Практична робота 8. Стандартизація в галузі інформаційної безпеки

Теоретичні відомості

ISO/IEC 27001 – міжнародний стандарт в галузі IT, назва якого «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» (Information technology – Security techniques – Information security management systems – Requirements).

ISO/IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації. Він також включає в себе вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації. Вимоги, викладені в ISO/IEC 27001 є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру.

ISO/IEC 27002 – стандарт інформаційної безпеки, опублікований організаціями ISO і IEC. Він має назву Інформаційні технології – Технології безпеки – Практичні правила менеджменту інформаційної безпеки (Information technology – Security techniques – Code of practice for information security management). До 2007 року цей стандарт називався ISO/IEC 17799.

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

Розглянемо приклади вразливостей інформаційної безпеки, які можуть бути використані для реалізації відповідних загроз для організації (табл. 7.1).

Таблиця 7.1 – Приклади загроз інформаційної безпеки

Приклади загроз	Приклади вразливостей
Фізичне пошкодження/втрата обладнання/інформації від пожежі	– Відсутність пожежної сигналізації – Відсутність системи пожежогасіння – Наявність легкозаймистих матеріалів – Неякісна електропроводка – Відсутність захисту від блискавки – Неконтрольований ремонт – Наявність зловмисного підпалювача – Халатність персоналу – Необізнаність персоналу – Злочинні дії
Фізичне пошкодження/втрата обладнання/інформації від пошкодження водою/повінню	– Невдале розташування будівлі – Невдале розміщення обладнання у підвальному приміщенні/на перших поверхах будівлі – Приміщення в аварійному стані – Неякісна каналізаційна система
Фізичне пошкодження/втрата обладнання/інформації – від техногенної аварії	– Наявність будівництва поряд – Старе приміщення (в аварійному стані) – Неякісна каналізаційна система – Відсутність контролю системи електроживлення – Відсутність резервних джерел електроживлення – Відсутність резервних каналів зв’язку – Відсутність резервного обладнання – Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата обладнання/інформації від крадіжки	– Неефективна система охорони – Недостатній контроль за переміщенням майна – Недбалість персоналу – Неправильний підбор персоналу – Необізнаність персоналу – Відсутність резервного обладнання/програмного забезпечення
Фізичне пошкодження/втрата обладнання/інформації від кліматичних та метеорологічних явищ	– Старе приміщення (в аварійному стані) – Неякісна каналізаційна система – Відсутність контролю системи електроживлення – Відсутність резервних джерел електроживлення – Відсутність резервних каналів зв’язку – Відсутність резервного обладнання – Відсутність віддаленого резервного пункту

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Фізичне пошкодження/втрата обладнання/інформації від електромагнітної радіації	– Відсутність екранування серверного приміщення – Чутливість обладнання до електромагнітної радіації – Неефективна охорона
Часткове/повне пошкодження /втрата обладнання/даних від збоїв електроживлення	– Неправильний розрахунок необхідної потужності електроживлення – Відсутність контролю та моніторингу системи електроживлення – Відсутність резервних джерел електроживлення – Відсутність резервного обладнання – Відсутність або недостатність вимог з інформаційної безпеки в угодах з третіми сторонами – Неефективне обслуговування обладнання працівниками третіх сторін або персоналом банку
Часткове/повне пошкодження /втрата обладнання/даних від недбалості персоналу	– Недосвідченість персоналу – Відсутність системи моніторингу роботи IT інфраструктури – Неефективна охорона – Відсутність контролю за переміщенням майна – Відсутність або недостатність тестування обладнання/програмного забезпечення – Можливість використання обладнання/програмного забезпечення не за призначенням – Неефективне розмежування прав доступу до програмного забезпечення/даних – Недостатня захищеність вузла доступу до загальних мереж (Інтернет) від зовнішніх зловмисників – Недостатньо ефективна система розподілу прав доступу до інформації – Невихід із системи під час залишення працівником робочого місця – Передача/втрата контролю за носіями криптографічних ключів – Передача/компрометація паролів доступу – Передача або повторне використання середовища збереження даних без знищення інформації – Невиконання процедур резервного копіювання – Незахищене зберігання даних/документів – Неконтрольоване копіювання інформації

