування бізнесу і доступності інформації у потрібних масштабах часу; особливу увагу треба приділити оцінці внутрішніх та зовнішніх залежностей бізнесу та наявних контрактів;

d) функціональні процедури для супроводження незавершеного відновлення та поновлення;

e) документування погоджених процедур та процесів;

f) відповідну освіту штату щодо погоджених процедур та процесів, охоплюючи антикризове управління;

g) тестування та оновлення планів.

Процес планування повинен взяти до уваги необхідні цілі бізнесу, наприклад, поновлення певних комунікаційних послуг клієнтам у прийнятний час. Повинні бути ідентифіковані послуги та ресурси, які сприяють цьому, охоплюючи кадрове забезпечення, ресурси, що не обробляють інформацію, а також заходи з нейтралізації несправностей для засобів оброблення інформації. Такі заходи з нейтралізації несправностей можуть охоплювати заходи з третіми сторонами у вигляді двосторонніх угод або комерційні послуги приєднання.

Плани безперервності бізнесу повинні враховувати вразливості організації, і тому можуть містити чутливу інформацію, яка потребує відповідного захисту. Копії планів безперервності бізнесу повинні зберігатися у віддаленому місці на достатній відстані, щоб уникнути будь-якого ушкодження від лиха на основному місцезнаходженні. Керівництво повинне забезпечити актуальність копій планів безперервності бізнесу і захист з таким же рівнем безпеки, який застосовано на основному місцезнаходженні. Інші дані, необхідні для виконання планів безперервності, повинні також зберігатися у віддаленому місці.

Якщо використовуються альтернативні тимчасові місця, рівень

застосовуваних контролів безпеки для них повинен бути еквівалентним рівневі основного місця.

Додаткова інформація

Слід відзначити, що плани та дії з антикризового управління (див. 14.1.3 f) можуть відрізнятися від управління безперервністю бізнесу; тобто, може мати місце кризова ситуація, яка може врегульовуватися звичайними процедурами управління.

14.1.4 Структура планування безперервності бізнесу

Контроль

Для забезпечення несуперечливості всіх планів, несуперечливого врахування вимог інформаційної безпеки та ідентифікації пріоритетів тестування і підтримки, повинна підтримуватись єдина структура планів безперервності бізнесу.

Настанова щодо впровадження

Кожний план безперервності бізнесу повинен описувати підхід до безперервності, наприклад, підхід до забезпечення доступності та безпеки інформації та інформаційної системи. Кожний план повинен також визначати план ескалації та умови його активації, так само, як індивідуальну відповідальність за виконання кожної складової плану. Коли ідентифіковано нові вимоги, будь-які існуючі процедури аварійних дій, наприклад, плани евакуації або заходи з нейтралізації несправностей, повинні бути належним чином виправлені. Програми управління організаційними змінами повинні охоплювати процедури забезпечення того, що питання безперервності бізнесу завжди належним чином ураховані.

Кожний план повинен мати окремого власника. Процедури аварійних дій, плани з ручної нейтралізації несправностей та плани відбудовування повинні охоплюватися відповідальністю власників відповідних залучених бізнес-ресурсів або процесів. За заходи з нейтралізації несправностей альтернативних технічних послуг, таких як оброблення інформації та комунікаційні засоби зв’язку, повинні, як правило, бути відповідальні постачальники цих послуг.

Структура планування безперервності бізнесу повинна враховувати ідентифіковані вимоги інформаційної безпеки і розглядати наведене нижче:

a) умови активації планів, які описують процес, якому треба слідувати (наприклад, як оцінювати ситуацію, хто має бути залучений) до активації кожного плану;

b) процедури аварійних дій, що описують дії, яких треба вжити після інциденту, котрий наражає на небезпеку функціонування бізнесу;

c) процедури нейтралізації несправностей, які описують дії, яких треба вжити для переміщення суттєвої бізнес-діяльності чи послуг підтримки до альтернативних тимчасових місць і поновлення функціонування бізнес-процесів у потрібний проміжок часу;

d) тимчасові процедури функціонування для супроводження незавершеного відновлення та поновлення;

e) процедури відбудовування, які описують дії, що треба вжити для повернення до звичайного функціонування бізнесу;

f) графік підтримки, який визначає, як і коли план тестуватиметься, та процедуру підтримки плану;

g) діяльність з поінформовування, освіти та навчання, розроблена для створення розуміння процесів безперервності бізнесу та забезпечення того, що процес залишається ефективним;

h) відповідальності осіб, які описують, хто відповідальний за виконання якої складової плану. За необхідності повинні бути призначені заступники;

i) критичні активи та ресурси, які повинні бути здатні виконувати процедури аварійних дій, нейтралізації несправностей та відбудови.

