Додаток
до розпорядження голови
районної в місті ради
від 17.09.2015 № 194-р

ПОЛОЖЕННЯ
про придбання, розробку та обслуговування інформаційних систем

ЗМІСТ

1. Загальні положення

Метою даного Положення є забезпечення впевненості в тому, що безпека є невід'ємною властивістю інформаційних систем, які впроваджують, і забезпечити виконання вимог щодо безпеки під час їх розроблення та експлуатації.

Положення розповсюджується на всі структурні підрозділи виконкому.

Відповідальність за контролювання процесів придбання, розробки

та обслуговування інформаційних систем, а також за контролювання дотримання вимогам даного Положення несе керуючий справами виконкому Довгинцівської районної в місті ради.

Розподіл відповідальності за виконання кожним із процесів придбання, розробки та обслуговування інформаційних систем визначається посадовими інструкціями та розпорядженнями голови районної в місті ради.

При використанні нормативних документи, посилання на які є в даному положенні, необхідно застосовувати актуальні редакції цих документів.

2. Терміни та визначення

В даному положенні використовуються терміни та визначення понять згідно ДСТУ ISO/IEC 27001:2010 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», а також такі:

Валідація – процес, що дозволяє визначити, наскільки точно з позицій потенційного користувача деяка модель представляє задані сутності реального світу.

Додаток (застосунок, застосовна програма, прикладна програма) – користувацька комп'ютерна програма, що дає змогу вирішувати конкретні прикладні задачі користувача.

Інформаційна система – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

Криптографічний захист інформації – вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Сальдо – різниця між надходженнями і витратами за певний проміжок часу.

Сирцевий код – будь-який набір інструкцій або оголошень, написаних комп'ютерною мовою програмування і у формі, що її може прочитати і модифікувати людина.

3. Нормативні посилання

ДСТУ ISO/IEC 27001:2010 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».

ISO/IEC 15408-1:2009 «Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model».

ISO/IEC 27005:2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

ISO/IEC 11770-1:2010 «Information technology - Security techniques - Key management - Part 1: Framework».

ISO/IEC 9796-2:2010 «Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации».

ISO/IEC 9796-3:2006 «Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма.

ISO/IEC 14888-1:2008 «Information technology - Security techniques - Digital signatures with appendix -- Part 1: General».

ISO/IEC 14888-2:2008 «Information technology - Security techniques -- Digital signatures with appendix - Part 2: Integer factorization based mechanisms».

ISO/IEC 14888-3:2006 «Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms».

4. Придбання, розробка та обслуговування інформаційних систем

4.1. Вимоги захисту інформаційних систем

Інформаційні системи включають операційні системи, інфраструктуру, додатки, готові продукти, послуги, а також додатки, розроблені користувачем. Проектування і реалізація інформаційних систем, підтримуючих організаційний процес, можуть бути вирішальними для захисту. Перед розробкою та / або реалізацією інформаційних систем повинні бути визначені та погоджені вимоги захисту.

Всі вимоги захисту повинні бути виявлені на стадії визначення вимог проекту та обґрунтовані, узгоджені і документально підтверджені як частина загального економічного обґрунтування проекту для інформаційної системи.

4.1.1. Аналіз та специфікація вимог захисту засобів управління

Формулювання вимог для нових інформаційних систем, або поліпшення існуючих інформаційних систем повинні специфікувати вимоги для засобів управління захистом.

Специфікація вимог для засобів управління повинна враховувати автоматизовані засоби управління, які потрібно впровадити в інформаційну систему, і потреби в допоміжних ручних засобах управління. Аналогічні дії повинні враховуватися при оцінці пакетів програм, розроблюваних або придбаних для додатків.

Вимоги захисту та засобів управління повинні відображати ділову цінність залучених інформаційних активів і можливий збиток для виконкому, який може відбутися в результаті збою в захисті або відсутності захисту.

Системні вимоги для захисту інформації та процесів реалізації за-

хисту повинні бути інтегровані на ранніх стадіях проектування інформаційних систем. Засоби управління, введені на стадії проектування, значно дешевше для реалізації й обслуговування, ніж ті, які включені в ході реалізації або після реалізації.

Якщо продукти купуються, то необхідно слідувати офіційному процесу випробування і придбання. У договорах з постачальником повинні бути обумовлені певні вимоги захисту. Якщо функціональність захисту в пропонованому продукті не задовольняє встановленим вимогам, тоді ризик, що привноситься, і пов'язані з ним засоби управління мають бути переглянуті до придбання продукту. Якщо поставляються додаткові функціональні можливості і вони є причиною ризику для системи захисту, то вони повинні бути блоковані, або пропонована схема управління повинна бути переглянута, з метою визначити, чи може бути вилучено перевагу з наявної поліпшеної функціональності.

