Лекція 11. Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах (ІКС)

11.1. Процедури ідентифікації, автентифікації, авторизації користувачів.

11.2. Захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші).

11.3. Резервування інформації та компонентів інформаційно-телекомунікаційних системах.

11.1. Процедури ідентифікації, автентифікації, авторизації користувачів

Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах відбувається згідно закону України «Про захист інформації в інформаційно-комунікаційних системах». Відповідно до цього закону наводиться наступне визначення:

Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Для захисту інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах використовуються процедури ідентифікації, автентифікації й авторизації необхідні для підтвердження істинності суб'єкта, забезпечення його роботи в системі, і визначення законності прав суб'єкта на даний об'єкт або на визначені дії з ним.

Ідентифікація – це процес розпізнавання елемента системи, зазвичай за допомогою заздалегідь визначеного ідентифікатора або іншої унікальної інформації; кожний суб'єкт або об'єкт системи повинний бути однозначно ідентифікуємим.

Автентифікація – це перевірка істинності ідентифікації користувача, процесу, пристрою або іншого компоненту системи (звичайно здійснюється перед дозволом доступу); а також перевірка цілісності й авторства даних при їхньому збереженні або передачі для запобігання несанкціонованої модифікації.

Авторизація – це надання суб'єкту прав на доступ до об'єкта.

Приведемо приклад з доступом в онлайн-банкінг. Кожну дію користувача й системи розглянемо докладно.

Перебуваючи на сайті банку, користувач вирішує зайти в особистий кабінет, щоб зробити грошовий переказ. На сторінці особистого кабінету система спочатку просить ввести ідентифікатор. Це може бути логін, ім'я й прізвище, адреса електронної пошти або номер мобільного телефону.

Який конкретно вид даних необхідно ввести – залежить від ресурсу. Дані, які вказувалися при реєстрації, необхідно ввести для одержання доступу. Якщо при реєстрації вказувалося кілька типів даних – і логін, і адреса електронної пошти, і номер мобільного, то система сама підкаже що їй конкретно потрібно.

Введення цих даних необхідний для ідентифікації людини за монітором як користувача конкретно цього банку.

Якщо користувач як ідентифікатор увів «Олександр Ковальчук», і система знайшла у своїй базі запис про користувача з таким іменем, то ідентифікація завершилася.

Після ідентифікації випливає процес автентифікації, у якому користувачеві потрібно довести, що він є людиною, яка реєструвалася під іменем Олександр Ковальчук.

Для доказу необхідна наявність одного з типів автентифікаційних даних:

- Щось, властиве тільки користувачеві. Біометричні дані: сканери особи, відбитки пальців або сітківки ока.
- Щось, відоме тільки користувачеві. Сюди ставляться pin-коди, паролі, графічні ключі, секретні слова.
- Щось, наявне в користувача. У даній якості може виступати токен, тобто компактний пристрій, призначене для забезпечення інформаційної безпеки користувача, також використовується для ідентифікації власника. Найпростіші токени не вимагають фізичного підключення до комп'ютера – у них є дисплей, де відображається число, яке користувач уводить у систему для здійснення входу; більш складні підключаються до комп'ютерів за допомогою USB і Bluetooth-Інтерфейсів.

Найпоширеніший тип автентифікаційних даних – це пароль. Саме тому так важливо створювати й правильно зберігати свої паролі.

Після введення користувачем пароля система перевіряє: чи відповідає умовний пароль «Q45fp02@13» користувачеві з іменем Олександр Ковальчук. У такий спосіб відбувається автентифікація.

Якщо всі вірно, і пари логін-пароль вірні, то система надасть користувачеві доступ до його ресурсів і здійснення банківських операцій, тобто відбудеться авторизація.

Описані процеси завжди відбуваються тільки в такому порядку: ідентифікація, автентифікація, авторизація. Увесь ланцюжок втратить зміст, якщо, наприклад, сайт спочатку надасть доступ до коштів користувача, а потім буде уточнювати, чи він це насправді.

Процеси ідентифікації, автентифікації й авторизації характерні не тільки для онлайн-банкінгу, але й для електронної пошти, соціальних мереж і інших ресурсів.

Розглянемо яким чином реалізуються ці процедури.

Ідентифікація

Ідентифіка́ція: (лат. *identifico* – ототожнювати) – процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Ідентифікація використовується для отримання інформації про суб'єкт системи на основі наданого ним ідентифікатора. Є початковою процедурою надання доступу до системи. Після неї здійснюється автентифікація та авторизація.

