МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”



**Реферат**

*на тему:*

«Захист периметру і контроль доступу до об’єктів організації»

Виконав:

Ст. гр. УІ -42

**Гончарук О.В.**

Перевірив:

Шандра З.А.

Львів 2011

План

Вступ

1. **Загальні методи захисту інформації у робочому середовищі організації**

1.1 Інвентаризація ресурсів

1.2 Безпека персоналу

1.2.1Реагування на небезпечні події

**2. Фізичний захист периметрів**

2.1 Фізичний захист обладнання

2.1.1 Реагування на події, що таять погрозу безпеки

2.2 Створення захищених зон

2.3 Захист обладнання

2.3.1 Захист від шкідливого програмного забезпечення

1. **Обслуговування систем**

3.1 Оперування з носіями інформації і їхній захист

3.2 Обмін даними і програмами

3.2.1 Управління доступом користувачів

3.2.1.1 Обов'язки користувачів

3.2.2 Управління доступом до комп'ютерів

3.3 Управління доступом до додатків

**4. Перевірка безпеки інформаційних систем**

4.1Аудит систем

Висновок

Список використаних джерел

Вступ

Сучасні інформаційні технології потребують організації високого рівня захисту даних. Колективне користування інформаційними ресурсами вимагає чіткої постановки задачі захисту окремих папок та файлів та мережевих ресурсів взагалі від несанкціонованого втручання інформаційних зловмисників, вірусів та небезпечних програм. Найважливішим етапом на цьому рівні є фізичний захист самого інформаційного ресурсу. Якщо ж на такому ресурсі зберігаються конфіденційні дані, вони повинні знаходитися у безпечному місці. Метою мого проекту є фізичний захист інформації за допомогою вбудованих засобів операційних систем, апаратного та програмного забезпечення, а також проведення аудиторського аналізу приміщень, у яких розташовується інформаційний ресурс.

Суть інформаційної безпеки — забезпечити безперебійну роботу організації і звести до мінімуму збиток від подій, що таять погрозу безпеки, за допомогою їхнього запобігання і зведення наслідків до мінімуму.

Управління інформаційною безпекою дозволяє колективно використовувати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів.

Інформаційна безпека складається з трьох основних компонентів:

а) конфіденційність: захист конфіденційної інформації від несанкціонованого розкриття чи перехоплення;

б) цілісність: забезпечення точності і повноти інформації і комп'ютерних програм;

в) доступність: забезпечення доступності інформації і життєво важливих сервисів для користувачів, коли це потрібно.

Інформація існує в різних формах. Її можна зберігати на комп'ютерах, передавати по обчислювальних мережах, роздруковувати чи записувати на папері, а також озвучувати в розмовах. З погляду безпеки усі види інформації, включаючи паперову документацію, бази даних, плівки, мікрофільми, моделі, магнітні стрічки, дискети, розмови й інші способи, використовувані для передачі знань і ідей, вимагають належного захисту.

1. **Загальні методи захисту інформації у робочому середовищі організації**

**1.1 Інвентаризація ресурсів**

Інвентаризація ресурсів допомагає переконатися в тому, що забезпечується їхній ефективний захист, крім того, перелік ресурсів може знадобитися для інших виробничих цілей, наприклад, при вживанні заходів по охороні здоров'я і по техніці безпеки, для страхування чи фінансових цілей. Інвентаризацію необхідно провести для всіх основних ресурсів, зв'язаних з кожною інформаційною системою. Кожен ресурс повинний бути чітко ідентифікований, а його власник і категорія таємності погоджені і задокументовані. Прикладами ресурсів, пов'язаних з інформаційними системами, є:

а) інформаційні ресурси: бази даних і файли даних, системна документація, посібники користувача, навчальні матеріали, операційні процедури і процедури підтримки, плани забезпечення безперебійної роботи організації, процедури переходу на аварійний режим;

б) програмні ресурси: прикладне програмне забезпечення, системне програмне забезпечення, інструментальні засоби й утиліти;

в) фізичні ресурси: комп'ютери і комунікаційне устаткування, магнітні носії даних (стрічки і диски), інше технічне устаткування (блоки живлення, кондиціонери), меблі, приміщення;

г) сервіси: обчислювальні і комунікаційні сервіси, інші технічні сервіси (опалення, освітлення, енергопостачання, кондиціонування повітря).

Секретна інформація і вихідні дані систем, що підтримують секретну інформацію, повинні мати відповідні грифи таємності. Однак часто інформація перестає бути конфіденційною через деякий проміжок часу, наприклад, коли вона стає загальнодоступною. Це варто взяти до уваги, тому що надмірне засекречування інформації може привести до невиправданих, додаткових витрат організації.

Вихідні дані інформаційних систем, що містять секретну інформацію, повинні мати відповідний гриф таємності. Цей гриф повинний відбивати категорію таємності найбільш уразливої інформації у виведених даних. Прикладами таких вихідних даних є друковані звіти, інформація, виведена на екрани дисплеїв, дані, збережені на магнітних носіях (стрічках, дисках, касетах), електронні повідомлення і передані файли.

Фізичні мітки є найбільш придатною формою маркування. Однак у деяких випадках, наприклад, для електронної передачі даних, можуть знадобитися інші засоби, такі, як процедури, чи контракти поштові повідомлення для виконання функцій маркування.

**1.2 Безпека персоналу**

Користувачі повинні бути навчені процедурам захисту і правильному поводженню з інформаційними ресурсами.

Необхідно також офіційно, у писемній формі, затвердити дозволений користувачам доступ (права й обмеження).

Користувачі повинні одержати необхідні відомості про політику організації і прийнятих у ній процедурах, включаючи вимоги до безпеки й інших засобів контролю, а також навчитися правильно користуватися інформаційними ресурсами (наприклад, знати процедуру входу в систему, уміти користатися пакетами програм) перед тим, як вони одержать доступ до інформаційних систем.

Ці міри необхідні для того, щоб гарантувати, що процедури захисту виконуються правильно, і для зведення ризику порушення конфіденційності, цілісності і доступності даних через помилку користувача до мінімуму.

Цієї політики варто дотримувати як у відношенні співробітників організації, так і у відношенні користувачів зі сторонніх організацій.

**1.2.1 Реагування на небезпечні події**

Про події, що стосуються безпеки, необхідно негайно повідомляти по адміністративних каналах.

Усі співробітники і підрядчики повинні бути ознайомлені з процедурою повідомлення про різні типи інцидентів (порушення безпеки, погроза, чи збій), що можуть уплинути на безпеку ресурсів організації. Варто зобов'язати користувачів без зволікання повідомляти про усе що спостерігається чи підозрілих випадках такого роду у відповідну службу підтримки системи захисту. В організації повинна бути установлена формальна процедура накладення дисциплінарних стягнень на співробітників, що порушують режим безпеки.

Варто встановити формальну процедуру повідомлення, а також процедуру реагування на події, яка описує міри, що слід прийняти після одержання повідомлення про інцидент. Усі співробітники і підрядчики повинні бути ознайомлені з цією процедурою; вони зобов'язані повідомляти про такий рід подій у відповідну службу підтримки системи захисту.

Користувачі інформаційних систем зобов'язані реєструвати будь-які слабості в системі безпеки, або погрози системам чи сервісам і повідомляти про них. Користувачі повинні негайно доводити подібні інциденти до відома свого безпосереднього керівництва, або постачальників відповідних послуг. Необхідно інформувати користувачів про те, що ні при яких обставинах вони не повинні намагатися перевіряти передбачувані слабості в системі захисту.

Це потрібно для захисту самих користувачів, оскільки їх дії по тестуванню слабості можуть бути витлумачені як спроби несанкціонованого використання системи.

Варто зобов'язати користувачів інформаційних систем реєструвати усі випадки, коли функціонування програмного забезпечення представляється їм неправильним, тобто не відповідної специфікації; вони повинні сповіщати про це в місцеву службу технічної підтримки інформаційних систем або безпосередньо постачальнику даних послуг.