Якщо це буде визнано доречним, наприклад, з причини вартості, керівництво може захотіти використовувати незалежно оцінені та сертифіковані продукти. Додаткову інформацію про критерії оцінки для засобів захисту в області інформаційних технологій можна знайти в ISO/IEC 15408-1 або в інших стандартах з оцінки або сертифікації, за обставинами.

У технічному звіті ISO/IEC 27005 дано керівні вказівки по використанню процесів менеджменту ризиків для визначення вимог для засобів управління захистом.

4.2. Правильна обробка в додатках

Для забезпечення правильної обробки в додатках, включаючи додатки, розроблені користувачем, повинні бути спроектовані відповідні засоби управління. Ці засоби управління повинні включати валідацію вхідних даних, внутрішньої обробки і вихідних даних.

Додаткові засоби керування можуть бути необхідні для систем, які обробляють важливу, цінну або критичну інформацію, або мають вплив на таку інформацію. Такі засоби управління мають бути визначені на основі вимог захисту та оцінки ризиків.

4.2.1. Валідація вхідних даних засобу управління

Повинна здійснюватися валідація даних, які вводяться в додатки, з метою гарантування того, що ці дані є правильними і доречними.

Перевірки повинні застосовуватися до вхідних даних ділових угод, незмінних даних і таблиць. Повинні бути розглянуті наступні керівні вказівки:

1. Подвійне введення або інші перевірки вхідних даних, такі як граничні перевірки або обмеження полів конкретними діапазонами вхідних даних для того, щоб виявляти такі помилки:

- значення поза діапазону;
- невірні символи в полях даних;
- припущення або неповні дані;
- перевищення верхніх і нижніх меж обсягу даних;

- недозволені або суперечливі контрольні дані.

2. Періодичний аналіз вмісту ключових областей або файлів даних для того, щоб підтвердити їх достовірність та цілісність.

3. Контроль твердих копій вхідних документів на предмет будь-яких недозволених змін (всі зміни у вхідних документах повинні бути дозволені).

4. Процедури для реакції на помилки, виявлені валідацією.

5. Процедури для перевірки правдоподібності вхідних даних.

6. Визначення обов'язків всього персоналу, залученого в процес введення даних.

7. Створення журналу реєстрації діяльності, пов'язаної з процесом введення даних.

Можна розглянути автоматичне обстеження і валідацію вхідних даних, якщо це застосовно, для того, щоб знизити ризики помилок і запобігти стандартні атаки, включаючи переповнювання буфера і введення коду.

4.2.2. Управління внутрішньої обробкою

У додатки повинні бути вбудовані валідаційні перевірки, з метою запобігання будь-якого псування інформації внаслідок помилок обробки або умисних дій.

Проектування та реалізація програм слід забезпечувати, щоб ризики збоїв в обробці, що призводять до втрати цілісності, були мінімізовані. Конкретні області, які треба розглянути, включають наступне:

- використання функцій додавання, модифікації і видалення для того, щоб здійснювати зміни в даних;

- процедури для запобігання роботи програм в неправильному порядку або роботи після збою попередньої обробки;

- використання підходящих програм для того, щоб відновлюватися після збоїв, з метою забезпечення правильної обробки даних;

- захист від атак, що використовують перевантаження / переповнення буфера.

Повинні бути підготовлені відповідні контрольні листи, діяльність повинна бути документально підтверджена, а результати мають залишатися захищеними.

Приклади перевірок, які можна вбудувати, включають наступне:

- засоби управління з'єднаннями або пакетами для того, щоб узгодити сальдо файлів даних після поновлення угод;

- засоби управління сальдо для того, щоб перевіряти початкове сальдо по відношенню до попереднього кінцевого сальдо, а саме:

- засоби управління від виконання до виконання [run-to-run];

- підсумкові дані оновлень файлу;

- засоби управління від програми до програми [program-to-program];

- валідація вхідних даних, створюваних системою;

- перевірки на цілісність, автентичність або яку-небудь іншу характеристику захисту даних або програмного забезпечення, що заван-

тажуються або підкачуються між центральними та віддаленими комп'ютерами;

- контрольні суми записів і файлів;

- перевірки для забезпечення того, щоб прикладні програми виконувалися в правильний час;

- перевірки для забезпечення того, щоб програми виконувалися в правильному порядку, щоб їх виконання припинялося у разі збою, і щоб подальша обробка була зупинена до тих пір, поки проблема не буде вирішена;

- створення журналу реєстрації дій, пов'язаних з обробкою.