Механізм ідентифікації

Ідентифікація дозволяє суб'єктові (користувачу, процесу, який діє від імені певного користувача) повідомити своє ім'я за допомогою унікального параметра – ідентифікатора (логін, наприклад), який є відомим іншій стороні. Під час ідентифікації здійснюється порівняння заявленого суб'єктом параметра на відповідність відомому іншій стороні. В разі успішної ідентифікації відбувається Автентифікація. Шляхом автентифікації інша сторона переконується що суб'єкт саме той за кого він себе видає (використовується пароль у випадку парольної автентифікації або інший секретний параметр).

Цифровий підпис

Цифровий підпис представлений у комп’ютері у вигляді ряду бінарних цифр. Він обчислюється з використанням таких правил і наборів параметрів, згідно з якими можна перевірити особу, що підписала, і цілісність даних. Цифровий підпис робиться з використанням криптографічної технології, що відома як Криптографія відкритого ключа, на основі унікально зв’язаних пар цифр, де один ключ застосовується для створення підпису (приватний ключ), а другий – для підтвердження підпису (відкритий ключ). В основі цифрового підпису лежать два процеси: генерування підпису і перевірка підпису. При генеруванні підпису застосовується приватний ключ для отримання цифрового підпису. В процесі перевірки підпису використовується відкритий ключ, який відповідає приватному ключу. В кожного користувача є пара ключів підпису: приватний і відкритий. Вважається, що відкриті ключі можуть бути відомі широкому колу осіб. Приватними ж ключами не діляться ні з ким. Кожен може перевірити підпис користувача за допомогою відкритого ключа, що належить цьому користувачу. Зв’язок між відкритим і приватним ключами такий, що неможливо отримати ключ за допомогою розрахунків на основі ключа перевірки.

Інфраструктура відкритого ключа (ІВК) сприяє управлінню і розповсюдженню цим ключем. Цифровий підпис може бути підрозділений на три алгоритми по відношенню до генерування і перевірки, і далі подано їх опис.

Таблиця 11.1 – Приклади ідентифікації

Варіант ідентифікації	**Чинники автентифікації**	**Результат ідентифікації (ідентифікатор)**
Ідентифікація користувача	1) Логін/пароль («я знаю»)	Логін
Ідентифікація по банківській карті	1) мікропроцесорна банківська карта («я маю»); 2) ПІН-код («я знаю»)	Обліковий номер картки (PAN) – зчитується з банківської картки
Ідентифікація по банківській картці з біоверифікацією	1) мікропроцесорна банківська карта («я маю»); 2) біометричний фактор (відбиток пальця) («я є»)	Обліковий номер картки (PAN) – зчитується з банківської картки
Ідентифікація товару за штрих-кодом	1) штрих-код («я маю»)	Обліковий номер товару
Ідентифікація файлу за контрольною сумою	1) контрольна сума («я є»)	ім'я файлу
Ідентифікація громадянина з електронного підпису	1) носій електронного підпису («я маю»); 2) пароль доступу до носія («я знаю»)	Ідентифікатор сертифіката (СНІЛС – для сертифіката ключа перевірки кваліфікованого електронного підпису)

Присвоєння суб'єкту ідентифікатора (тобто реєстрацію суб'єкта в інформаційній системі) іноді також називають ідентифікацією.

Автентифікація

Автентифіка́ція (з грец. αυθεντικός; реальний або істинний) – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора..

З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

Механізм автентифікації

Один із способів автентифікації в інформаційній системі полягає у попередній ідентифікації на основі користувацького ідентифікатора («логіна», від англ. *login* – реєстраційного імені користувача) і пароля – певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом в мережі. Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх зі значенням, яке зберігається в спеціальній захищеній базі даних і,

у випадку успішної автентифікації проводить авторизацію з подальшим допуском користувача до роботи в системі.

Види автентифікації

Слабка автентифікація

Традиційну автентифікацію за допомогою пароля називають ще однофакторною або слабкою, оскільки, за наявності певних ресурсів, перехоплення або підбір пароля є справою часу. Не останню роль в цьому грає людський чинник – чим стійкішим до злому методом підбору є пароль, тим важче його запам'ятати людині і тим вища ймовірність, що він буде додатково записаний, що підвищить ймовірність його перехоплення або викрадення. І навпаки – легкі для запам'ятовування паролі (наприклад, часто вживані слова або фрази, дати народження, імена близьких, назви моніторів чи найближчого обладнання) в плані стійкості до злому є дуже не вдалими. Як вихід, впроваджуються одноразові паролі, проте їхнє перехоплення також можливе.

Багатофакторна автентифікація

Автентифікація, що здійснюється з використанням двох чи більше факторів.