Варто установити процедури, що негайно повинний виконати користувач, який підозрює, що збій викликаний шкідливою програмою, наприклад, комп'ютерним вірусом. При розробці таких процедур варто звернути особливу увагу на наступні моменти:

а) Записати «симптоми» і всі повідомлення, що з'являються на екрані.

б) Припинити роботу на комп'ютері і, якщо можливо, відключити його. Негайно повідомити про інцидент у службу технічної підтримки інформаційних систем. Якщо устаткування підлягає огляду, то його необхідно від’єднати від мереж організації, перш ніж знову включити живлення. Не використовувати на інших комп'ютерах дискети, записані на цьому комп'ютері.

в) Негайно повідомити про подію в службу підтримки системи захисту.

Ні при яких обставинах користувачі не повинні намагатися видалити підозріле програмне забезпечення. Відновлення програмного забезпечення повинні виконувати фахівці, що мають відповідні знання і досвід роботи.

Варто визначити формальну процедуру накладення дисциплінарних стягнень на співробітників, що порушили прийняті в організації політику і процедури безпеки. Ця процедура повинна служити стримуючим фактором для співробітників, що схильні зневажати процедурами захисту. Крім того, вона повинна забезпечувати правильний і справедливий розгляд справ співробітників, підозрюваних у серйозному чи постійному порушенні безпеки. Процедура накладення дисциплінарних стягнень повинна бути розроблена з урахуванням кадрової політики організації і затверджена керівництвом.

**2. Фізичний захист периметрів**

Фізичний захист повинний бути заснований на визначених периметрах безпеки і забезпечуватися шляхом установки в організації ряду бар'єрів, розташованих у стратегічних місцях. Вимоги до кожного захисного бар'єра і його місцеві розташування повинні визначатися цінністю ресурсів і сервісів, а також ризиками порушення безпеки й існуючими захисними мірами. Кожен рівень фізичного захисту повинний мати визначений периметр безпеки, у межах якого повинний бути забезпечений належний рівень захисту.

Для комп'ютерів і інших інформаційних ресурсів периметр безпеки може обмежувати область підвищеної безпеки, комп'ютерний зал, закритий на замок офіс; периметр безпеки може ґрунтуватися і на інших видах фізичних границь.

Пропонуються наступні рекомендації**:**

а) Периметр безпеки повинний відповідати цінності ресурсів, що захищаються.

б) Периметр безпеки повинний бути чітко визначений.

в) Допоміжне устаткування (наприклад, фотокопіювальні апарати, факс-машини) повинні бути так розміщені, щоб зменшити ризик несанкціонованого доступу до захищених областей або компрометації конфіденційної інформації.

г) Фізичні бар'єри повинні по необхідності простиратися від підлоги до стелі, щоб запобігти несанкціонованому доступу у приміщення і забрудненню навколишнього середовища.

д) Не слід надавати стороннім особам інформацію про те, що робиться в захищених областях без потреби.

е) Варто розглянути можливість встановлення заборони на роботу поодинці без належного контролю; це необхідно як для безпеки, так і для запобігання шкідливих дій.

ж) Комп'ютерне устаткування, що належать організації, варто розміщати в спеціально призначених для цього місцях, окремо від устаткування, контрольованого сторонніми організаціями.

з) У неробочий час захищені області повинні бути фізично недоступні (закриті на замки) і періодично перевірятися охороною.

и) Персоналу, що здійснює технічне обслуговування систем, повинний бути наданий доступ у захищені області тільки в разі потреби і після одержання дозволу. По необхідності доступ такого персоналу (особливо до конфіденційних даних) варто обмежити, а їх дії варто відслідковувати.

и) У межах периметра безпеки використання фотографічної, звукозаписної і відео апаратури повинне бути заборонено, за винятком санкціонованих випадків.

У захищених областях варто установити належний контроль доступу в приміщення, щоб тільки персонал, що має відповідні повноваження, мав до них доступ. Пропонується розглянути наступні засоби контролю:

а) За відвідувачами захищених областей необхідно установити нагляд, а дата і час їхнього входу і виходу повинні реєструватися. Відвідувачам повинний бути наданий доступ для конкретних, дозволених цілей.

б) Весь персонал, що працює в захищених областях, повинний носити на одязі добре помітні ідентифікаційні картки; крім того, варто рекомендувати їм запитувати пропуск у незнайомих осіб.

в) Необхідно негайно вилучити права доступу в захищені області в співробітників, що звільняються з даного місця роботи.

**2.1 Фізичний захист обладнання**

Необхідно забезпечити фізичний захист устаткування від погроз порушення безпеки і небезпек, що представляються навколишнім середовищем.

Захист устаткування інформаційних систем (включаючи устаткування, використовуване за межами організації) необхідний як для того, щоб зменшити ризик несанкціонованого доступу до даних, так і для того, щоб не допустити його втрату або ушкодження. Варто також приділити увагу проблемам розміщення устаткування і його утилізації. Можуть знадобитися спеціальні міри для захисту від несанкціонованого доступу й інших небезпек, а також для захисту допоміжного устаткування, наприклад, системи електроживлення і кабельного розведення.

Устаткування інформаційних систем повинне бути так розміщено і захищено, щоб зменшити ризик, зв'язаний із впливом навколишнього середовища і несанкціонованим доступом.

Пропонуються наступні рекомендації:

а) Устаткування варто розміщати так, щоб по можливості звести до мінімуму зайвий доступ у робочі приміщення. Робочі станції, що підтримують конфіденційні дані, повинні бути розташовані так, щоб вони були завжди на очах.

б) Варто розглянути можливість ізоляції областей, що вимагають спеціального захисту, щоб понизити необхідний рівень загального захисту.

в) Для ідентифікації можливих небезпек пропонується використовувати наступний контрольний список:

· пожежа;

· задимлення;

· затоплення;

· запилення;

· вібрація;

· вплив хімічних речовин;

· перешкоди в електроживленні;

· електромагнітна радіація.

г) Варто заборонити прийом їжі і паління в місцях розміщення комп'ютерного устаткування.

д) Варто розглянути можливість використання спеціального захисту, наприклад, клавіатурних мембран, для устаткування в промислових середовищах.

е) Варто розглянути можливі небезпеки як на даному поверсі, так і на сусідніх поверхах.

Устаткування необхідно захищати від збоїв у системі електроживлення й інших неполадках в електричній мережі. Джерело живлення повинне відповідати специфікаціям виробника устаткування.

Варто розглянути необхідність використання резервного джерела живлення. Для устаткування, що підтримує критично важливі виробничі сервіси, рекомендується установити джерело безперебійного живлення. План дій у надзвичайних ситуаціях повинний включати міри, які необхідно прийняти по закінченні терміну придатності джерел безперебійного живлення. Устаткування, що працює з джерелами безперебійного живлення, необхідно регулярно тестувати відповідно до рекомендацій виробника.

Кабелі електроживлення і мережеві кабелі для передачі даних необхідно захищати від розкриття для цілей перехоплення інформації й ушкодження. Для зменшення такого ризику в приміщеннях організації пропонується реалізувати наступні захисні міри:

а) Кабелі електроживлення і лінії зв'язку, що йдуть до інформаційних систем, повинні бути проведені під землею (по можливості) чи захищені належним чином за допомогою інших засобів.

б) Необхідно розглянути заходи для захисту мережевих кабелів від їхнього несанкціонованого розкриття для цілей перехоплення даних і від ушкодження, наприклад, скориставшись екранами або проклавши ці лінії так, щоб вони не проходили через загальнодоступні місця.

в) Для винятково уразливих чи критично важливих систем варто розглянути необхідність вживання додаткових заходів, таких, як:

* шифрування даних;
* установка броньованих екранів і використання приміщень, що замикаються;
* використання інших маршрутів або середовищ передачі даних.