Дані, які були введені правильно, можуть бути пошкоджені апаратними помилками, помилками обробки або внаслідок навмисних дій.

Необхідні валідаційні перевірки будуть залежати від характеру програми та ділового впливу будь-якого пошкодження даних.

4.2.3. Цілісність повідомлень

Повинні бути визначені вимоги до забезпечення автентичності та захисту цілісності повідомлень в додатках, і повинні бути визначені і реалізовані відповідні засоби управління.

Повинна виконуватися оцінка ризиків для захисту, з метою з'ясувати, чи потрібна цілісність повідомлення, і виявити найбільш підходящі методи реалізації.

Криптографічні методи, можуть використовуватися як адекватні засоби реалізації аутентифікації повідомлень.

4.2.4. Валідація вихідних даних

Повинна здійснюватися валідація виводу даних з програми, з метою забезпечення того, щоб обробка інформації, що зберігається, була правильною і відповідною обставинам.

Валідація вихідних даних може включати в себе наступне:

- перевірки правдоподібності для того, щоб з'ясувати, чи є вихідні дані коректними;

- погодження лічильника команд для забезпечення обробки всіх даних;

- надання зчитувачу або наступній системі обробки достатньої інформації для того, щоб визначити правильність, повноту, точність і класифікацію інформації;

- процедури реагування на валідаційні випробування вихідних даних;

- визначення обов'язків всього персоналу, залученого в процес виводу даних;

- створення протоколу діяльності в процесі валідації виводу даних.

Зазвичай, системи та програми створюються на тому припущенні, що, пройшовши належну валідацію, верифікацію і випробування, документальне підтвердження, перевірку і тестуючи, вихідні дані завжди будуть правильними.

Тим не менш, це припущення не завжди вірно; тобто системи, які були випробувані, все ще можуть за деяких обставин видати вірні вихідні дані.

4.3. Криптографічні засоби управління

Метою криптографічного засобу управління є – забезпечення захисту конфіденційності, автентичності або цілісності інформації.

Повинна бути розроблена політика з використання криптографічних засобів управління. Для того щоб підтримувати використання криптографічних методів, має здійснюється розподіл ключів.

4.3.1. Політика щодо використання криптографічних засобів управління

Повинна бути розроблена і реалізована політика з використання криптографічних засобів управління для захисту інформації.

При розробці криптографічної політики має бути розглянуто наступне:

- підхід керівництва до використання криптографічних засобів управління по виконкому, включаючи загальні принципи, відповідно до яких повинна захищатися ділова інформація;
- на основі оцінки ризиків повинен бути визначений необхідний рівень захисту, з урахуванням типу, строгості і якості необхідного шифрувального алгоритму;
- використання шифрування для захисту важливої інформації, яку переносять мобільними або змінними носіями, пристроями або через лінії зв'язку;
- підхід до розподілу ключів, включаючи методи для роботи із захистом криптографічних ключів та відновлення зашифрованої інформації в випадку втрачених, розкритих або пошкоджених ключів;
- ролі та обов'язки, наприклад, хто відповідає за наступне:
- реалізація політики;
- розподіл ключів, включаючи генерування ключів;
- стандарти, які належить прийняти для результативної реалізації у виконкомі (для якого ділового процесу яке рішення використовується);
- вплив використання зашифрованої інформації на засоби управління, які залежать від контролю вмісту (наприклад, виявлення вірусів).

При реалізації організаційної політики в області криптографії, увага повинна бути приділена нормам і державним обмеженням, які можуть ставитися до використання криптографічних методів.

Криптографічні засоби керування можуть використовуватися для досягнення інших цілей захисту, наприклад, таких:

- конфіденційність: використання шифрування інформації для захисту важливої або критичної інформації, як збереженої, так і переданої;
- цілісність / автентичність: використання цифрових підписів або кодів аутентифікації повідомлень для захисту автентичності та цілісності збереженої або переданої важливої або критичної інформації;

- використання криптографічних методів для того, щоб отримати доказ того, що відбулась подія або дія тощо.

Прийняття рішення з питання того, чи доречне криптографічне рішення, повинно розглядатися як частина більш широкого процесу оцінки ризиків і вибору засобів управління. Ця оцінка може потім бути використана для визначення того, чи доречний криптографічний засіб управління, який тип засобу управління повинен бути застосований, для якої мети і для яких ділових процесів.