14.1.5 Тестування, підтримування та переоцінка планів безперервності бізнесу

Контроль

Плани безперервності бізнесу треба регулярно тестувати та оновлювати, щоб забезпечити, що вони актуальні та ефективні.

Настанова щодо впровадження

Тестування плану безперервності бізнесу повинні забезпечувати, що всі члени команди відновлення та інший відповідний штат поінформовані щодо планів та своїх відповідальностей стосовно безперервності бізнесу та безпеки інформації і знають свою роль при здійсненні плану.

Графік тестування плану(ів) безперервності бізнесу повинний позначати, як і коли повинен тестуватися кожний елемент плану. Кожний елемент плану(ів) повинен тестуватися часто.

Щоб надати гарантію того, що план(и) будуть діяти в реальному житті, повинні використовуватися різноманітні методи. Вони повинні включати:

a) перевірку різних сценаріїв «на столі» (обговорення заходів відновлення бізнесу з використанням прикладів переривань);

b) моделювання (особливо, для навчання людей щодо їх ролей в післяінцидентному або післякризовому управлінні);

c) тестування технічного відновлення (пересвідчення, що інформаційні системи можуть бути ефективно поновлені);

d) тестування відновлення на додатковому місцезнаходженні (звичайний бізнес процес паралельно з операціями відновлення не на основному місці);

e) тестування засобів та послуг постачальника (пересвідчення, що надані ззовні послуги та продукція будуть відповідати контрактним зобов'язанням);

f) повні репетиції (тестування, що організація, персонал, обладнання, засоби та процеси можуть впоратися з перериваннями).

Ці методи можуть застосовуватися будь-якою організацією. Вони повинні застосовуватися у спосіб, який є суттєвим для конкретного плану відновлення. Результати тестів повинні записуватися та, за необхідності, вживатися дії для вдосконалення планів.

Повинна бути призначена відповідальність за регулярні перегляди кожного

плану безперервності бізнесу. За ідентифікацією змін у бізнес-заходах, які ще не відображено в планах безперервності бізнесу, повинне слідувати відповідне оновлення плану. Ця офіційно оформлена процедура контролю змін повинна забезпечити, що оновлені плани розповсюджуються та повторно вводяться в дію регулярними переглядами повного плану.

Прикладами змін, де повинне розглядатися оновлення планів безперервності бізнесу, є придбання нового обладнання, модернізація систем та зміни в:

a) персоналі;
b) адресах та номерах телефонів;
c) бізнес-стратегії;
d) розміщенні, засобах та ресурсах;
e) законодавстві;
f) контракторах, постачальниках та основних клієнтах;
g) процесах – нових, чи відмінених;
h) ризику (функціональному або фінансовому).

15 Відповідність

15.1 Відповідність правовим вимогам

Ціль: Уникнути порушень будь-якого закону, вимог, що діє на підставі закону, нормативних або контрактних зобов'язань та будь-яких вимог безпеки.

Предметом вимог, що діють на підставі закону, нормативних та контрактних вимог безпеки може бути проектування, функціонування, використання інформаційних систем та управління ними.

Рекомендації щодо певних правових вимог треба одержувати від юрисконсультів організації або практикуючих юристів, які мають належну кваліфікацію. Законодавчі вимоги у різних країнах відрізняються і можуть змінюватися для інформації, яку створено в одній країні та передають до іншої країни (тобто закордонного потоку даних).

15.1.1 Ідентифікація застосовного законодавства

Контроль

Усі суттєві 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.

Настанова щодо впровадження

Аналогічним чином повинні бути визначені та задокументовані певні контролі та індивідуальні відповідальності для задоволення цих вимог.

15.1.2 Права інтелектуальної власності (IPR)

Контроль

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.