Необхідно здійснювати належне технічне обслуговування устаткування, щоб забезпечити його постійну доступність і цілісність. Пропонуються наступні рекомендації:

а) Технічне обслуговування устаткування повинне здійснюватися через проміжки часу, що рекомендуються постачальником, і відповідно до інструкцій.

б) Ремонт і обслуговування устаткування повинен виконувати тільки персонал підтримки, що має відповідні повноваження.

в) Необхідно реєструвати всі несправності і неполадки.

Використання устаткування інформаційних систем (незалежно від того, хто їм володіє), що підтримують виробничі процеси, за межами організації повинно бути санкціоновано керівництвом; рівень захисту такого устаткування повинний бути таким же, як і для устаткування, розташованого на території організації. Пропонуються наступні рекомендації:

а) Співробітникам забороняється використовувати персональні комп'ютери для продовження роботи вдома, якщо не встановлена процедура перевірки на наявність вірусів.

б) Під час поїздок забороняється залишати устаткування і носії інформації в загальнодоступних місцях без догляду. Портативні комп'ютери варто провозити як ручний багаж.

в) Під час поїздок портативні комп'ютери уразливі стосовно крадіжок, втрати і несанкціонованого доступу. Для таких комп'ютерів варто забезпечити належний захист доступу, щоб запобігти несанкціонованому доступу до інформації, що зберігається в них.

г) Варто завжди дотримуватися інструкції виробника, що стосуються захисту устаткування, наприклад, захищати устаткування від впливу сильних електромагнітних полів.

Ризики порушення безпеки (наприклад, ушкодження, крадіжки, перехоплення), можуть значно варіюватися від місця до місця; це варто обов'язково враховувати при визначенні найбільш придатних захисних засобів.

Дані організації можуть бути скомпрометовані внаслідок недбалої утилізації устаткування. Перед утилізацією устаткування всі його компоненти, включаючи носії інформації, наприклад, жорсткі диски, необхідно перевіряти, щоб гарантувати, що конфіденційні дані і ліцензоване програмне забезпечення було вилучено. Ушкоджені запам'ятовуючі пристрої, що містять особливо коштовні дані, можуть вимагати оцінки ризиків для того, щоб визначити, чи можна їх знищувати, ремонтувати або позбутися від них.

**2.1.1** **Реагування на події, що таять погрозу безпеки**

Про події, що стосуються безпеки, необхідно негайно повідомляти по адміністративних каналах.

Усі співробітники і підрядчики повинні бути ознайомлені з процедурою повідомлення про різні типи інцидентів (порушення безпеки, погроза, збій), що можуть вплинути на безпеку ресурсів організації. Варто зобов'язати користувачів без зволікання повідомляти про все що спостерігається чи підозрілих випадках такого роду у відповідну службу підтримки системи захисту. В організації повинна бути установлена формальна процедура накладення дисциплінарних стягнень на співробітників, що порушують режим безпеки.

**2.2** **Створення захищених зон**

Інформаційні системи, що підтримують критично важливі сервіси організації, повинні бути розміщені в захищених областях.

Такі системи повинні бути також захищені фізично від несанкціонованого доступу, ушкодження і перешкод. Їх варто розмістити в захищених областях, обмежених визначеним периметром безпеки, з належним контролем доступу в приміщення і захисні бар'єри. Для зменшення ризику несанкціонованого доступу або ушкодження паперової документації і носіїв інформації, рекомендується задати чіткі правила використання робочого столу.

**2.3 Захист обладнання**

Необхідно забезпечити фізичний захист устаткування від погроз порушення безпеки і небезпек, що представляються навколишнім середовищем.

Захист устаткування інформаційних систем (включаючи устаткування, використовуване за межами організації) необхідний як для того, щоб зменшити ризик несанкціонованого доступу до даних, так і для того, щоб не допустити його втрат або ушкодження. Варто також приділити увагу проблемам розміщення устаткування і його утилізації. Можуть знадобитися спеціальні міри для захисту від несанкціонованого доступу й інших небезпек, а також для захисту допоміжного устаткування, наприклад, системи електроживлення і кабельного розведення.

**2.3.1 Захист від шкідливого програмного забезпечення**

Для запобігання і виявлення випадків впровадження шкідливого програмного забезпечення, потрібно вживання належних заходів обережності.

В даний час існує цілий ряд шкідливих методів, що дозволяють використовувати уразливість комп'ютерних програм стосовно їх несанкціонованої модифікації, з такими іменами, як „комп’ютерні віруси”, „мережеві хробаки”, „Троянські коні” і „логічні бомби”. Адміністратори інформаційних систем повинні бути завжди готові до небезпеки проникнення шкідливого програмного забезпечення в системи і по необхідності вживати спеціальних заходів по запобіганню або виявленню його впровадження. Зокрема украй важливо вжити заходів обережності для запобігання і виявлення комп'ютерних вірусів на персональних комп'ютерах.

Необхідно реалізувати заходи для виявлення і запобігання проникнення вірусів у системи і процедури інформування користувачів про їхню шкоду. Користувачам варто нагадати, що запобігання вірусів краще, ніж ліквідація наслідків від їхнього проникнення. В основі захисту від вірусів повинні лежати високі знання і розуміння правил безпеки, належні засоби управління доступом до систем і наступні конкретні рекомендації:

1.Організація повинна визначити формальну політику, що вимагає дотримання умов ліцензій на використання програмного забезпечення і заборонити використання несанкціонованих програм.

2.Противірусні програмні засоби, розроблені постачальником з доброю репутацією, варто використовувати в такий спосіб:

* програмні засоби виявлення конкретних вірусів (які повинні регулярно оновлятися і використовуватися відповідно до інструкцій постачальника) варто застосовувати для перевірки комп'ютерів і носіїв інформації на наявність відомих вірусів або як запобіжний захід, або як повсякденна процедура;
* програмні засоби виявлення змін, внесених у дані, повинні бути по необхідності інстальовані на комп'ютерах для виявлення змін у виконуваних програмах;
* програмні засоби нейтралізації вірусів варто використовувати з обережністю і тільки в тих випадках, коли характеристики вірусів цілком вивчені, а наслідки від їхньої нейтралізації передбачувані;

3.Необхідно проводити регулярну перевірку програм і даних у системах, що підтримують критично важливі виробничі процеси. Наявність випадкових файлів і несанкціонованих виправлень повинна бути виявлена за допомогою формальних процедур.

4.Дискети невідомого походження варто перевіряти на наявність вірусів до їхнього використання.

Необхідно визначити управлінські процедури й обов'язки по повідомленню про випадки поразки систем комп'ютерними вірусами і вживанню заходів по ліквідації наслідків від їхнього проникнення. Варто скласти належні плани забезпечення безперебійної роботи організації для випадків вірусного зараження, у тому числі плани.

**3.Обслуговування систем**

Заходи для обслуговування систем вимагаються для підтримки цілісності і доступності сервісів.

Необхідно визначити повсякденні процедури для зняття резервних копій з даних, реєстрації подій і збоїв, а також для спостереження за середовищем, у якій функціонує устаткування.

Резервні копії з критично важливих виробничих даних і програм повинні зніматися регулярно. Для забезпечення можливості відновлення всіх критично важливих виробничих даних і програм після виходу з ладу комп'ютера або відмови носія інформації, необхідно мати належні засоби резервного копіювання. Процедури резервного копіювання для окремих систем повинні задовольняти вимогам планів забезпечення безперебійної роботи організації.

Пропонуються наступні рекомендації:

1. Мінімальну дублюючу інформацію разом з точними і повними записами про резервні копії варто зберігати у вилученому місці на достатній відстані для того, щоб уникнути наслідків від аварії на основному робочому місці. Необхідно створити принаймні три покоління резервних копій даних для важливих виробничих додатків.

2. Резервні копії повинні бути належним чином захищені фізично від впливу навколишнього середовища у відповідності зі стандартами, прийнятими на основному робочому місці. Засоби захисту носіїв інформації, прийняті на основному робочому місці, варто поширити на місце збереження резервних копій.