Багатофакторна автентифікація (**БФА**, англ. *multi-factor authentication*, MFA) – розширена автентифікація, метод контролю доступу до комп'ютера, в якому користувачеві для отримання доступу до інформації необхідно пред'явити більше одного «доказу механізму автентифікації». До категорій таких доказів відносять:

- Знання – інформація, яку знає суб'єкт. Наприклад, пароль, пін-код.
- Володіння – річ, якою володіє суб'єкт. Наприклад, електронна або магнітна карта, токен, флеш-пам'ять.
- Властивість, якою володіє суб'єкт. Наприклад, біометрія, унікальні природні відмінності: обличчя, відбитки пальців, райдужна оболонка очей, капілярні візерунки, послідовність ДНК.

Фактори автентифікації

Ще до появи комп'ютерів використовувалися різні відмінні риси суб'єкта, його характеристики. Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності та вартості впровадження. Виділяють 3 фактори автентифікації:

- **Фактор знання, щось, що ми знаємо – пароль**. Це таємні відомості, якими повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замку або особистий ідентифікаційний номер (PIN). Парольний механізм може бути досить легко втілений і має низьку вартість. Але має суттєві недоліки: зберегти пароль у таємниці часто буває складно, зловмисники постійно вигадують нові способи крадіжки, злому і підбору пароля (див. бандитський криптоаналіз, метод грубої сили). Це робить парольний механізм слабозахищеним. Велика кількість секретних питань, такі як «Де ви народилися?», елементарні приклади фактора знань, тому що вони можуть бути відомі широкому загалу людей, або бути досліджені.

– **Фактор володіння, щось, що ми маємо – пристрій автентифікації**. Тут важлива сама обставина володіння суб'єктом якимось особливим предметом. Це може бути особиста печатка, ключ від замка, для комп'ютера це файл даних, що містять характеристику. Характеристика часто вбудовується в особливий пристрій автентифікації, наприклад, пластикова картка, смарт-картка. Для зловмисника роздобути такий пристрій стає більш складно, ніж зламати пароль, а суб'єкт може відразу ж повідомити в разі крадіжки пристрою. Це робить даний метод більш захищеним, ніж парольний механізм, проте вартість такої системи більш висока.

– **Фактор властивості, щось, що є частиною нас – біометрика**. Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос або особливість очка. З точки зору суб'єкта, даний спосіб є найбільш простим: не треба запам'ятовувати пароль, ні переносити з собою пристрій автентифікації. Однак біометрична система повинна володіти високою чутливістю, щоб підтверджувати авторизованого користувача, але відкидати зловмисника зі схожими біометричними параметрами. Також вартість такої системи досить велика. Але, незважаючи на свої недоліки, біометрика залишається досить перспективним фактором.

Безпека

Багатофакторна автентифікація може істотно зменшити імовірність викрадення особистих даних в інтернеті, оскільки знання пароля жертви недостатньо для здійснення шахрайства. Тим не менш, в залежності від реалізації, системи з багатофакторною автентифікацією можуть бути вразливими для атак типу «фішингу», «людина-в-браузері», «людина посередині», тощо.

Вибираючи для системи той чи інший фактор або спосіб автентифікації, необхідно, насамперед, відштовхуватися від необхідної ступеня захищеності, вартості побудови системи, забезпечення мобільності суб'єкта.

Таблиця 11.2 – Таблиця для порівняння

Рівень ризику	**Вимоги до системи**	**Технологія автентифікації**	**Приклади застосування**
Низький	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційних відомостей **не будуть мати значних наслідків**	Рекомендується мінімальна вимога – використання багаторазових паролів	Реєстрація на порталі в мережі Інтернет

Середній	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційних відомостей заподіють **невеликий збиток**	Рекомендується мінімальна вимога – використання одноразових паролів	Здійснення банківських операцій
Високий	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційних відомостей завдадуть **значної шкоди**	Рекомендується мінімальна вимога – використання багатофакторної автентифікації	Проведення великих міжбанківських операцій керівним апаратом

Двофакторна автентифікація

Двофакторна автентифікація (**ДФА**, англ. *two-factor authentication*, також відома як *двоетапна верифікація*), є типом багатофакторної автентифікації. ДФА – представляє собою технологію, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів.

Хорошим прикладом двофакторної автентифікації є авторизація Google і Microsoft. Коли користувач заходить з нового пристрою, крім автентифікації по імені та паролю, його просять ввести шестизначний (Google) або восьмизначний (Microsoft) код підтвердження. Ви можете отримати його за допомогою SMS, або голосового дзвінка на ваш телефон, він може бути взятий з заздалегідь складеного реєстру разових кодів або ви можете використовувати додаток-автентифікатор, генеруючий новий одноразовий пароль за короткі проміжки часу. Вибрати один з методів можна в налаштуваннях вашого Google або Microsoft-акаунта.