Настанова щодо впровадження

Для захисту будь-яких матеріалів, які можна вважати інтелектуальною власністю, повинні розглядатися наведені нижче настанови:

a) публікація політики відповідності правам інтелектуальної власності, яка визначає правове використання програмного забезпечення та інформаційних продуктів;

b) придбання програмного забезпечення лише через відомі та визнані джерела, щоб забезпечити, що авторські права не порушуються;

c) підтримка поінформованості щодо політики захисту прав інтелектуальної власності та надання попередження про намір вжиття дисциплінарних дій проти персоналу, який їх порушує;

d) підтримка відповідних реєстрів активів та ідентифікація всіх активів з вимогами захисту прав інтелектуальної власності;

e) підтримка доказів та свідоцтв володіння ліцензіями, мастер-дисків, керівництв тощо;

f) запровадження контролів, щоб забезпечити, що не перевищена будь-яка кількість дозволених користувачів;

g) виконання перевірок, що інстальовано лише авторизоване програмне забезпечення та ліцензовані продукти;

h) надання політики підтримки належних умов ліцензування;

i) надання політики вилучення або передавання програмного забезпечення іншим;

j) використання належних інструментів аудиту;

k) відповідність термінам та умовам щодо програмного забезпечення та інформації, отриманих із загальнодоступних мереж;

l) відсутність відмінного від дозволеного авторським правом дублювання, перетворення в інший формат або виділення з комерційних записів (кіно, аудіо);

m) недопущення відмінного від дозволеного авторським правом повного або часткового копіювання книг, статей, звітів або інших документів.

Додаткова інформація

Права інтелектуальної власності включають авторське право на програмне забезпечення або документ, права на промисловий зразок, торгові марки, патенти та ліцензії на початковий текст.

Патентований програмний продукт зазвичай постачається згідно з ліцензійною угодою, яка визначає терміни та умови ліцензії, наприклад, обмеження використання продуктів визначеними комп'ютерами або обмеження копіювання створенням лише резервних копій. Ситуація з IPR стосовно програмного забезпечення, розробленого організацією, повинна бути пояснена штату.

Законодавчі, нормативні та контрактні вимоги можуть накладати обмеження на копіювання патентованих матеріалів. Зокрема, вони можуть вимагати, щоб можна було використовувати лише матеріал, розроблений організацією, або який ліцензовано чи надано організації розробником. Порушення авторського права може призвести до судового позову, який може залучати кримінальне переслідування.

15.1.3 Захист організаційних записів

Контроль

Відповідно до вимог, що діють на підставі закону, нормативних, контрактних і бізнес вимог, важливі записи повинні бути захищені від втрати, знищення та фальсифікації.

Настанова щодо впровадження

Записи повинні бути класифіковані за типами, наприклад, облікові записи, записи баз даних, журнали трансакцій, журнали аудиту та процедури функціонування, кожна з подробицями щодо періоду тривалого зберігання та типу запам'ятовуючого носія, наприклад, папір, мікрофіш, магнітний, оптичний.

Будь-які відповідні криптографічні ключові дані, а також програми, пов'язані з зашифрованими архівами або цифровими підписами (див. 12.3), для уможливлення розшифрування записів повинні також зберігатися протягом строку зберігання записів.

Треба розглянути можливість псування носіїв, використаних для зберігання записів. Процедури зберігання та оброблення повинні запроваджуватися відповідно до рекомендацій виробника. З метою довготермінового зберігання треба розглянути використання паперу та мікрофішів.

Там, де вибрані електронні засоби зберігання, для захисту від втрат через майбутні заміни техніки повинні бути наявними процедури забезпечення доступу до даних (до зчитування як носіїв, так і формату) протягом періоду тривалого збереження.

Системи зберігання даних повинні обиратися таким чином, щоб необхідні дані можна було віднайти у прийнятному форматі за прийнятний період часу та залежно від вимог, які повинні виконуватися.

Система зберігання та оброблення повинна забезпечувати чітку ідентифікацію записів та періоду їх тривалого зберігання, як визначено застосовним національним або регіональним законодавством чи нормативами. Ця система повинна дозволяти відповідне знищення записів після цього періоду, якщо вони непотрібні організації.

Для досягнення цих цілей захисту записів, в організації треба вжити наведені нижче кроки:

a) повинні бути видані настанови щодо тривалого зберігання, зберігання, оброблення та вилучення записів та інформації;

b) повинен бути складений графік тривалого зберігання, який ідентифікує записи і період часу, протягом якого вони повинні тривало зберігатися;

c) повинні підтримуватися інвентарні описи джерел ключової інформації;

d) повинні бути запроваджені належні контролі для захисту записів та інформації від втрати, знищення та фальсифікації.