3. Резервні дані необхідно регулярно тестувати, щоб бути упевненим, що на них можна буде покластися у випадку аварії.

Власники даних повинні задати період зберігання критично важливих виробничих даних, а також вимоги до постійного збереження архівних копій.

Оператори комп'ютерів повинні вести журнал реєстрації усіх виконуваних завдань. Цей журнал повинний по необхідності включати:

* час запуску й останова систем;
* підтвердження коректного оперування з файлами даних і вихідною інформацією від комп'ютерів.

Журнали реєстрації подій повинні регулярно звірятися з операційними процедурами.

Необхідно сповіщати про збої в роботі систем і починати відповідні коригувальні міри. Зафіксовані користувачами збої, що стосуються проблем з комп'ютерними і комунікаційними системами, варто заносити в журнал реєстрації. Повинні існувати чіткі правила обробки зареєстрованих збоїв, включаючи наступні:

а) аналіз журналу реєстрації збоїв для забезпечення їхнього задовільного вирішення;

б) аналіз коригувальних мір, ціль яких складається в перевірці того, чи не скомпрометовані засоби управління безпекою і чи є почата міра санкціонованою.

Для визначення умов, що можуть несприятливо позначитися на роботі комп'ютерного устаткування і для вживання коригувальних заходів, необхідно постійно стежити за навколишнім середовищем, у тому числі за вологістю, температурою і якістю джерел електроживлення. Такі процедури варто реалізовувати відповідно до рекомендацій постачальників.

* 1. **Оперування з носіями інформації і їхній захист**

Необхідно контролювати комп'ютерні носії даних і забезпечити їхній фізичний захист.

Варто визначити належні операційні процедури для захисту комп'ютерних носіїв інформації (магнітні стрічки, диски, касети), вхідних/вихідних даних і системної документації від ушкодження, викрадення і несанкціонованого доступу.

Для управління такими зйомними носіями інформації, як магнітні стрічки, диски, касети і роздруківки, необхідно мати відповідні процедури. Пропонуються наступні засоби контролю в робочому середовищі:

а) Застосування системи збереження даних, у якій забороняється використовувати описові мітки, тобто по мітках не можна визначити, які дані зберігаються на запам'ятовуючому пристрої.

б) Стирання попереднього вмісту повторно використовуваних носіїв інформації, що підлягають видаленню з організації, якщо вони більше не потрібні.

в) Одержання письмової санкції на видалення всіх носіїв інформації з організації і реєстрація усіх випадків їхнього видалення в контрольному журналі.

г) Збереження всіх носіїв інформації в надійному, захищеному середовищі відповідно до інструкцій виробників.

Усі процедури і рівні повноважень повинні бути чітко задокументовані.

Щоб захистити конфіденційні дані від несанкціонованого розкриття або використання, необхідно визначити процедури оперування з такими даними. Повинні бути підготовлені процедури для безпечного оперування з усіма носіями вхідних і вихідних конфіденційних даних, наприклад, документів, телексів, магнітних стрічок, дисків, звітів, незаповнених чеків, рахунків і ін. Пропонується розглянути наступні пункти:

а) оперування з носіями вхідної і вихідної інформації і їхнє маркування;

б) формальна реєстрація одержувачів даних, що мають відповідні повноваження;

в) забезпечення повноти вхідних даних;

г) підтвердження одержання переданих даних (по необхідності);

д) надання доступу до даних мінімальному числу осіб;

е) чітке маркування всіх копій даних для одержувача, що має відповідні повноваження;

ж) перевірка списків одержувачів із правом доступу до даних через регулярні проміжки часу.

Системна документація може містити конфіденційну інформацію, наприклад, опис прикладних процесів, процедур, структури даних і процесів підтвердження повноважень. Для захисту системної документації від несанкціонованого доступу, необхідно застосовувати наступні засоби контролю:

а) Системна документація повинна зберігатися в надійних шафах під замком.

б) Список осіб із правом доступу до системної документації повинний бути максимально обмежений, а дозвіл на її використання повинен видаватися власником додатка.

в) Документацію, створювану комп'ютерами, варто зберігати окремо від інших файлів додатків, і їй варто привласнити належний рівень захисту доступу.

Для видалення комп'ютерних носіїв інформації, що більше не потрібні, вимагаються надійні і перевірені процедури. Конфіденційна інформація може просочитися за межі організації і потрапити в руки осіб, що не мають відповідних прав, унаслідок недбалого видалення комп'ютерних носіїв даних. Для зведення такого ризику до мінімуму варто визначити чіткі процедури надійного видалення носіїв інформації. Пропонуються наступні рекомендації:

· Носії даних, що містять конфіденційну інформацію, необхідно надійно видаляти, наприклад, за допомогою їхнього спалювання або здрібнювання (дроблення), чи звільнення від даних для використання іншими додатками усередині організації.

· Для ідентифікації носіїв даних, що можуть потребувати надійного видалення, пропонується використовувати наступний контрольний список:

o вхідна документація, наприклад, телекси;

o копіювальний папір;

o вихідні звіти;

o одноразові стрічки для принтерів;

o магнітні стрічки;

o зйомні диски;

o роздруківки програм;

o тестові дані;

o системна документація.

Кожен випадок видалення носіїв конфіденційної інформації необхідно (по можливості) реєструвати в контрольному журналі.

* 1. **Обмін даними і программами**

Обміни даними і програмами необхідно контролювати. Такі обміни варто здійснювати на основі формальних угод. Повинні бути встановлені процедури і стандарти для захисту носіїв інформації під час їхнього транспортування. Необхідно враховувати наслідки для виробничої діяльності і системи безпеки від використання електронного обміну даними і повідомленнями електронної пошти, а також вимоги до засобів управління безпекою.

Комп'ютерні носії даних можуть бути уразливі стосовно несанкціонованого доступу, використання й ушкодження під час транспортування. Для захисту комп'ютерних носіїв інформації, що транспортуються з однієї організації в іншу, пропонуються наступні засоби контролю:

а) Використання надійних кур'єрів і транспорт. Узгодження списку кур'єрів, наділених відповідними повноваженнями, з керівництвом і реалізація процедури ідентифікації кур'єрів.

б) Забезпечення належного захисту вмісту упакування від можливого фізичного ушкодження під час транспортування відповідно до інструкцій виробників.

в) Вживання спеціальних заходів (по необхідності) для захисту конфіденційної інформації від несанкціонованого розкриття або модифікації.

Приклади:

а) використання контейнерів закритого типу;

б) доставка за допомогою кур'єрів;

в) упакування, захищене від стороннього втручання (яке дозволяє виявити спроби її розкриття);

г) у виняткових випадках поділ вантажу на кілька частин і їхня посилка різними маршрутами.

Для зменшення ризику, якому піддаються виробничі процеси і система безпеки, зв'язана з використанням електронної пошти, варто застосовувати (по необхідності) відповідні засоби контролю. Електронна пошта відрізняється від традиційних видів зв'язку швидкістю, структурою повідомлень, ступенем формальності й уразливістю стосовно перехоплення. Для зменшення ризику, якому піддаються виробничі процеси і система безпеки, пов'язаного з застосуванням електронної пошти, необхідно використовувати належні засоби контролю. Пропонується розглянути наступні пункти:

а) уразливість електронних повідомлень стосовно несанкціонованого перехоплення і модифікації;

б) уразливість даних, що пересилаються по електронній пошті, стосовно помилок, наприклад, неправильна адресація чи напрямок повідомлень не по призначенню, а також надійність і доступність системи в цілому;

в) вплив зміни характеристик комунікаційного середовища на виробничі процеси, наприклад, вплив підвищеної швидкості передачі даних або зміни системи адресації між організаціями й окремими особами;

г) правові розуміння, такі, як необхідність перевірки джерела повідомлень і ін.;

д) наслідки для системи безпеки від розкриття змісту каталогів;

е) необхідність вживання захисних заходів для контролю вилученого доступу користувачів до електронної пошти.