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Часткове/повне пошкодження /втрата даних від відмови телекомунікаційного обладнання	– Відсутність резервних каналів зв'язку – Відсутність резервного телекомунікаційного обладнання – Недбалість персоналу – Необізнаність персоналу – Відсутність або недостатність вимог безпеки в угодах з провайдерами зв'язку – Зловмисні дії персоналу провайдерів зв'язку – Погане з'єднання та розміщення кабелів – Наявність єдиної точки відмови
Часткове/повне пошкодження /втрата даних від порушення експлуатації обладнання/ програмного забезпечення	– Необізнаність персоналу – Відсутність системи моніторингу роботи IT інфраструктури – Недосконала IT система – Ускладнений інтерфейс користувача – Відсутність документації – Недосконале або нове програмне забезпечення – Відсутність або недостатність тестування обладнання/програмного забезпечення – Відсутність перевірки цілісності програмного забезпечення під час його запуску – Можливість використання обладнання/програмного забезпечення не за призначенням – Неефективне розмежування прав доступу до програмного забезпечення/даних – Наявність єдиної точки відмови
Часткове/повне пошкодження /втрата даних від неавторизованого використання обладнання/програмного забезпечення	– Відсутність контролю за використанням обладнання/програмного забезпечення – Відсутність контролю за внесенням змін до складу обладнання/програмного забезпечення – Наявність незахищеного з'єднання з публічними мережами – Відсутність політик використання обладнання/програмного забезпечення – Неефективне розмежування прав доступу до програмного забезпечення/обладнання – Неефективна політика управління мережею

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Часткове/повне пошкодження /втрата даних від збою обладнання/програмного забезпечення	– Відсутність плану забезпечення безперервної роботи – Необізнаність персоналу – Відсутність системи моніторингу роботи IT інфраструктури – Недосконале або нове програмне забезпечення – Відсутність контролю цілісності програмного забезпечення під час його запуску – Відсутність або недостатність тестування обладнання/програмного забезпечення – Можливість використання обладнання/програмного забезпечення не за призначенням – Неефективне розмежування прав доступу до програмного забезпечення/даних – Наявність єдиної точки відмови – Відсутність або недосконаліть системи резервного копіювання інформації – Відсутність резервного обладнання – Неадекватне реагування для підтримки сервісів – Відсутність або недосконаліть угоди про рівень обслуговування третіми сторонами
Часткове/повне пошкодження /втрата даних від неправильного використання обладнання/ програмного забезпечення	– Необізнаність персоналу – Відсутність системи моніторингу роботи IT інфраструктури – Недосконала IT система – Ускладнений інтерфейс користувача – Відсутність документації – Недосконале або нове програмне забезпечення – Відсутність або недостатність тестування обладнання/програмного забезпечення – Можливість використання обладнання/програмного забезпечення не за призначенням – Неефективне розмежування прав доступу до програмного забезпечення/даних – Відсутність або недосконаліть системи резервного копіювання інформації – Відсутність резервного обладнання – Неадекватне реагування для підтримки сервісів

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Компрометація інформації за допомогою віддаленого шпигунства	– Небезпечна архітектура мережі – Відсутність або неефективність ідентифікації та аутентифікації користувача – Передавання паролів у відкритому вигляді – Незахищене з'єднання з публічними мережами – Недостатній контроль за функціонуванням та управлінням мережею – Недостатня обізнаність персоналу у питаннях інформаційної безпеки
Компрометація інформації за допомогою підслуховування	– Наявність незахищених комунікаційних ліній – Відсутність процедури безпечного проведення нарад – Наявність незахищеного конфіденційного трафіку – Необізнаність персоналу
Компрометація інформації за допомогою відновлення середовища, що повторно використовується	– Відсутність процедури знищення інформації – Необізнаність персоналу – Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за допомогою розкриття/ продажу інформації працівниками	– Неправильний підбір персоналу – Необізнаність персоналу у питаннях інформаційної безпеки – Відсутність класифікації інформації – Відсутність затвердженої процедури поводження з інформацією з обмеженим доступом – Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки – Незахищене з'єднання з публічними мережами – Відсутність контролю за роботою електронної пошти – Відсутність або неефективність ідентифікації та аутентифікації користувача – Недостатній контроль за функціонуванням та управлінням мережею – Неефективне розмежування прав доступу до програмного забезпечення/даних