Додаткова інформація

Деякі записи можуть потребувати безпечного тривалого зберігання для задоволення вимог, що діють на підставі закону, нормативних, контрактних вимог, а також для підтримки основної бізнес-діяльності. Прикладами є записи, які можуть знадобитися як докази функціонування організації в межах нормативних правил або правил, що діють на підставі закону, щоб забезпечити захист від потенційних громадянських чи кримінальних позовів, чи для підтвердження фінансового стану організації відносно акціонерів, зовнішніх сторін та аудиторів. Період часу та вміст даних для тривалого збереження інформації може встановлюватися національним законом або нормативами.

Подальшу інформацію стосовно управління організаційними записами можна знайти в ISO 15489-1.

15.1.4 Захист даних та приватність персональної інформації

Контроль

Захист даних і приватність повинні забезпечуватися згідно з вимогами відповідного законодавства, нормативів і, за наявності, статей контракту.

Настанова щодо впровадження

Повинна бути розроблена й запроваджена політика організації щодо захисту даних і приватності. Ця політика повинна бути доведена до відома всіх осіб, залучених до оброблення персональної інформації.

Відповідність цій політиці та всьому суттєвому законодавству й нормативам щодо захисту даних вимагає відповідної структури управління та контролю. Часто найкраще цього досягають шляхом призначення відповідальної особи, як, наприклад, службовця із захисту даних, який повинен надавати настанови для керівників, користувачів та постачальників послуг щодо їх особистої відповідальності і певних процедур, яким треба слідувати. Відповідальність за оброблення персональної інформації та забезпечення поінформованості щодо принципів захисту даних повинна здійснюватися згідно з відповідним законодавством та нормативами. Повинні бути запроваджені відповідні технічні та організаційні заходи для захисту персональної інформації.

Додаткова інформація

Багато країн ввело законодавство, яке встановлює контролі збирання, оброблення та передавання персональних даних (взагалі інформацію щодо існуючих осіб, які можуть бути ідентифіковані за цією інформацією). Залежно від відповідного національного законодавства такі контролі можуть накладати обов’язки на тих, хто збирає, обробляє та поширює персональну інформацію, а можуть обмежувати можливість передавання таких даних до інших країн.

15.1.5 Запобігання зловживанню засобами оброблення інформації

Контроль

Треба утримувати користувачів від використання засобів оброблення інформації для неавторизованих цілей.

Настанова щодо впровадження

Керівництво повинне затвердити використання засобів оброблення інформації. Будь-яке не затверджене керівництвом використання цих засобів не для цілей бізнесу (див. 6.1.4) або для будь-яких неавторизованих цілей повинне розглядатись як неналежне використання засобів оброблення. Якщо будь-яку неавторизовану діяльність ідентифіковано моніторингом або іншими способами, на таку діяльність треба звернути увагу певного керівника, який забезпечує розгляд належних дисциплінарних та/або правових дій.

До запровадження процедур моніторингу треба отримати правові рекомендації.

Усі користувачі повинні бути поінформовані щодо точної галузі застосування дозволеного їм доступу та щодо наявності моніторингу для

виявлення неавторизованого використання. Цього можна досягти наданням користувачам письмової авторизації, копія якої повинна бути підписана користувачем і безпечно тривало зберігатися організацією. Найманий персонал організації, контракторів та користувачів третьої сторони треба сповістити, що ніякий доступ не буде дозволений, крім авторизованого.

При реєстрації повинне бути надане застережне повідомлення для зазначення, що засіб оброблення інформації, з яким розпочато роботу, належить організації, та що неавторизований доступ не дозволяється. Користувач повинен підтвердити і відповідно відреагувати на повідомлення на екрані для продовження процедури реєстрації (див. 11.5.1).

Додаткова інформація

Засоби оброблення інформації організації призначені головним чином або виключно для цілей бізнесу.

Виявлення вторгнення, перевірка вмісту та інші інструменти моніторингу можуть допомогти запобігти та виявити зловживання засобами оброблення інформації.

Багато країн мають законодавство для захисту від зловживання комп'ютерами. Використання комп'ютера для неавторизованих цілей може бути кримінальним злочином.