Перевага двофакторної автентифікації через мобільний пристрій:

– Не потрібні додаткові токени, тому що мобільний пристрій завжди під рукою.

– Код підтвердження постійно змінюється, а це безпечніше, ніж однофакторний логін-пароль

Недоліки двофакторної автентифікації через мобільний пристрій:

– Мобільний телефон повинен ловити мережу, коли відбувається автентифікація, інакше повідомлення з паролем просто не дійде.

– Ви ділитеся з кимось вашим мобільним телефоном, що впливає на ваше особисте життя і може бути в майбутньому на нього буде приходити спам.

– Текстові повідомлення (SMS), які, потрапляючи на ваш мобільний телефон, можуть бути перехоплені.

– Текстові повідомлення приходять з деякою затримкою, так як деякий час йде на перевірку.

– Сучасні смартфони використовуються як для одержання пошти, так і для отримання SMS. Як правило електронна пошта на мобільному телефоні завжди включена. Таким чином, усі акаунти, для яких пошта є ключем, можуть бути зламані (перший фактор). Мобільний пристрій (другий фактор). Висновок: смартфон змішує два чинника в один.

Зараз майже всі великі сервіси, такі як Microsoft, Google, Yandex, Dropbox, Facebook, вже надають можливість використовувати двофакторну автентифікацію. Причому для всіх з них можна використовувати єдиний додаток *автентифікатор*, що відповідає певним стандартам, такі як Google Authenticator, Microsoft Authentificator, Authy або FreeOTP.

Законодавство та регулювання

Стандарт безпеки даних для індустрії платіжних карток (PCI), вимога 8.3, вимагає використання багатофакторної автентифікації (MFA) для всього віддаленого доступу до мережі, що походить із-за межі мережі, до середовища даних карт (CDE). Починаючи з PCI-DSS версії 3.2, використання MFA потрібне для будь-якого адміністративного доступу до CDE, навіть якщо користувач знаходиться в межах надійної мережі.

Практична реалізація

Багато продуктів з функцією багатофакторної автентифікації вимагають від користувача клієнтське програмне забезпечення, для того, щоб система багатофакторної автентифікації запрацювала. Деякі розробники створили окремі настановні пакети для входу в мережу, ідентифікаційних даних веб-доступу VPN-підключення. Щоб використовувати з цими продуктами токен або смарт-карту, потрібно встановити на PC чотири або п'ять пакетів спеціального програмного забезпечення. Це можуть бути пакети, які використовуються для здійснення контролю версії або це можуть бути пакети для перевірки конфліктів з бізнес-додатками. Якщо доступ може бути проведений з використанням вебсторінок, то тоді можна обійтися без непередбачених витрат. З іншими програмними рішеннями багатофакторної автентифікації, такими як «віртуальні» токени або деякі апаратні токени, жодне не може бути встановлено безпосередніми користувачами.

Багатофакторна автентифікація не стандартизована. Існують різні форми її реалізації. Отже, проблема полягає в її здатності до взаємодії. Існує багато процесів і аспектів, які необхідно враховувати при виборі, розробці, тестуванні, впровадженні та підтримці цілісної системи управління ідентифікацією безпеки, включаючи всі релевантні механізми автентифікації і супутніх технологій: це все описав Brent Williams, в контексті «Identity Lifecycle»

Багатофакторна автентифікація має ряд недоліків, які перешкоджають її поширенню. Зокрема людині, яка не розбирається в цій області, складно стежити за розвитком апаратних токенів або USB-штекерів. Багато користувачів не можуть самостійно встановити сертифіковане програмне забезпечення, так як не володіють відповідними технічними навичками. Загалом, багатофакторні рішення вимагають додаткових витрат на встановлення та оплату експлуатаційних витрат. Багато апаратні комплекси, засновані на токенах,

запатентовані, і деякі розробники стягують з користувачів щорічну плату. З точки зору логістики, розмістити апаратні токени важко, так як вони можуть бути пошкоджені або втрачені. Випуск токенів в таких областях, як банки, або інших великих підприємствах повинен бути відрегульований. Крім витрат на установку багатофакторної автентифікації значну суму також становить оплата технічного обслуговування.

Посилена автентифікація

У відповідності до вимог Європейської директиви PSD2 в платіжних системах використовується так звана посилена автентифікація, коли для автентифікації використовуються принаймні два різних типи факторів. Типами факторів є:

– властивість, якою володіє суб'єкт;
– знання – інформація, яку знає суб'єкт;
– володіння – річ, якою володіє суб'єкт.

Сувора автентифікація

Автентифікація, під час якої використовується інформація без розкриття цієї інформації. Як правило, реалізується за допомогою асиметричних криптографічних алгоритмів.