**3.2.1 Управління доступом користувачів**

Для управління процесом надання прав доступу до інформаційних систем вимагаються формальні процедури.

Ці процедури повинні містити в собі всі стадії життєвого циклу управління доступом користувачів — від початкової реєстрації нових користувачів до видалення облікових записів користувачів, що більше не мають потреби в доступі до інформаційних систем. Особливу увагу варто приділити необхідності управлання процесом надання привілейованих прав доступу, що дозволяють користувачам обійти засоби системного контролю.

Для управління доступом до всіх багатокористувацьких інформаційних систем повинна існувати формальна процедура реєстрації і видалення облікових записів користувачів.

Доступ до багатокористувацьких інформаційних систем необхідно контролювати за допомогою формального процесу реєстрації користувачів, що повинний, наприклад:

а) перевіряти, чи надано користувачу дозвіл на використання системи її власником;

б) перевіряти, чи достатній рівень доступу до системи, наданий користувачу, для виконання покладених на нього функцій і чи не суперечить він політиці безпеки, прийнятої в організації, чи не компрометує він принцип поділу обов'язків;

в) надавати користувачам їх права доступу в письмовому виді;

г) вимагати від користувачів підписання зобов'язання, щоб показати, що вони розуміють умови доступу;

д) вимагати від постачальників послуг, щоб вони не надавали доступ до систем доти, поки не будуть закінчені процедури визначення повноважень;

е) вести формальний облік усіх зареєстрованих осіб, що використовують систему;

ж) негайно вилучати права доступу в тих користувачів, що змінили роботу або залишили організацію;

з) періодично перевіряти і видаляти користувальницькі ідентифікатори й облікові записи, що більше не вимагаються;

и) перевіряти, чи не видані користувальницькі ідентифікатори, що більше не потрібні, іншим користувачам.

Використання спеціальних привілеїв варто обмежити і контролювати.

Для багатокористувацьких систем, що вимагають захисту від несанкціонованого доступу, надання привілеїв необхідно контролювати за допомогою формального процесу визначення повноважень у такий спосіб:

а) Ідентифікувати привілеї, зв'язані з кожним програмним продуктом, підтримуваним системою, наприклад, з операційною системою чи СУБД, а також категорії співробітників, яким їх необхідно надати.

б) Надати привілеї окремим особам тільки у випадку крайньої необхідності й у залежності від ситуації, тобто тільки коли вони потрібні для виконання ними своїх функцій.

в) Реалізувати процес визначення повноважень і вести облік усіх наданих привілеїв. Не слід надавати привілеї до закінчення процесу визначення повноважень.

г) Сприяти розробці і використанню системних програм, щоб уникнути необхідності надання привілеїв користувачам.

д) Користувачі, яким надані великі привілеї для спеціальних цілей, повинні використовувати інший користувальницький ідентифікатор для звичайної роботи.

В даний час паролі є основним засобом підтвердження повноважень доступу користувачів до комп'ютерних систем. Призначення паролів необхідно контролювати за допомогою формального процесу управління, вимоги до якого повинні бути наступними:

а) Вимагати від користувачів підписання зобов'язання по збереженню персональних паролів і паролів робочих груп у секреті.

б) У тих випадках, коли користувачі повинні самі вибирати свої паролі, видати їм надійні тимчасові паролі, які вони зобов'язані негайно змінити. Тимчасові паролі також видаються у випадку, коли користувачі забувають свої паролі. Тимчасові паролі повинні видаватися тільки після позитивної ідентифікації користувача.

в) Передавати тимчасові паролі користувачам надійним способом. Варто уникати передачу паролів через посередників або за допомогою незахищених (незашифрованих) повідомлень електронної пошти. Користувачі повинні підтвердити одержання паролів.

Існують інші технології, наприклад, перевірка дійсності підпису, який варто розглянути в тому випадку, якщо забезпечення більш високого рівня безпеки виправдано.

Для забезпечення ефективного контролю за доступом до даних і інформаційних систем керівництво повинне реалізовувати формальний процес перегляду прав доступу користувачів через регулярні проміжки часу. Такий процес повинний забезпечувати наступне:

а) перегляд повноважень доступу користувачів через регулярні проміжки часу; рекомендується період у 6 місяців;

б) перегляд дозволу на надання спеціальних привілейованих прав доступу через більш короткі проміжки часу; рекомендується період у 3 місяці;

в) перевірка наданих привілеїв через регулярні проміжки часу, щоб не допустити одержання користувачами несанкціонованих привілеїв.

**3.2.1.1 Обов'язки користувачів**

Украй важливою умовою підтримки належного режиму безпеки є участь і допомога зареєстрованих користувачів.

Користувачі повинні знати свої обов'язки по забезпеченню ефективного контролю доступу, особливо що стосується використання паролів і захисту користувальницького устаткування.

Паролі є основним засобом підтвердження повноважень доступу користувачів до комп'ютерних систем. Пропонуються наступні рекомендації з вибору і використання паролів:

а) Призначати індивідуальні паролі для забезпечення підзвітності.

б) Зберігати паролі в секреті.

в) Не записувати паролі на папері, якщо не представляється можливим їх збереження в захищеному місці.

г) Змінювати паролі всякий раз, коли є вказівки на можливу компрометацію систем або паролів.

д) Вибирати паролі, що містять не менш шести символів.

е) При виборі паролів не слід використовувати:

· місяці року, дні тижня і т.п.;

· прізвища, ініціали і реєстраційні номера автомобілів;

· назви й ідентифікатори організацій;

· номера телефонів чи групи символів, що складаються з одних цифр;

· користувальницькі ідентифікатори й імена, а також ідентифікатори груп і інші системні ідентифікатори;

· більш двох однакових символів, що випливають друг за другом;

· групи символів, що складаються з одних букв.

ж) Змінювати паролі через регулярні проміжки часу (приблизно через 30 діб) і уникати повторного чи циклічного використання старих паролів.

з) Частіше змінювати паролі для привілейованих системних ресурсів, наприклад, паролі доступу до визначених системних утиліт.

и) Змінювати тимчасові паролі при першому вході в систему.

и) Не включати паролі в сценарії автоматичного входу в системи, наприклад, у макроси або функціональні клавіші.

Якщо користувачам необхідний доступ до багатьох систем і платформ і від них потрібно підтримка декількох паролів, то їм варто рекомендувати використовувати один єдиний надійний пароль для входу в усі системи, що забезпечує мінімальний рівень захисту для збереження паролів.

Користувачі повинні забезпечити належний захист устаткування, залишеного без нагляду. Устаткування, установлене на робочих місцях користувачів, наприклад, робочі станції і файлові сервери, може потребувати спеціального захисту від несанкціонованого доступу в тих випадках, коли воно залишається без догляду на тривалий час. Усі користувачі і підрядчики повинні знати вимоги до безпеки і процедури захисту устаткування, залишеного без догляду, а також свої обов'язки по забезпеченню такого захисту. Пропонуються наступні рекомендації:

а) Завершити активні сеанси зв'язку по закінченню роботи, якщо їх не можна захистити за допомогою відповідного блокування.

б) Вийти з мейнфреймів по закінченні сеансу зв'язку. Не обмежуватися тільки вимиканням ПК чи термінала.

в) Захистити ПК чи термінали, що не використовуються, за допомогою блокування з ключем або еквівалентного засобу контролю, наприклад, доступом по паролю.

**3.2.2** **Управління доступом до комп'ютерів**

Доступ до комп'ютерних систем необхідно контролювати.

Такий доступ варто надавати тільки зареєстрованим користувачам. Комп'ютерні системи, що обслуговують багатьох користувачів, повинні бути здатні робити наступне:

а) ідентифікувати і перевіряти дійсність особистості користувачів, а також по необхідності термінал або місцезнаходження кожного зареєстрованого користувача;

б) фіксувати випадки успішного і безуспішного доступу до систем;

в) надати систему управління паролями, що забезпечує вибір надійних паролів;

г) по необхідності обмежити час підключення користувачів.