Законність моніторингу використання відрізняється в різних країнах і може вимагати від керівництва сповіщення всіх користувачів щодо такого моніторингу та/або отримання їх згоди. Там, де система, з якою розпочато роботу, використовується для загального доступу (наприклад, загальнодоступний веб-сервер) і є об'єктом моніторингу безпеки, повинне бути показане повідомлення про це.

15.1.6 Нормативи щодо криптографічних контролів

Контроль

Криптографічні контролі повинні використовуватися відповідно до усіх застосовних угод, законів та нормативів.

Настанова щодо впровадження

Для відповідності усім застосовним угодам, законам та нормативам треба розглянути наведені нижче позиції:

a) обмеження імпорту та експорту комп'ютерних апаратних засобів та програмного забезпечення для виконання криптографічних функцій;

b) обмеження імпорту та експорту комп'ютерних апаратних засобів та програмного забезпечення, розроблених для долучення в них криптографічних функцій;

c) обмеження використання шифрування;

d) обов'язкові або віддані на розсуд методи доступу повноважних органів країни до інформації, зашифрованої за допомогою апаратних або програмних засобів для забезпечення конфіденційності вмісту.

Для забезпечення відповідності національним законам та нормативам

повинні бути отримані правові рекомендації. До того, як передати зашифровану інформацію або криптографічні контролі до іншої країни, також повинні бути отримані правові рекомендації.

15.2 Відповідність політикам та стандартам безпеки і технічна відповідність

Ціль: Забезпечити відповідність систем політикам та стандартам безпеки організації.

Безпека інформаційних систем повинна регулярно переглядатися.

Такі перегляди повинні здійснюватися згідно з належними політиками безпеки та технічними платформами, і повинен виконуватися аудит інформаційних систем на відповідність застосовним стандартам запровадження безпеки та задокументованим контролям безпеки.

15.2.1 Відповідність політикам та стандартам безпеки

Контроль

Для досягнення відповідності політикам та стандартам безпеки керівники повинні забезпечити, що всі процедури безпеки в межах сфери їх відповідальності виконуються коректно.

Настанова щодо впровадження

Керівники повинні в межах сфери їх відповідальності регулярно переглядати відповідність оброблення інформації належним політикам безпеки, стандартам та будь-яким іншим вимогам безпеки.

Якщо в результаті перегляду виявлено будь-яку невідповідність, керівники повинні:

a) визначити причини невідповідності;

b) оцінити потребу в діях, щоб забезпечити, що невідповідність не повториться;

c) визначити та впровадити належну коригувальну дію;

d) здійснити перегляд вжитої коригувальної дії.

Результати перегляду і коригувальних дій, виконаних керівниками, повинні реєструватися, а ці записи повинні підтримуватися. Керівники повинні звітувати про результати особам, які проводять незалежні перегляди (див. 6.1.8), якщо незалежний перегляд має місце в сфері їх відповідальності.

Додаткова інформація

Моніторинг функціонування системи міститься в 10.10.

15.2.2 Перевірка технічної відповідності

Контроль

Інформаційні системи повинні регулярно перевірятися на відповідність стандартам впровадження безпеки.

Настанова щодо впровадження

Перевірка технічної відповідності повинна здійснюватися або вручну (за підтримки, якщо необхідно, належних інструментів програмного забезпечення) досвідченим системним інженером, та/або за допомогою автоматизованого інструментарію, який генерує технічний звіт для подальшої інтерпретації технічним спеціалістом.

Якщо використовують тестування на проникнення або оцінка вразливості, повинна бути виявлена обачність, оскільки такі дії можуть призвести до компрометації безпеки системи. Такі тестування повинні бути запланованими, задокументованими та повторюваними.

Будь-яка перевірка технічної відповідності повинна виконуватися лише компетентними авторизованими особами або під наглядом таких осіб.

Додаткова інформація

Перевірка технічної відповідності включає обстеження операційних систем, щоб забезпечити, що контролі апаратного та програмного забезпечення впроваджено коректно. Такий вид перевірки відповідності потребує експертизи технічного спеціаліста.

Перевірка відповідності також включає, наприклад, тестування на проникнення і оцінку вразливостей, які можуть здійснюватися незалежним експертом, з яким укладено контракт спеціально для цих цілей. Це може бути корисним при виявленні вразливостей в системі та для перевірки, наскільки ефективними є контролі запобігання неавторизованому доступу внаслідок цих вразливостей.