Способи автентифікації

Парольна

Здійснюється на основі володіння користувачем певною конфіденційною інформацією.

Біометрична

Біометрична автентифікація основана на унікальності певних антропометричних характеристик людини. У галузі інформаційних технологій термін біометрія застосовується в значенні технології ідентифікації особистості. Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів. Найчастіше використовуються:

1. Параметри голосу.
2. Візерунок райдужної оболонки ока і карта сітківки ока – Автентифікація за райдужною оболонкою ока.
3. Риси обличчя.
4. Форма долоні.
5. Відбитки пальців.
6. Форма і спосіб особистого підпису – Електронний цифровий підпис, Верифікація підпису.

Етапи

Основні етапи проектування системи біометричної автентифікації на основі динамічного підпису в цілому. Розробка математичної моделі динамічного підпису і методів його обробки. Реалізація алгоритму роботи модуля автентифікації системи на основі створеної математичної моделі і методів обробки. Реалізація системи автентифікації у складі інформаційної

системи. Тестування системи автентифікації. Модифікація коду фрагментів системи у процесі функціонування системи.

Перший етап – проектування, полягає у аналізі вимог, які ставляться до системи і на їх основі проектується архітектура системи автентифікації в цілому. Враховується сфера застосування системи, зокрема задається її точність, надійність, зручність; операційна система (ОС) у якій буде функціонувати ПЗ та інші параметри. У випадку розробки універсальної системи необхідно передбачити можливість зміни цих параметрів інтегратором (адміністратором) системи, а також бажано розробляти кросплатформенне ПЗ, незалежне від ОС. Розробити рольову модель роботи системи – скористатися апаратом об'єктно-орієнтованого аналізу і об'єктно-орієнтованого проектування. Рекомендується використовувати уніфіковану мову програмування UML для проектування і моделювання інформаційної системи, а також дотримуватися наступних принципів: модульність – кожна компонента системи є модулем, який просто модифікується, замінюється і виконує відведену йому специфічну роль; підтримка відкритих стандартизованих протоколів для передачі даних, взаємодії об'єктів і форматів збереження файлів; документованість – усі методи (функції), класи, об'єкти детально і доступно документувати.

Другий етап – розробка математичної моделі є ключовим. Необхідно вдало підібрати підхід до побудови моделі: стохастичний чи детермінований, на думку авторів це стохастичний підхід. Розробка математичної моделі передбачає: розробку моделі, яка враховувала б ключові особливості об'єкта дослідження і вибір діагностичних ознак; проведення аналізу цих діагностичних ознак і розробка методів для попередньої обробки. У випадку використання статистичного підходу – дослідити статистичні характеристики діагностичних ознак. Ці дослідження дозволяють зробити висновки про адекватність моделі.

Третій етап – на основі математичної моделі розробляється алгоритм, який реалізується на деякій мові програмування. Особливу увагу слід привернути на реалізацію системи вводу підпису

За допомогою унікального предмета

Здійснюється за допомогою додаткових предметів (токен автентифікації, смарт-карта) або атрибутів (криптографічний сертифікат).

Протоколи автентифікації

Протоколи автентифікації – категорія криптографічних протоколів, які забезпечують надійну автентифікацію особи.

Існує багато різноманітних протоколів автентифікації:

- AKA.
- CAVE-based authentication.
- Challenge-handshake authentication protocol (CHAP).
- CRAM-MD5.
- Diameter.
- EAP.
- Host Identity Protocol (HIP).
- Kerberos.

- MS-CHAP і MS-CHAPv2 різновиди CHAP.
- LAN Manager.
- NTLM, також відомий як NT LAN Manager.
- Password-authenticated key agreement протоколи.
- Password Authentication Protocol (PAP).
- Protected Extensible Authentication Protocol (PEAP).
- RADIUS.
- Secure Remote Password protocol (SRP).
- TACACS і TACACS+.
- RFID-Authentication Protocols.
- Woo Lam 92 (protocol).
- Протокол Нідхема-Шредера.

Авторизація

Авторизація – керування рівнями та засобами доступу до певного захищеного ресурсу, як у фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних. З позицій інформаційної безпеки Авторизація є частиною процедури надання доступу для роботи в інформаційній системі, після ідентифікації і автентифікації.