Існують також більш могутні і дорогі системи управління доступом, такі, як системи оперативного реагування на проблеми. Використання таких систем виправдано у випадку високого ризику порушення режиму безпеки організації.

Для аутентификации підключень до конкретних вузлів мережі варто розглянути можливість автоматичної ідентифікації терміналів. Автоматична ідентифікація терміналів — це засіб, який можна використовувати для тих додатків, для яких важливо, щоб сеанс зв'язку можна було ініціювати тільки з конкретного термінала. Ідентифікатор, привласнений терміналу, можна використовувати для вказівки того, чи дозволено конкретному терміналу ініціювати сеанс зв'язку або робити визначені дії. Для забезпечення безпеки термінального ідентифікатора, можливо буде потрібно фізичний захист термінала.

Доступ до інформаційних систем варто здійснювати за допомогою надійної процедури входу в систему.

Процедура входу в комп'ютерну систему (logon) повинна зводити ризик несанкціонованого доступу до мінімуму, тому вона повинна давати мінімум інформації про систему, щоб уникнути надання зайвої допомоги незареєстрованному користувачу. Надійна процедура входу в систему повинна виконувати наступні функції:

а) не виводити на екран ідентифікатори системи або додатки доти, поки не завершиться процес входу в систему;

б) виводити на екран загальне попередження про те, що тільки зареєстровані користувачі мають право доступу до комп'ютера;

в) не надавати довідкову інформацію під час виконання процедури входу в систему, що могла б зробити допомогу незареєстрованному користувачу;

г) перевіряти вірогідність реєстраційної інформації тільки по завершенні введення всіх даних. При виникненні збійної ситуації система не повинна вказувати, яка частина введених даних правильна чи неправильна;

д) обмежити кількість невдалих спроб входу в систему (рекомендується три спроби), перш ніж ужити заходів:

· по реєстрації невдалої спроби;

· по примусовому введенню тимчасової затримки між подальшими спробами входу в систему;

· по розриві каналу зв'язку;

е) розірвати канал зв'язку і не подавати довідкову інформацію після відкинутої спроби входу в систему;

ж) задати мінімальну і максимальну тривалість процедури входу в систему. При її підвищенні система повинна перервати процедуру входу;

з) виводити на екран наступну інформацію при завершенні успішного входу в систему:

· дату і час попередньої успішної спроби входу в систему;

· подробиці про невдалі спроби входу в систему, початих з моменту останнього успішного входу в неї.

Для відстеження дій окремих осіб, усім користувачам необхідно привласнити унікальні персональні ідентифікатори. Користувальницькі ідентифікатори не повинні вказувати на рівень привілеїв користувача, наприклад, адміністратор, спостерігач і т.п.

У виняткових ситуаціях, у випадку явних переваг для організації, можна використовувати загальний користувальницький ідентифікатор для групи чи користувачів конкретного завдання. Такі випадки повинні бути затверджені керівництвом і задокументовані. Для забезпечення підзвітності можуть знадобитися додаткові засоби контролю.

Для аутентификации користувачів необхідно використовувати ефективну систему управління паролями. Паролі є основним засобом підтвердження повноважень доступу користувача до комп'ютерної системи. Системи управління паролями повинні надавати ефективний, інтерактивний засіб забезпечення надійних паролів.

Надійна система управління паролями повинна:

а) по необхідності примушувати користувачів до застосування індивідуальних паролів для забезпечення підзвітності;

б) по необхідності дозволяти користувачам вибирати і змінювати свої власні паролі, а також включати процедуру їхнього підтвердження, щоб уникнути помилок при їхньому наборі;

в) задати мінімальну кількість символів у паролях;

г) примушувати користувачів до зміни паролів через регулярні проміжки часу в тих випадках, коли вони самі підтримують свої паролі;

д) по необхідності примушувати привілейованих користувачів, наприклад тих, хто має доступ до системних утиліт, до більш частої зміни паролів;

е) змушувати користувачів змінювати тимчасові паролі при першому вході в систему в тих випадках, коли вони самі вибирають свої паролі;

ж) вести облік попередніх користувальницьких паролів, наприклад, за останні 12 місяців і запобігати їхньому повторному використанню користувачами;

з) не виводити паролі на екран при їхньому наборі на клавіатурі;

и) зберігати файли паролів окремо від основних даних прикладної системи;

и) зберігати паролі в зашифрованому виді, використовувати однобічний алгоритм шифрування;

к) змінювати паролі, задані постачальником програмного забезпечення за замовчуванням, після його інсталяції;

л) в ідеалі перевіряти, чи вибрав користувач надійний пароль, наприклад, за допомогою перевірки, чи не заснований пароль на наступних даних:

· місяці року, дні тижня і т.п.;

· назви й ідентифікатори організацій;

· користувальницькі ідентифікатори, імена користувачів, ідентифікатори груп і інші системні ідентифікатори;

· більш ніж два однакових символи, що випливають друг за другом;

· групи символів, що складаються з одних цифр чи одних букв.

Необхідно розглянути можливість використання сигналу тривоги, що попереджає про примус, для тих користувачів, що можуть бути мішенню для примуса.

Для бездіяльних терміналів у зонах підвищеного ризику, наприклад, у загальнодоступних місцях або місцях, що знаходяться поза межами досяжності адміністраторів безпеки організації, чи обслуговуючих систем підвищеного ризику, необхідно установити час простою для запобігання доступу незареєстрованних користувачів. Засіб установлення часу простою повинний очищати екран термінала і завершувати сеанси зв'язку з додатками і мережними сервісами після заданого періоду бездіяльності. Час простою повинен задаватися виходячи з ризику порушення режиму безпеки користувальницького термінала.

Додатковий захист додатків підвищеного ризику можна забезпечити за допомогою обмеження часу підключення. Обмеження періоду підключення термінала до комп'ютерних систем дозволяє зменшити імовірність несанкціонованого доступу. Застосування такого засобу контролю варто розглянути для комп'ютерних систем, що підтримують конфіденційні додатки, особливо для систем з терміналами, встановленими в зонах підвищеного ризику, наприклад, у загальнодоступних місцях чи місцях, що знаходяться поза межами досяжності адміністраторів безпеки організації. Прикладами таких обмежень є:

а) використання визначених інтервалів часу дозволеного доступу, наприклад, для пакетної передачі файлів, чи регулярних інтерактивних сеансів зв'язку невеликої тривалості;

б) обмеження часу підключення роботи організації, якщо не потрібна робота в понаднормовий час.

* 1. **Управління доступом до додатків**

Для управління доступом до прикладних систем і даних, необхідно використовувати логічні засоби контролю доступу.

Логічний доступ до комп'ютерних програм і даних варто надавати тільки зареєстрованим користувачам. Прикладні системи повинні:

а) контролювати доступ користувачів до даних і додатків відповідно до політики управління доступом, прийнятої в організації;

б) забезпечувати захист програм-утиліт, що здатні обійти засоби контролю систем і додатків від несанкціонованого доступу;

в) не порушувати захист інших систем, з якими вони розділяють інформаційні ресурси.

Користувачам прикладних систем, у тому числі обслуговуючому персоналу варто надавати доступ до даних і додатків відповідно до політики управління доступом до інформації, виходячи з індивідуальних потреб у виробничих додатках. Щоб задовольнити вимоги політики управління доступом, необхідно розглянути наступні засоби контролю:

а) надання системи меню для контролю доступу до додатків;

б) обмеження знання користувачами даних і функцій прикладних систем, доступ до яких їм не дозволений, за допомогою відповідного редагування користувальницької документації;

в) контроль повноважень доступу користувачів, наприклад, прав на читання, запис, видалення, виконання;

г) гарантування того, що вихідні дані від прикладних систем, що підтримують конфіденційну інформацію, містять тільки необхідні дані і посилаються тільки на термінали і комп'ютери, доступ до яких дозволений, включаючи періодичний аналіз таких вихідних даних для забезпечення видалення непотрібної інформації.