Тестування на проникнення та оцінка вразливостей надає миттєвий знімок системи у певному стані в певний час. Миттєвий знімок обмежено тими частинами системи, які дійсно тестувалися під час спроб(и) проникнення. Тестування на проникнення та оцінка вразливостей не замінює оцінку ризику.

15.3 Розгляд аудиту інформаційних систем

Ціль: Мінімізувати втручання в процес аудиту інформаційних систем та максимізувати ефективність цього процесу.

Повинні бути контролі, щоб убезпечити операційні системи та інструменти аудиту під час аудитів інформаційних систем

Захист також потрібний для убезпечення цілісності та попередження зловживання інструментами аудиту.

15.3.1 Контролі аудиту інформаційних систем

Контроль

Вимоги аудиту та діяльність, що охоплює перевірки операційних систем, повинні бути ретельно сплановані та погоджені, щоб мінімізувати ризик порушення бізнес-процесів.

Настанова щодо впровадження

Треба звернути увагу на наведені нижче настанови:

a) вимоги аудиту повинні бути погоджені з відповідним керівництвом;

b) галузь застосування перевірок повинна бути погодженою та контрольованою;

c) перевірки повинні обмежуватися доступом до програмного забезпечення та даних тільки для читання;

d) доступ не тільки для читання повинен дозволятися лише до окремих копій системних файлів, які після завершення аудиту повинні знищуватися, або їм повинен надаватися належний захист, якщо є зобов'язання щодо зберігання таких файлів згідно з вимогами до документування аудитів;

e) ресурси для виконання перевірок повинні чітко ідентифікуватися і робитися доступними;

f) вимоги щодо спеціального або додаткового оброблення повинні бути визначені та погоджені;

g) треба здійснювати моніторинг усякого доступу та реєструвати його для генерації журналу посилань; для критичних даних або систем треба розглянути використання журналу посилань з позначкою часу;

h) усі процедури, вимоги та відповідальності повинні бути задокументовані;

i)особа(и), яка здійснює(-ють) аудит, повинна(і) бути незалежними від діяльності, щодо якої аудит здійснюється.

15.3.2 Захист інструментів аудиту інформаційних систем

Контроль

Доступ до інструментів аудиту інформаційних систем повинен бути захищений, щоб запобігти будь-якому можливому зловживанню чи компрометації.

Настанова щодо впровадження

Інструменти аудиту інформаційних систем, наприклад, програмне забезпечення або файли даних, повинні бути відокремлені від систем розроблення та працюючих систем і не повинні утримуватися в бібліотеках магнітних стрічок або користувацьких зонах, доки не буде надано належний рівень додаткового захисту.

Додаткова інформація

Якщо до аудиту залучено треті сторони, може бути ризик зловживання цими третіми сторонами інструментами аудиту і ризик доступу до інформації організації цієї третьої сторони. Для урахування цих ризиків можуть бути розглянуті такі контролі, як 6.2.1 (для оцінки ризиків) та 9.1.2 (для обмеження фізичного доступу), а також треба вжити подальші дії, такі, як негайна зміна паролів, розкритих аудиторам.

Бібліографія

ISO/IEC Guide 2:1996, Standardization and related activities - General vocabulary

ISO/IEC Guide 73:2002, Risk management - Vocabulary - Guidelines for use in standards

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

ISO/IEC TR 13335-3:1998, Information technology - Guidelines for the Management of IT Security - Part 3: Techniques for the Management of IT Security

ISO/IEC 13888-1:1997, Information technology - Security techniques - Non-repudiation - Part 1: General

ISO/IEC 11770-1:1996 Information technology - Security techniques - Key management - Part 1: Framework

ISO/IEC 9796-2:2002 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms

ISO/IEC 9796-3:2000 Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms

ISO/IEC 14888-1:1998 Information technology - Security techniques - Digital signatures with appendix - Part 1: General

ISO/IEC 15408:1:1999 Information technology - Security techniques - Evaluation Criteria for IT security - Part 1: Introduction and general model

ISO/IEC 14516:2002 Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services

ISO 15489-1:2001 Information and documentation - Records management - Part 1: General

ISO 10007:2003 Quality management systems - Guidelines for configuration management

ISO/IEC 12207:1995 Information technology - Software life cycle processes

ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing

OECD Guidelines for the Security of Information Systems and Networks: ‘Towards a culture of security’. 2002