Політика щодо використання криптографічних засобів управління необхідна для того, щоб витягти максимум переваг і мінімізувати ризики використання криптографічних методів, а також для того, щоб уникнути недоречного або неправильного використання. При використанні цифрових підписів, увага повинна бути приділена всім хто має відношення до справи законам, зокрема, законам, що описує умови, за яких цифровий підпис юридично обов'язковий за законом.

Треба вдатися до поради фахівця для того, щоб визначити відповідний рівень захисту і визначити відповідні специфікації, які забезпечать необхідний захист і підтримають реалізацію безпечної системи розподілу ключів.

4.3.2. Розподіл ключів

Для підтримки використання криптографічних методів необхідно застосовувати розподіл ключів.

Всі криптографічні ключі повинні бути захищені від модифікації, втрати і руйнування. Крім того, секретним і особистим ключам потрібен захист від недозволеного розкриття. Обладнання, що використовується для того, щоб генерувати, зберігати і архівувати ключі, має бути фізично захищене.

Система розподілу ключів повинна бути заснована на узгодженому наборі стандартів, процедур і безпечних методів для наступного:

- генерування ключів для різних криптографічних систем і різних додатків;
- генерування та отримання сертифікатів відкритого ключа;
- роздача ключів призначеним користувачам, включаючи те, як ключі повинні бути активовані по отриманні;
- зберігання ключів, включаючи те, як повноважні користувачі отримують доступ до ключів;
- зміна або оновлення ключів, включаючи правила відносно того, коли ключі повинні змінюватися, і як це буде робитися;
- робота з розкритими ключами;
- анулювання ключів, включаючи те, як ключі повинні бути вилучені або дезактивовані, наприклад, якщо ключі були розкриті або якщо користувач йде з виконкому (в такому випадку ключі також повинні бути архівовані);
- відновлення ключів, які загубилися або пошкодилися, як частина менеджменту безперервності діяльності, наприклад, для відновлення зашифрованої інформації;

- архівування ключів, наприклад, для інформації, що архівується, або для інформації, резервна копія якої створюється;

- руйнування ключів;

- реєстрація і аудит дій, пов'язаних з розподілом ключів.

Для того, щоб знизити ймовірність розкриття, повинні бути визначені дати активізації та дезактивації для ключів, щоб ключі можна було використовувати тільки протягом обмеженого періоду часу. Цей період часу повинен залежати від обставин, при яких використовується криптографічний засіб управління, і від прийнятого ризику.

На додаток до захищеного розподілу секретних і приватних ключів, також повинна бути продумана аутентифікація відритих ключів. Цей процес аутентифікації може бути здійснено з використанням сертифікатів відкритого ключа, які зазвичай випускаються сертифікуючим органом, який повинен бути визнаний виконкомом з підходящими засобами управління і прийнятими процедурами для того, щоб забезпечити необхідний ступінь довіри.

Зміст угод про рівень обслуговування або договорів із зовнішніми постачальниками криптографічних послуг, наприклад, сертифікаційним органом, повинен охоплювати питання відповідальності, надійності послуг і часу реагування для надання послуг.

Розподіл криптографічних ключів є суттєвим для результативного використання криптографічних методів. ISO/IEC 11770-1 дає додаткову інформацію про розподіл ключів. Типи криптографічних методів:

- методи секретних ключів, коли дві сторони або більше спільно використовують один і той же ключ, і цей ключ використовується як для шифровки, так і для дешифрування інформації; цей ключ повинен зберігатися в секреті, оскільки кожен, хто має доступ до ключа, має можливість декодувати всю інформацію, зашифровану з цим ключем, або ввести недозволену інформацію, використовуючи ключ;

- методи відкритих ключів, коли кожен користувач має пару ключів, відкритий ключ (який може бути відкритий кожному) і особистий ключ (який повинен триматися в секреті); методи відкритих ключів можуть використовуватися для шифрування і створення цифрових підписів.

Існує загроза підробки цифрового підпису шляхом заміни відкритого ключа користувача. Ця проблема вирішується використанням сертифіката відкритого ключа.

Криптографічні методи також можуть використовуватися для захисту криптографічних ключів. Може знадобитися передбачити процедури для обробки юридичних запитів на доступ до криптографічних ключів, наприклад, може знадобитися зробити зашифровану інформацію доступною в незашифрованому вигляді як доказ у судовій справі.

4.4. Захист системних файлів

Метою захисту системних файлів є забезпечення захисту системних файлів.

Доступ до системних файлів і вихідному тексті програми повинен

керуватись, а проектування і допоміжна діяльність у галузі інформаційних технологій повинна здійснюватись захищеним способом. Необхідно дбати про те, щоб уникнути розкриття важливих даних у випробувальному середовищі.