Більшість комп'ютерних систем підтримують одну чи кілька системних програм-утиліт, що здатні обійти засоби контролю системи і додатків. Необхідно обмежити і ретельно контролювати використання таких системних утиліт. Пропонується використовувати наступні засоби контролю (по можливості):

а) захист системних утиліт за допомогою паролів;

б) ізоляція системних утиліт від прикладного програмного забезпечення;

в) надання доступу до системних утиліт мінімальному числу надійних, зареєстрованих користувачів;

г) надання дозволу на спеціальне використання системних утиліт;

д) обмеження доступності системних утиліт, наприклад, часом внесення санкціонованої зміни;

е) реєстрація усіх випадків використання системних утиліт;

ж) визначення і документування рівнів повноважень доступу до системних утиліт;

з) видалення всіх непотрібних утиліт і системних програм.

Для зведення ризику ушкодження комп'ютерних програм до мінімуму, необхідно здійснювати твердий контроль за доступом до бібліотек вихідних текстів програм:

а) Не слід зберігати бібліотеки вихідних текстів програм у робочих системах (по можливості).

б) Необхідно призначити бібліотекаря програм для кожного додатка.

в) Обслуговуючий персонал не повинний мати необмежений доступ до бібліотек вихідних текстів програм.

г) Не слід зберігати розроблювальні чи супроводжувані програми в робочих бібліотеках вихідних текстів програм.

д) Відновлення бібліотек вихідних текстів програм і видача текстів програм програмістам повинні вироблятися тільки призначеним бібліотекарем після одержання санкції на доступ до додатка від керівника обслуговуючого персоналу.

е) Роздруківки програм варто зберігати в захищеному місці.

ж) Необхідно фіксувати усі випадки доступу до бібліотек вихідних текстів програм у контрольному журналі.

з) Застарілі версії вихідних текстів програм необхідно архівувати з чіткою вказівкою точної дати і часу їхнього використання разом із усім допоміжним програмним забезпеченням і інформацією про управління виконанням завдань, визначенням даних і процедур.

и) Супровід і копіювання бібліотек вихідних текстів програм необхідно здійснювати у відповідності зі строгими процедурами управління процесом внесення змін.

Вразливі системи можуть вимагати виділеного (ізольованого) обчислювального середовища. Деякі прикладні системи настільки уразливі стосовно можливої втрати даних, що вимагають спеціального запиту.

Уразливість може вказувати на необхідність запуску додатка на виділеному комп'ютері або поділу ресурсів тільки з надійними прикладними системами. Додаток також може не мати ніяких обмежень. Пропонуються наступні рекомендації:

а) Уразливість прикладної системи повинна бути явно визначена її власником і задокументована.

б) У випадку, коли уразливий додаток запускається в колективно використовуваному середовищі, необхідно ідентифікувати прикладні системи, з якими він буде розділяти ресурси, і погодити їхнє використання з власником цього додатка.

Спостереження за доступом до систем і їхнім використанням

Для забезпечення відповідності політиці управління доступом і стандартам необхідно стежити за системами.

Це необхідно для того, щоб визначити ефективність вжитих заходів і забезпечити відповідність моделі політики управління доступом.

Усі надзвичайні ситуації і події, пов'язані з порушенням режиму безпеки, необхідно реєструвати в контрольному журналі. Записи в такому журналі варто зберігати протягом заданого проміжку часу для надання допомоги в майбутніх розслідуваннях і здійсненні контролю за доступом. Крім відкинутих спроб входу в системи, доцільно також реєструвати випадки успішного доступу до них. Контрольний журнал повинний включати наступні дані:

· ідентифікатори користувачів;

· дата і час входу і виходу із системи;

· ідентифікатор місцезнаходження термінала (по можливості).

Необхідно встановити процедури спостереження за використанням систем.

Такі процедури вимагаються для забезпечення виконання користувачами тільки явно дозволених процесів. Рівень контролю, необхідний для окремих систем, варто визначити за допомогою незалежної оцінки ризиків. Необхідно розглянути наступні пункти:

· невдалі спроби доступу до систем;

· аналіз сеансу входу в систему на предмет виявлення несанкціонованого використання або відновлених користувальницьких ідентифікаторів;

· виділення і використання ресурсів із привілейованим доступом;

· відстеження окремих дій;

· використання конфіденційних ресурсів.

Усі дії, пов'язані зі спостереженням за системами, повинні бути формально дозволені керівництвом.

Для забезпечення точності контрольних журналів, що можуть знадобитися для розслідувань або як свідчення під час судових розглядів і при накладенні дисциплінарних стягнень, важливо правильно встановити системний годинник комп'ютерів. Неточні контрольні журнали можуть перешкодити таким розслідуванням і підірвати довіру до такого свідчення.

У тих випадках, коли комп'ютер або комунікаційний пристрій підтримує годинник реального часу, необхідно їх встановити відповідно до прийнятого стандарту.

Захист файлів прикладних систем

Підтримка цілісності прикладних систем повинна бути обов'язком користувача або групи розробки, якій прикладна система або програмне забезпечення належить.

Варто здійснювати твердий контроль за реалізацією програмного забезпечення в робочих системах. Щоб звести ризик ушкодження робочих систем до мінімуму, необхідно реалізувати наступні засоби контролю:

а) Відновленням робочих бібліотек програм повинний займатися тільки призначений бібліотекар після одержання санкції на доступ до додатка від керівника персоналу, що обслуговує інформаційні системи.

б) У робочих системах варто зберігати тільки виконувані програми (по можливості).

в) Виконувані програми не слід запускати на робочих системах доти, поки вони не пройдуть тестування і не будуть прийняті користувачами, а відповідні бібліотеки вихідних текстів програм не будуть оновлені.

г) Необхідно фіксувати усі випадки відновлення робочих бібліотек програм у контрольному журналі.

д) Попередні версії програм варто зберегти — запобіжний захід при надзвичайних ситуаціях.

Тестові дані необхідно захищати і контролювати. Тестування систем і їхнє приймання звичайно вимагають значні обсяги тестових даних, що близькі до реальних даних настільки, наскільки це можливо. Необхідно уникати використання реальних баз даних, що містять персональні дані. Перш ніж використовувати такі дані, їх необхідно знеособити. Для захисту реальних даних при їхньому використанні для цілей тестування, пропонуються наступні засоби контролю:

а) Процедури управління доступом, що застосовуються для робочих прикладних систем, повинні також застосовуватися для тестуючих прикладних систем.

б) Необхідно одержати окремий дозвіл усякий раз, коли реальні дані копіюються в тестуючу прикладну систему.

в) Реальні дані варто видалити з тестуючої прикладної системи відразу після завершення процесу тестування.

г) Випадки копіювання реальних даних необхідно реєструвати в контрольному журналі

**4. Перевірка безпеки інформаційних систем**

Усі підрозділи організації варто регулярно перевіряти, щоб забезпечити відповідність прийнятій політиці і стандартам безпеки. Перевірці підлягають:

а) інформаційні системи і їхні постачальники;

б) інформація і власники даних;

в) користувачі;

г) керівництво.

Власники інформаційних систем повинні організовувати регулярні перевірки своїх систем на відповідність прийнятій політиці безпеки, стандартам і іншим вимогам до їхнього захисту.

Інформаційні ресурси необхідно регулярно перевіряти на відповідність стандартам забезпечення безпеки. Технічна перевірка на таку відповідність містить у собі огляд робочих систем, щоб гарантувати правильну реалізацію засобів управління безпекою програмного й апаратного забезпечення. Цей вид перевірки вимагає звертання за технічною допомогою до фахівців. Така перевірка повинна проводитися досвідченим системним інженером вручну або автоматично за допомогою пакета програм, що створює технічний звіт для наступної обробки технічним фахівцем.

Такі перевірки повинні проводитися тільки компетентними законними особами або під їхнім спостереженням.