OECD Guidelines for Cryptography Policy, 1997

IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

ISO/IEC 18028-4 Information technology - Security techniques - IT Network security - Part 4: Securing remote access

ISO/IEC TR 18044 Information technology - Security techniques - Information security incident management

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ**.**

ISO/IEC Guide 2:1996 Стандартизація та пов’язана з нею діяльність - Загальний словник

ISO/IEC Guide 73:2002, Управління ризиком - Словник – Настанови із використання в стандартах

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

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

ISO/IEC 13888-1:1997, Інформаційні технології - Методи захисту - Неспростовність - Частина 1: Загальні положення

ISO/IEC 11770-1:1996 Інформаційні технології - Методи захисту - Управління ключами - Частина 1: Інфраструктура

ISO/IEC 9796-2:2002 Інформаційні технології - Методи захисту - Схеми цифрового підпису з відновленням повідомлення - Частина 2: Механізми, основані на факторизації цілого числа

ISO/IEC 9796-3:2000 Інформаційні технології - Методи захисту - Схеми цифрового підпису з відновленням повідомлення - Частина 3: Механізми, основані на дискретному логарифмі

ISO/IEC 14888-1:1998 Інформаційні технології - Методи захисту - Цифрові

підписи з додатком - Частина 1: Загальні положення

ISO/IEC 15408:1:1999 Інформаційні технології - Методи захисту - Критерії оцінювання безпеки ІТ - Частина 1: Вступ та загальна модель

ISO/IEC 14516:2002 Інформаційні технології - Методи захисту – Настанови з використання та управління послугами третьої довіреної сторони

ISO 15489-1:2001 Інформація та документація - Управління записами - Частина 1: Загальні положення

ISO 10007:2003 Системи управління якістю - Настанови щодо управління конфігурацією

ISO/IEC 12207:1995 Інформаційні технології - Процеси життєвого циклу програмного забезпечення

ISO 19011:2002 Настанови з аудиту систем управління якістю та/або довкіллям

OECD Настанови OECD стосовно безпеки інформаційних систем та мереж: „До культури безпеки”

OECD Настанови OECD щодо криптографічної політики

IEEE P1363-2000: Стандартні специфікації криптографії відкритого ключа

ISO/IEC 18028-4 Інформаційні технології - Методи захисту - Безпека мереж ІТ - Частина 4: Убезпечення віддаленого доступу

ISO/IEC TR 18044 Інформаційні технології - Методи захисту - Управління інцидентом інформаційної безпеки

АЛФАВІТНИЙ ПОКАЖЧИК

А

Б

В

Д

Е

З

І

К

	діловою безперервністю 14
	доступом користувача 11.2
	замінюваними носіями 10.7.1
	змінами 10.1.2
	змінами до послуг третьої особи 10.2.3
	зобов’язання щодо інформаційної безпеки 6.1.1
	інцидентами інформаційної безпеки 13, 13.2
	комунікаціями та роботою 10
	криптографічними ключами 12.3.2
	можливостями 10.3.1
	обов’язками 8.2.1
	паролями користувача 11.2.3
	переважним доступом 11.2.2
	системою паролів 11.5.3
	технічними уразливостями 12.6
управління ключами 12.3.2	
управління комунікаціями та роботою 10	
управління можливостями 10.3.1	
управління підключенням мереж 11.4.6	
кімнати, офіси та обладнання, захищені 8.1.1	
класифікація	
	інформації 7.2
	рекомендації 7.2.1
клієнти, засоби безпеки при справі 6.2.2	
код джерела, контроль доступу 12.4.3	
компетентність, розуміння та навчання щодо інформаційної безпеки 8.2.2	
контактування	
	з групами особливого інтересу 6.1.7
	з органами влади 6.1.6
Моніторинг 10.10	
	використання системи 10.10.2
	та перегляд послуг третьої особи 10.2.2
конфіденційність 2.5	
користувач	
	залишене без нагляду обладнання 11.3.2
	ідентифікація для зовнішніх з’єднань 11.4.2
	ідентифікація та підтвердження автентичності 11.5.2
	контроль доступу 11.2
	управління паролем 11.2.3
	обов’язки 11.3
	права доступу, перегляд 11.2.4
	реєстрація 11.2.1
криптографічні контролі 12.3	
	політика використання 12.3.1
	упорядкування 15.1.6

Л

М

Н

О

П

Р

С

Т

У

Ф

Код УКНД 35.040