4.4.1. Управління системним програмним забезпеченням

Повинні бути прийняті процедури для управління установкою програмного забезпечення в операційних системах.

З метою мінімізувати ризики псування для операційних систем, для управління змінами мають бути розглянуті наступні керівні вказівки:

- оновлення операційного програмного забезпечення, програм та бібліотек програм повинно виконуватися тільки підготовленими адміністраторами з відповідного дозволу керівництва;
- операційні системи повинні зберігати лише затверджені виконувані програми і не повинні зберігати програми, що знаходяться в розробці, або компіляторі;
- додатки і системне програмне забезпечення повинно реалізовуватися тільки після проведення всебічних і успішних випробувань; випробування повинні включати випробування на практичність, безпеку, вплив на інші системи та зручність для користувача, і повинні виконуватися в окремих системах; повинно бути проведено оновлення всіх відповідних бібліотек вихідних програм;
- система управління конфігурацією повинна використовуватися для того, щоб зберігати контроль над всім реалізованим програмним забезпеченням, а також системною документацією;
- повинна бути прийнята стратегія відкату (відновлення попереднього стану) перш, ніж будуть реалізовуватися зміни;
- повинен вестися контрольний журнал всіх оновлень в бібліотеках системних програм;
- попередні версії прикладного програмного забезпечення повинні зберігатися на випадок надзвичайної ситуації;
- старі версії програмного забезпечення повинні зберігатися в архіві разом з усією необхідною інформацією та параметрами, процедурами, деталями конфігурації і допоміжним програмним забезпеченням стільки, скільки дані зберігаються в архіві.

Програмне забезпечення, що постачається постачальником і яке використовується в операційних системах, повинно підтримуватися на рівні, підтримуваному постачальником. З часом, програмні постачальники перестануть підтримувати більш старі версії програмного забезпечення. Виконком повинен врахувати ризики, пов'язані з розрахунком на непідтримуване програмне забезпечення.

Будь-яке рішення про перехід до нової версії повинно враховувати ділові вимоги до змін, а також захист версії, тобто введення нових функціональних можливостей в області захисту або серйозність проблем в галузі захисту, впливають на цю версію. Повинні застосовуватися латки до програмного забезпечення, якщо вони можуть допомогти

усунути або зменшити слабкі місця захисту.

Фізичний або логічний доступ повинен надаватися постачальникам тільки в цілях підтримки, коли це необхідно, і з схвалення керівництва. Діяльність постачальника повинна постійно контролюватися.

Комп'ютерне програмне забезпечення може покладатися на програмне забезпечення і модулі, що поставляються ззовні, які повинні постійно контролюватися і управлятися для того, щоб уникнути недозволених змін, які можуть привнести слабкі місця в захист.

Версія операційних систем повинна змінюватися лише тоді, коли є вимога зробити так, наприклад, якщо поточна версія операційної системи більше не підтримує ділові вимоги. Зміна версій не повинна відбуватися тільки тому, що стала доступною нова версія операційної системи. Нові версії операційних систем можуть бути менш безпечними, менш стабільними і гірше розуміються, ніж поточні системи.

4.4.2. Захист випробувальних даних системи

Випробувальні дані повинні вибиратися ретельно, і повинні бути захищені і керовані.

Треба уникати використання робочих баз даних, що містять особисту інформаційну чи будь-яку іншу важливу інформацію, в цілях випробування. Якщо особиста інформація або інформація, яка важлива в іншому відношенні, використовується в цілях випробування, то всі важливі подробиці і зміст повинні бути видалені або модифіковані до невпізнання перед використанням.

Наступні керівні вказівки повинні застосовуватися для захисту робочих даних, коли ті використовуються в цілях випробування:

- процедури управління доступом, які застосовуються до робочих прикладних систем, повинні також застосовуватися до випробувальних прикладних систем;
- повинен бути окремий дозвіл тоді, коли робоча інформація копіюється в випробувальну прикладну систему;
- робоча інформація повинна бути стерта з випробувальної прикладної системи негайно після того, як випробування буде завершено;
- копіювання та використання робочої інформації повинні бути зареєстровані для того, щоб забезпечити ведення контрольного журналу.

Системне і приймальне випробування зазвичай вимагають великих обсягів випробувальних даних, які близькі до робочих даних настільки, наскільки це можливо.

4.4.3. Управління доступом до сирцевого коду програми

Доступ до сирцевого коду програми повинен бути обмежений.

Сирцевий код програми - це код, написаний програмістами, який компілюється (і зв'язується) для того, щоб створювати модулі. Певні мови програмування не проводять формальної відмінності між сирцевим кодом і модулями, так як модулі створюються в той час, коли вони активуються.