11.2. Захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші)

Формальне визначення політики безпеки називають математичною моделлю безпеки. Згідно вимог нормативних документів у галузі захисту інформації в інформаційних системах, системи захисту інформації будують на основі математичних моделей захисту інформації. Використання цих моделей дозволяє теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки. Формальна теорія захисту інформації почала розвиватися відносно недавно, але сьогодні існує багато математичних моделей, які описують різні аспекти безпеки і надають доказову теоретичну базу для побудови сучасних систем захисту інформації

Захист інформації за допомогою кінцевих автоматів

Кінцевий або Скінче́нний автома́т (англ. *finite-state machine*, машина зі скінченною кількістю станів) – особливий різновид автомата – абстракції, що використовується для опису шляху зміни стану об'єкта в залежності від поточного стану та інформації отриманої ззовні. Його особливістю є скінченність множини станів автомату.

Кінцеві автомати – з погляду інформатики це автомати, які є дискретні перетворювачі інформації. До них відносяться перетворювачі, в яких міститься кінцева множина вхідних і кінцеве вихідних сигналів, а також кінцева множина внутрішніх станів

Поняття скінченного автомата було запропоновано як математичну модель технічних приладів дискретної дії, оскільки будь-який такий пристрій (в силу скінченності своїх розмірів) може мати тільки скінченну кількість станів.

Виявлення кіберзагроз з використанням моделі кінцевих автоматів засноване на моделюванні кінцевими автоматами процесів інформаційної взаємодії абонентів інформаційної системи (ІС) за протоколами передачі даних. Кінцевий автомат описується множинами вхідних даних, вихідних даних і внутрішніх станів. Кіберзагрози фіксуються по «аномальним» переходам ІС зі стану в стан. Передбачається, що в ІС «штатні» переходи системи зі стану в стан визначено, а невідомі стану і переходи в ці стану реєструються як аномальні. Перевагою цієї моделі є спрощений підбір класифікаційних ознак для ІС та розгляд малого числа переходів зі стану в стан. Модель дозволяє виявляти кіберзагрози в потоці обробки даних мережевими протоколами в режимі близькому до реального масштабу часу. До недоліків моделі слід віднести необхідність розробки великого числа складних експертних правил для порівняльного аналізу необхідних і аномальних станів і переходів системи. Експертні правила оцінки станів ІС взаємопов'язані з характеристиками мережевих протоколів передачі даних

Захист інформації за допомогою управління потоками

Однією з основних функцій системи розмежування доступу є управління потоками даних з метою запобігання запису даних на носії невідповідного рівня. Для цього використовується **політика безпеки інформаційних потоків**.

Крім керування доступом суб’єктів до об’єктів системи проблема захисту інформації має ще один аспект. Для одержання інформації про який-небудь об’єкт системи зовсім необов'язково шукати шляхи несанкціонованого доступу до нього. Необхідну інформацію можна одержати, спостерігаючи за обробкою необхідного об'єкта, тобто використовуючи канали витоку інформації. У системі завжди існують інформаційні потоки. Тому адміністраторові необхідно визначити, які інформаційні потоки в системі є «легальними», тобто не ведуть до витоку інформації, а як-ведуть до витоку. Тому виникає необхідність розробки правил, що регламентують керування інформаційними потоками в системі. Звичайне керування інформаційними потоками застосовується в рамках виборчої або повноважної політики, доповнюючи їх і сприяючи підвищенню надійності системи захисту.

Захист інформації за допомогою моделі безпеки Bell-LaPadula

Основна теорема безпеки Белла-Лападули вказує, що якщо інформаційна система стартує роботу з безпечного стану і перехід зі стану в стан безпечний, то всі стан системи безпечні.

Модель **Белла-ЛаПадули (BLP)** – це модель кінцевого автомата, яка використовується для забезпечення контролю доступу в державних і військових програмах. Він був розроблений Девідом Елліоттом Беллом і Леонардом Дж. ЛаПадулою за чіткими вказівками Роджера Р. Шелла, щоб формалізувати політику багаторівневої безпеки (MLS) Міністерства оборони США (DoD). Модель є формальною моделлю переходу між станами політики комп'ютерної безпекиякий описує набір правил контролю доступу, які використовують мітки безпеки на об'єктах і дозволи для суб'єктів. Мітки безпеки варіюються від найбільш конфіденційних (наприклад, «Цілком таємно») до найменш чутливих (наприклад, «Несекретно» або «Публічно»).

Модель Белла-ЛаПадули є прикладом моделі, де немає чіткого розмежування між захистом і безпекою.