**4.1Аудит систем**

Для зведення ризику виникнення збоїв у виробничих процесах до мінімуму вимоги до аудита і роботи, пов'язані з перевіркою робочих систем, варто акуратно запланувати і погодити. Пропонується розглянути наступне:

а) Вимоги до аудита систем повинні бути погоджені з відповідним керівництвом.

б) Масштаб перевірок необхідно погодити і контролювати.

в) Перевірки повинні бути обмежені доступом до даних і програм тільки на читання.

г) Інші типи доступу (відмінні від доступу тільки на читання) повинні бути дозволені для окремих копій системних даних, які необхідно стерти по завершенні процесу аудита.

д) Необхідно явно ідентифікувати інформаційні ресурси для проведення перевірок і зробити їх доступними.

е) Необхідно визначити вимоги до спеціальної чи додаткової обробки і погодити їх з постачальниками послуг.

ж) Усі випадки доступу варто відслідковувати і фіксувати в контрольному журналі для довідок.

з) Усі процедури, вимоги й обов'язки необхідно задокументувати.

Доступ до засобів аудита систем, тобто до програм і файлів даних необхідно захищати, щоб запобігти їх можливому несанкціонованому використанню або компрометації. Такі засоби варто ізолювати від розроблювальних і робочих систем, і їх не слід зберігати в бібліотеках магнітних стрічок і на робочих місцях користувачів, якщо вони не забезпечені належним додатковим захистом.

Ефективний захист інформації є одним з найголовніших аспектів при побудові надійної інформаційної системи будь-якої організації.

Висновок

Системи контролю доступу призначені для обмеження і дозволу переміщення людей в приміщеннях, будівлях і по території об'єкту, що охороняється. Робота системи контролю доступу базується на зчитуванні кодів з ідентифікаторів і їх порівнянні з кодами (даними) закладеними в пам'яті системи для визначення права співробітника або гостя для проходу на територію, що охороняється.

Всім співробітникам, а також відвідувачам компанії, в якій встановлена система контролю доступу, видаються спеціальні електронні перепустки, наприклад, проксиміті ідентифікатори, у вигляді пластикових карток або брелоків, які містять персональні коди доступу. Зчитувачі встановлюються біля входу в контрольоване приміщення, розпізнають код ідентифікаторів. Інформація поступає в систему контролю доступу, яка на підставі аналізу даних про власника ідентифікатора, ухвалює рішення про допуск або заборону проходу співробітника на територію, що охороняється. У разі дозволу доступу, система приводить в дію виконавчі пристрої, такі як електромеханічні замки, турнікети, автоматичні шлагбауми або приводи воріт. Інакше двері блокуються, включається сигналізація і оповіщається охорона.

Системи контролю і управління доступом пройшли тривалий еволюційний шлях від простих кодонабірних пристроїв, керуючих дверним замком, до складних комп'ютерних систем, що охоплюють комплекси будівель, віддалених один від одного.

Сучасні системи контролю і управління доступом по своїх можливостях можуть забезпечити необхідний рівень охорони на крупних об'єктах, що містять сотні точок доступу і тисячі користувачів. Крім цього, системи служать основою для побудови інтегрованих систем безпеки, об'єднуючих охоронну і пожежну сигналізацію, засоби відео контролю і ін.

Системи контролю доступу можуть забезпечити наступний ряд можливостей:

* збір і обробку інформації про переміщення осіб по об'єкту;
* організацію і облік робочого часу;
* управління освітленням, ліфтами, вентиляцією і іншою сервісною автоматикою на об'єкті;
* управління режимами роботи і автоматикою автостоянок.

Автономні системи призначені для забезпечення контролю і управління доступом в окремі приміщення. Така система складається з автономного контроллера - мікропроцесорного приладу, що зберігає в собі базу даних ідентифікаторів і керує роботою решти елементів системи. Як виконавчий пристрій використовується електромагнітний замок, або клямка. Для ідентифікації користувача використовуються різні типи карт з відповідними зчитувачами (магнітні, проксиміті, штрихові).

Контроллер працює як правило з одним зчитувачем на вхід (зчитувач на вихід використовується лише в особливо важливих приміщеннях); для відкриття замку зсередини приміщення зазвичай використовується або кнопка, або датчик-комутатор руху. Для забезпечення правильності роботи всієї системи використовується датчик положення дверей. Для забезпечення нормального режиму роботи системи контролю доступу двері оснащуються доводчиком, а контролер - резервним джерелом живлення.

Мережеві системи призначені для забезпечення контролю і управління доступом на крупних об'єктах (банки, установи, підприємства). Виділяють чотири характерні типи точок доступу, де може бути застосований контроль:

* прохідні;
* офісні приміщення;
* приміщення з підвищеним рівнем безпеки;
* об'єкти на вулиці (ворота, шлагбауми для автостоянок і т.д.).
* Прохідні

Прохідні призначені для контролю доступу при вході на об'єкт. В більшості випадків тут використовуються турнікети або шлюзи, і як правило, присутня охорона, яка проводить додаткову візуальну перевірку і стежить за виникненням критичних ситуації. При великій кількості службовців виникають проблеми з пропускною спроможністю, тому додатковий контроль проводиться тільки для відвідувачів. Турнікети можуть бути напівростового типу, рідше використовуються турнікети з перекриттям отвору в повне зростання. Турнікети в більшості своїй не забезпечують фізичного перепону для проникнення, а служать тільки для впорядковування потоку людей і допомагають службі охорони контролювати вхід на об'єкт. Таким чином, основне їх завдання - обмежити можливість проходу декількох чоловік по одному пропуску (ідентифікатору). Турнікети можуть бути обладнані засобами сигналізації, що спрацьовують при спробах обходу (перестрибуванні). Для цього використовуються ІЧ - бар'єри, вагочутливі датчики та ін. Шлюзи або кабіни відносяться до пристроїв блокуючого типу, що перегороджують. Вони можуть при необхідності затримати людину в точці доступу. Шлюзи застосовуються на об'єктах з підвищеним рівнем безпеки. При цьому вони часто оснащуються додатковими засобами контролю (металлодетекторамі, детекторами вибухових і радіоактивних речовин і т.п.). На прохідних може виникнути потреба у відео контролі. При цьому введення коду, або зчитуванні ідентифікатора користувача, супроводжується виведенням зображень з бази даних і з відеокамери на монітор охоронця, (режим відеоідентифікації), який проводить їх порівняння. Для підвищення рівня безпеки застосовується дворівнева ідентифікація (наприклад, карта і код, карта і вага).

Офісні приміщення

Як правило, в самих офісних приміщеннях потрібний невисокий рівень захисту. Тут можна застосувати електромагнітні замки та зчитувачі дистанційного типу з великою відстанню зчитування (для того, щоб службовці не виймали картки з кишені - принцип вільних рук). Як виконавчі пристрої можуть застосовуватися електромагнітні клямки або електромагнітні замки.

Особливо важливі приміщення

У особливо важливих приміщеннях повинне застосовуватися багаторівневе встановлення особи (не менші два рівні), при необхідності - з біометричною ідентифікацією і клавіатурними зчитувачами. Тут також може використовуватися принцип "доступу двох або більше осіб". Клавіатурні зчитувачі, хоч і вважаються недостатньо захищеними від різних маніпуляцій (підбір коду, спостереження), мають певні переваги, наприклад, розрядність коду може бути вибрана довільно, причому код встановлюється користувачем і невідомий оператору системи.

Об'єкти на вулиці

Особливість даних об'єктів обумовлена застосуванням спеціальних пристроїв (автоматичні ворота, шлагбауми, протитаранні пристрої), що загороджують, а також спеціального кліматичного виконання зчитувачів і іншої апаратури для вуличної роботи. Як об'єкти контролю на вулиці може служити автотранспорт. Контроль доступу є невід'ємною частиною системи безпеки

Список використаних джерел:

1. <http://evgenius.nightmail.ru/publ.htm>
2. <http://ohrana-tera.com.ua/ua/sistemi_kontroly_dostupu.html>
3. <http://sst.kiev.ua/page_control_dostup.html>