Стандарти ISO 10007 та ISO/IEC 12207 надають додаткову інформацію про менеджмент конфігурації і процеси життєвого циклу програмного забезпечення.

Доступ до сирцевого коду програми і пов'язаних елементів (таких як проекти, специфікації, плани верифікації та плани валідації) повинен керуватися для того, щоб запобігти введенню недозволених виконуваних функцій і для того, щоб уникнути ненавмисних змін. Для сирцевого коду програми цього можна досягти шляхом керованого центрального зберігання такого коду, переважно в бібліотеках сирцевих програм. Потім повинні бути розглянуті наступні керівні вказівки для управління доступом до таких бібліотек вихідних програм, з метою знизити можливість псування комп'ютерних програм:

- де можливо, бібліотеки вихідних програм не повинні міститися в операційних системах;
- менеджмент вихідного коду програм і бібліотек вихідних програм повинен здійснюватися згідно встановлених процедур;
- допоміжний персонал не повинен мати необмежений доступ до бібліотек сирцевих програм;
- оновлення бібліотек сирцевих програм і пов'язаних елементів, а також випуск програмних джерел програмістам повинен здійснюватися тільки після того, як буде отримано відповідний дозвіл;
- роздруківки програм повинні перебувати в безпечному середовищі;
- повинен вестися контрольний журнал всіх доступів до бібліотек вихідних програм;
- супровід і копіювання бібліотек вихідних програм повинні підкорятися жорстким процедурам управління змінами.

4.5. Захист в процесах розробки та допоміжних процесах

Метою захисту в процесах розробки та допоміжних процесах є підтримування захисту прикладного системного програмного забезпечення та інформації.

Середовища проектування та допоміжні середовища повинно керуватись.

Відповідальні за прикладні системи, повинні також бути відповідальними за захист середовища проектування або допоміжного середовища. Вони повинні забезпечувати, щоб всі пропоновані зміни системи були проаналізовані для того, щоб забезпечити, що вони не піддають ризику захист або системи, або операційне середовище.

4.5.1. Процедури управління змінами

Реалізація змін повинна управлятися шляхом використання офіційних процедур управління змінами.

Офіційні процедури управління змінами повинні бути документтально підтверджені і приведені у виконання для того, щоб мінімізувати порчу інформаційних систем. Введення нових систем і суттєвих змін в існуючі системи має підкорятися офіційним процесу докумен-

тування, специфікації, випробування, управління якістю і керованої реалізації.

Цей процес повинен включати оцінку ризиків, аналіз впливів змін, а також специфікації необхідних засобів захисту. Цей процес також повинен забезпечувати, щоб існуючий захист і процедури керування не піддавалися ризику, щоб допоміжним програмістам був наданий доступ тільки в ті частини системи, які необхідні для їх роботи, і щоб була отримана офіційна згода та затвердження для будь-якої зміни.

Якщо тільки це практично здійснимо, то прикладні та операційні процедури управління змінами повинні бути інтегровані. Процедури зміни повинні включати в себе наступне:

- ведення запису узгоджених рівнів дозволу;
- забезпечення того, що зміни подаються повноважними користувачами;
- аналіз засобів управління і процедур забезпечення цілісності з метою гарантування того, що зміни не піддаваний їх ризику;
- виявлення всього програмного забезпечення, інформації, об'єктів баз даних і апаратних засобів, які вимагають поправок;
- отримання офіційного затвердження для докладних пропозицій до того як робота почнеться;
- забезпечення того, щоб повноважні користувачі прийняли зміни до реалізації;
- забезпечення того, щоб набір системної документації оновлювався по виконанню кожної зміни, і щоб стара документація архівувалася або ліквідувалася;
- підтримання управління версіями для всіх оновлень програмного забезпечення;
- ведення контрольного журналу всіх запитів на зміни;
- забезпечення того, щоб операційна документація і процедури, визначені користувачем, були змінені, як необхідно, щоб залишатися відповідними;
- забезпечення того, щоб реалізація змін відбувалася в правильний час і не заважала залученим діловим процесам.

Зміна програмного забезпечення може вплинути на операційне середовище. Хороша практика включає випробування нового програмного забезпечення в середовищі, відокремленою як від виробничих середовищ, так і від середовищ розробки. Це забезпечує контроль над новим програмним забезпеченням і дає можливість додаткового захисту робочої інформації, яка використовується в випробувальних цілях. Це повинно включати в себе латки, службові пакети та інші оновлення. Автоматизовані оновлення не повинні використовуватися в критичних системах, оскільки деякі оновлення можуть викликати збій в критичних додатках.