Особливості

Модель Белла-ЛаПадули фокусується на конфіденційності даних і контрольованому доступі до секретної інформації, на відміну від моделі цілісності Біби, яка описує правила захисту цілісності даних. У цій формальній моделі сутності інформаційної системи поділяються на суб'єкти та об'єкти. Визначено поняття « безпечний стан » і доведено, що кожен перехід стану зберігає безпеку шляхом переходу від безпечного стану до безпечного стану, таким чином індуктивно доводячи, що система задовольняє цілі безпеки моделі. Модель Белла-ЛаПадули побудована на концепції кінцевої машини з набором допустимих станів в комп'ютерній системі. Перехід з одного стану в інший визначається функціями переходу. Стан системи визначається як «безпечний», якщо єдині дозволені режими доступу суб'єктів до об'єктів відповідають політиці безпеки. Щоб визначити, чи дозволений певний режим доступу, дозвіл суб'єкта порівнюється з класифікацією об'єкта (точніше, з комбінацією класифікації та набору відсіків, що становить рівень *безпеки*), щоб визначити, чи суб'єкт авторизований для конкретного режиму доступу. Схема очищення/класифікації виражається в термінах решітки. Модель визначає одне правило дискреційного контролю доступу (DAC) і два обов'язкових контролю доступу(MAC) правила з трьома властивостями безпеки:

1. Проста властивість безпеки стверджує, що суб'єкт із даним рівнем безпеки може не читати об'єкт із вищим рівнем безпеки.

2. Властивість безпеки * (зірочка) вказує на те, що суб'єкт із даним рівнем безпеки не може писати в будь-який об'єкт із нижчим рівнем безпеки.

3. Властивість дискреційної безпеки використовує матрицю доступу для визначення дискреційного керування доступом.

Передача інформації з документа високої конфіденційності до документа меншої конфіденційності може відбуватися в моделі Белла-ЛаПадули через концепцію довірених суб'єктів. Довірені суб'єкти не обмежені власністю Star. Довірені суб'єкти мають бути продемонстровані як надійні щодо політики безпеки.

Модель безпеки Белла-ЛаПадули спрямована на контроль доступу та характеризується фразою «записати, прочитати» (WURD).

За допомогою Bell–LaPadula користувачі можуть створювати вміст лише на своєму власному рівні безпеки або вище (тобто секретні дослідники можуть створювати секретні чи надсекретні файли, але не можуть створювати загальнодоступні файли; без запису). І навпаки, користувачі можуть переглядати вміст лише на рівні безпеки або нижчому (тобто секретні дослідники можуть переглядати загальнодоступні чи секретні файли, але не можуть переглядати надсекретні файли; читання неможливе).

Модель Белла-ЛаПадули чітко визначила її сферу застосування. Він не розглядав наступне широко:

– Приховані канали. Коротко описано передачу інформації за допомогою заздалегідь обумовлених дій.

– Мережі систем. Пізніша модельна робота справді торкалася цієї теми.

– Політики за межами багаторівневої безпеки. Робота на початку 1990-х років показала, що MLS є однією з версій булевих політик, як і всі інші опубліковані політики.

Властивості

Властивість Strong Star

Модель Белла-ЛаПадули є моделлю розмежування доступу до інформації, що захищається. Вона описується скінченним автоматом з допустимим набором станів, у яких може знаходитись інформаційна система. Усі елементи у складі інформаційної системи поділені на суб'єкти і об'єкти. Кожному суб'єкту приписується рівень доступу, який відповідає рівню конфіденційності. Аналогічно об'єкту надається рівень таємності. Поняття захищеної визначається наступним чином: кожен стан системи повинен відповідати політиці безпеки, встановленої для даної інформаційної системи. Перехід між станами описується функціями переходу. Система знаходиться у безпечному стані тільки у тому випадку, коли у кожного суб'єкта наявний доступ тільки до тих об'єктів, до яких від дозволений на основі поточної політики безпеки. Для визначення права доступу суб'єкта до об'єкта рівень доступу суб'єкта порівнюється з рівнем таємності об'єкта, і на підставі цього приймається рішення щодо надання запитаного рівня доступу. Набори рівень доступу/рівень таємності описуються матрицею доступу. Основними правилами, що забезпечують розмежування доступу, є:

Проста властивість безпеки (The Simple Security)

Суб'єкт з рівнем доступу x_s може читати інформацію з об'єкта з рівнем таємності x_o тоді і тільки тоді, коли x_sперевищує x_o. Це правило також відоме під назвою «Немає читання зверху» (No read up, NRU). Наприклад, суб'єкт, який має доступ лише до нетаємних даних, спробує прочитати об'єкт з рівнем «цілком таємно», то йому буде відмовлено.

Властивість ★ (The ★-property)

Сутність властивості ★ (читається як «властивість зірочка») полягає у тому, що суб'єкт з рівнем доступу $_s$ може писати інформацію у об'єкт з рівнем таємності x_o тільки якщо x_o перевищує x_s. Це правило також відоме під назвою «Немає запису вниз» (No write down, NWD). Наприклад, якщо суб'єкт, який має

рівень доступу «цілком таємно» спробує записати у об'єкт з рівнем таємності «таємно», то йому буде відмовлено у цьому.