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Компрометація інформації за допомогою нелегального оброблення даних	– Неправильний підбір персоналу – Відсутність або неефективність ідентифікації та аутентифікації користувача – Доступність сервісів, в яких немає необхідності – Недостатній контроль за функціонуванням та управлінням мережею – Неефективне розмежування прав доступу до програмного забезпечення/даних – Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки – Відсутність ефективної процедури моніторингу дій користувачів – Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	– Необізнаність персоналу – Відсутність або неефективність навчання персоналу – Ускладнений інтерфейс користувача – Доступність сервісів, в яких немає необхідності – Відсутність документації – Неефективне розмежування прав доступу до програмного забезпечення/даних – Відсутність ефективної процедури моніторингу дій користувачів – Відсутність записів про роботу користувачів в журналах аудиту – Підробка програмного забезпечення
Компрометація інформації за рахунок неправильної роботи системи захисту інформації	– Помилки під час проектування та розроблення системи захисту інформації – Відсутність документації – Необізнаність персоналу – Відсутність або неефективність навчання персоналу – Ускладнений інтерфейс користувача – Відсутність контролю цілісності системи захисту інформації під час її запуску/ініціалізації – Відсутність записів про роботу системи захисту в журналах аудиту

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Компрометація інформації за рахунок навмисного невикористання системи захисту інформації	– Помилки під час проектування та розроблення системи захисту інформації – Відсутність записів про роботу системи захисту в журналах аудиту – Неправильний підбір персоналу – Відсутність регулярних аудитів – Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за рахунок компрометації паролів доступу	– Необізнаність персоналу – Порушення персоналом правил зберігання паролів – Доступність сервісів, в яких немає необхідності – Наявність незахищених таблиць паролів – Недосконале управління паролями доступу – Відсутність формальної процедури перегляду прав доступу користувачів – Неефективне розмежування прав доступу до програмного забезпечення/даних – Відсутність або неефективність процедур контролю прав доступу – Відсутність регулярних аудитів – Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки – Відсутність ефективної процедури моніторингу дій користувачів – Відсутність записів про роботу користувачів в журналах аудиту
Викривлення/підробка інформації/даних за рахунок помилок програмного забезпечення	– Помилки під час проектування та розробки програмного забезпечення в питаннях використання системи криптографічного захисту інформації – Невикористання електронного цифрового підпису для захисту цілісності електронних документів – Відсутність перевірки електронного цифрового підпису під час роботи з електронними документами, які зберігаються в базах/сховищах даних – Відсутність записів про роботу системи захисту в журналах аудиту – Відсутність документації – Ускладнений інтерфейс користувача

Продовження таблиці 7.1

Приклади загроз	Приклади вразливостей
Неправильна робота системи захисту інформації	– Помилки під час проектування та розроблення системи захисту інформації – Невикористання електронного цифрового підпису для захисту цілісності електронних документів – Відсутність документації – Необізнаність персоналу – Відсутність або неефективність навчання персоналу – Ускладнений інтерфейс користувача – Відсутність записів про роботу системи захисту в журналах аудиту
Компрометація/передача особистих ключів електронного цифрового підпису	– Помилки під час проектування та розроблення системи захисту інформації – Помилки під час генерації ключів, в тому числі генерація ключів без паролю – Неефективна процедура розповсюдження ключів – Відсутність документів стосовно поводження з ключами електронного цифрового підпису для користувачів – Відсутність записів про роботу системи захисту в журналах аудиту – Відсутність регулярних аудитів – Відсутність належного визначення відповідальності за інформаційну безпеку – Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки

Хід роботи

1. Ознайомитися з теоретичними матеріалами та стандартами.
2. Дайте відповідь на питання:
   – Для чого потрібна стандартизація в галузі інформаційної безпеки?
   – Які виділяють найпоширеніші види загроз інформаційної безпеки?
3. Визначити основні вразливості та можливі варіанти їх вирішення для вказаної викладачем організації. Вказати джерела цих загроз.