4.5.2. Технічний аналіз додатків після змін операційної системи

Коли операційні системи змінюються, ділові критичні програми

повинні аналізуватися і випробовуватися, з метою гарантування відсутності несприятливого впливу на організаційні операції або захист.

Цей процес повинен охоплювати наступне:

- аналіз процедур управління прикладними процесами і забезпечення цілісності з метою гарантування того, що вони не були піддані ризику зміни операційної системи;
- забезпечення того, що річний план підтримки та бюджет будуть охоплювати аналіз і випробування системи, що випливають із змін операційної системи;
- забезпечення того, щоб повідомлення про зміни операційної системи було надано завчасно, з метою уможливлення проведення належних випробувань та аналізу до реалізації;
- забезпечення того, щоб належні зміни були зроблені в планах забезпечення безперервності діяльності.

Спеціальна група або особа повинні бути призначені відповідальними за перевірку слабких місць і випусків латок і виправлень.

4.5.3. Обмеження на зміни в пакетах програм

Треба перешкоджати модифікаціям в пакетах програм, ці модифікації повинні бути обмежені необхідними змінами, і всі зміни повинні строго контролюватися.

На скільки можливо і практично здійснимо, пакети програм, що поставляються постачальниками, повинні використовуватися без модифікації. Якщо пакет програм необхідно модифікувати, то повинні бути розглянуті наступні пункти:

- ризики вбудованих засобів управління і процеси забезпечення цілісності, які піддаються ризику;
- чи повинна бути отримана згода постачальника;
- можливість отримання необхідних змін від постачальника у вигляді стандартних програмних оновлень;
- вплив, якщо виконком стає відповідальним за майбутній супровід програмного забезпечення в результаті змін.

Якщо зміни необхідні, то оригінальне програмне забезпечення повинно бути збережено, а зміни застосовані до чітко позначеної копії. Повинен бути реалізований процес управління оновленням програмного забезпечення для того, щоб гарантувати установку найбільш оновлених затверджених латок і оновлень додатків для всього дозволеного програмного забезпечення. Всі зміни повинні бути повністю випробувані і документально підтверджені для того, щоб вони могли застосовуватися повторно, якщо необхідно, до майбутніх програмним оновлень. Якщо потрібно, то модифікації повинні бути випробувані і валідовані незалежним оціночним органом.

4.5.4. Витік інформації

Можливості для витоку інформації повинні бути попереджені.

Наступне повинно бути розглянуто для того, щоб обмежити ризик витоку інформації, наприклад, через використання та експлуатацію

прихованих каналів:

- сканування вихідних носіїв інформації та засобів зв'язку на наявність прихованої інформації;

- маскування і модулювання поведінки систем і засобів зв'язку для того, щоб знизити ймовірність того, що третя сторона буде здатна простежити інформацію з такої поведінки;

- використання систем і програмного забезпечення, які, як вважається, мають високу цілісністю, наприклад, використовують оцінені продукти;

- регулярний постійний контроль діяльності персоналу та системи там, де це дозволено за існуючим законодавством чи нормам;

- постійний контроль використання ресурсів в комп'ютерних системах.

Приховані канали - це шляхи, які не призначені для проведення інформаційних потоків, але які можуть, тим не менш, існувати в системі або мережі. Наприклад, маніпулювання бітами в протоколах обміну пакетами може використовуватися як прихований метод сигналізації. Через їх природу, запобігання існуванню всіх можливих прихованих каналів буде важким, якщо не неможливим. Проте, експлуатація таких каналів часто здійснюється троянським кодом. Отже, прийняття заходів для захисту від троянського коду зменшує ризики експлуатації прихованих каналів. Запобігання недозволеного доступу до мережі, а також політика і процедури для того, щоб перешкоджати неправильне використання інформаційних послуг персоналом допоможуть захиститися від прихованих каналів.

4.5.5. Аутсорсінгова розробка програмного забезпечення

Аутсорсінгова розробка програмного забезпечення повинна бути під наглядом виконкому та постійно контролюватися виконкомом.

Якщо здійснюється аутсорсінг розробки програмного забезпечення, то повинні бути розглянуті наступні пункти:

- ліцензійні угоди, власність на код і права на інтелектуальну власність;

- сертифікація якості і точності виконаної роботи;

- заходи по умовному депонуванню на випадок відмови третьої сторони;

- права доступу для аудиту якості і точності зробленої роботи;

- договірні вимоги для якості та захисної функціональності коду;

- випробування перед установкою з метою виявити зловмисний і троянський код.

4.6. Менеджмент технічно слабких місць

Метою менеджменту технічно слабких місць є - зниження ризиків, які виникають при експлуатації опублікованих технічно слабких місць.

Менеджмент технічно слабких місць повинен реалізовуватися дієвим, систематичним і повторюваним способом з вимірюваннями, виконуваними для підтвердження його результативності. Ці міркування

повинні включати операційні системи, а також будь-які інші програми, які використовуються.

4.6.1. Управління технічно слабкими місцями

Повинна бути отримана своєчасна інформація про технічно слабкі місця використовуваних інформаційних систем, оцінена схильність виконкому впливу таких слабких місць, і вжито належних заходів для того, щоб врахувати пов'язаний з ними ризик.

Поточний і повний опис активів - це попередня умова для результативного управління технічно слабкими місцями. Специфічна інформація, необхідна для підтримки менеджменту технічно слабких місць, включає постачальника програмного забезпечення, номера версій, поточний стан розробки (наприклад, яке програмне забезпечення в яких системах встановлено) і людина (люди) у виконкомі, відповідальні за програмне забезпечення.

Відповідну та своєчасну дію має бути розпочато у відповідь на виявлення можливих технічно слабких місць. Треба виконувати наступні настанови для того, щоб встановити результативний процес менеджменту для технічно слабких місць:

- виконком повинен визначити і встановлювати ролі та обов'язки, пов'язані з менеджментом технічно слабких місць, включаючи постійний контроль слабкого місця, оцінку ризиків слабкого місця, накладення латок, відстеження активів та будь-які необхідні обов'язки з кординації;

- інформаційні ресурси, які будуть використовуватися для виявлення значущих технічно слабких місць і для підтримки поінформованості про них, повинні бути визначені для програмного забезпечення та іншої технології (заснованої на опису активів); ці інформаційні ресурси повинні оновлюватися на основі змін у опису, або коли виявляються інші нові або корисні ресурси;

- повинна бути визначена тимчасова шкала для того, щоб реагувати на повідомлення про можливі значущих технічно слабкі місця;

- як тільки можливе технічно вразливе місце буде виявлено, виконком повинен визначити пов'язані з ним ризики та дії, які потрібно вжити; така дія може включати в себе накладення латок на уразливі системи та / або застосування інших засобів управління;

- залежно від того, наскільки терміново необхідно розглянути технічно слабке місце, дію має бути виконано відповідно із засобами управління, пов'язаними з управлінням змінами або шляхом виконання процедур реагування на події в системі захисту інформації;

- якщо доступна латка, то повинні бути оцінені ризики, пов'язані з установкою латки (ризики, що накладалися вразливим місцем, повинні бути порівняні з ризиками установки латки);

- латки повинні випробовуватися та оцінюватися до того, як вони будуть встановлені, з метою забезпечити того, щоб вони були результативні, і що вони не приведуть до неприпустимих побічних ефектів; якщо ніякої латки немає в розпорядженні, то повинні бути розглянуті

інші засоби управління, такі як наступні:

- відключення послуг або можливостей, пов'язаних з уразливим місцем;
- адаптація або додавання засобів управління доступом, наприлад, брандмауерів, на кордонах мереж;
- підвищений постійний контроль для того, щоб виявити або запобігти фактичній атаці;
- підвищення обізнаності про слабке місце;
- контрольний журнал повинен вестися для всіх виконуваних процедур;
- процес менеджменту технічно слабкими місцями повинен регулярно контролюватися і оцінюватися для того, щоб забезпечити його результативність та ефективність;
- системи з високим ступенем ризику повинні бути розглянуті в першу чергу.

Правильне функціонування організаційного процесу менеджменту технічно слабкими місцями критично для багатьох організацій і, отже, повинно регулярно контролюватися. Точний опис є суттєвим для забезпечення того, що можливі значущі технічно слабкі місця виявлені.

Менеджмент технічно слабкими місцями може розглядатися як підфункція управління змінами і в цій якості може використовувати в своїх інтересах процес і процедури менеджменту змін.

Постачальники часто перебувають під значним тиском щодо того, щоб випускати латки якнайскоріше. Отже, латка може не звертатися до проблеми належним чином і може мати негативні побічні ефекти. Також, в деяких випадках, видалення латки може не бути легко досяжним після того, як латка буде накладена.

Якщо необхідне випробування латок не можливе, наприклад, через витрати або нестачу ресурсів, то може бути розглянута затримка в накладенні латки, з метою оцінити пов'язаний ризик, ґрунтуючись на досвіді, про який повідомили інші користувачі.

КЕРУЮЧИЙ СПРАВАМИ ВИКОНКОМУ О.О. ГИЖКО