Сильна властивість ★ (Strong ★ Property)

Сильна властивість ★ є альтернативною властивості ★, у якій суб'єкти можуть писати у об'єкти тільки з тим рівнем таємності, що відповідає рівню доступу суб'єкта. Таким чином, операція запису вгору, присутня при властивості ★, відсутня, а лише наявна операція запису у об'єкти з тим же рівнем доступу. Сильна властивість ★ зазвичай згадується у контексті багаторівневих систем керування базами даних і обумовлена вимогами цілісності[4]. Сильна властивість ★ передбачається моделлю Біби, де було показано, що стійка цілісність у поєднанні з моделлю Белла-ЛаПадули забезпечується читанням і записом у межах єдиного рівня таємності.

Принцип стійкості

Принцип стійкості моделі Белла-ЛаПадули стверджує, що рівень таємності/доступу суб'єкта або об'єкта не змінюється під час звернення. Є дві форми принципу стійкості. Принцип сильної стійкості стверджує, що рівень безпеки не зміниться під час нормальної роботи системи. Принцип слабкої стійкості стверджує, що рівень безпеки неможливо змінити таким чином, що порушилась політика безпеки. Принцип слабкої стійкості дозволяє дотримуватися принципу мінімуму повноважень у системі. Тобто процеси починаються з низьким рівнем ознайомленості, незалежно від рівня ознайомленості їх власників, і у процесах поступово накопичуються більш високі рівні обізнаності, по мірі потреби у діях, які вимагають підвищення рівня обізнаності.

Захист інформації за допомогою моделі безпеки Biba

Модель **Biba** або Модель **цілісності Biba**, розроблена Кеннетом Дж. Бібою в 1975 році, є формальною системою переходу між станами політики комп’ютерної безпеки, яка описує набір правил контролю доступу, призначених для забезпечення цілісності даних. Дані та суб’єкти групуються в упорядковані рівні цілісності. Модель розроблена таким чином, що суб’єкти не можуть пошкодити дані на рівні, вищому за суб’єкта, або бути зіпсованими даними з нижчого рівня, ніж суб’єкт.

Загалом модель була розроблена для розгляду цілісності як основного принципу, який є прямою протилежністю моделі Белла-ЛаПадули.

Особливості

Загалом, збереження *цілісності* даних має три цілі:

– Запобігайте зміні даних неавторизованими сторонами.

– Запобігайте неавторизованій зміні даних авторизованими сторонами.

– Підтримувати внутрішню та зовнішню узгодженість (тобто дані відображають реальний світ).

Ця модель безпеки спрямована на *цілісність* даних (а не на *конфіденційність*) і характеризується фразою: «читай, записуй». Це на відміну від моделі Белла-ЛаПадули, яка характеризується фразою «читай, записуй».

У моделі Biba користувачі можуть *створювати вміст лише на* рівні власної цілісності або нижче (ченець може написати молитовник, який можуть читати простолюдини, але не такий, який читатиме первосвященик). І навпаки, користувачі можуть *переглядати вміст лише на* рівні власної цілісності або вище (монах може читати книгу, написану первосвящеником, але не може читати брошуру, написану простолюдином). Інша аналогія, яку слід розглянути, це ланка військового командування. Генерал може писати накази полковнику, який може віддавати ці накази майору. Таким чином оригінальні накази генерала зберігаються недоторканими, а місія військових захищена (таким чином, «читайте» цілісність). І навпаки, рядовий ніколи не може віддавати накази своєму сержанту, який ніколи не може віддавати накази лейтенанту, також захищаючи цілісність місії («записати»).

Модель Біба визначає набір правил безпеки, перші два з яких подібні до моделі Белла-ЛаПадули. Ці перші два правила є протилежними правилам Белла-ЛаПадули:

1. Проста властивість цілісності стверджує, що суб'єкт із заданим рівнем цілісності не повинен зчитувати дані з нижчим рівнем цілісності (*без зчитування*).

2. Властивість цілісності * (зірочка) вказує на те, що суб'єкт із заданим рівнем цілісності не повинен записувати дані з вищим рівнем цілісності (*не записувати*).

3. Властивість виклику стверджує, що процес знизу не може запитувати вищий доступ; лише з предметами рівного або нижчого рівня.

Захист інформації за допомогою моделі безпеки Clark-Wilson

Модель цілісності **Кларка-Вілсона** забезпечує основу для визначення та аналізу політики цілісності для обчислювальної системи.

Модель в першу чергу стосується формалізації поняття інформаційної цілісності. Цілісність інформації підтримується шляхом запобігання пошкодженню елементів даних у системі через помилку або зловмисний намір. Політика цілісності описує, як елементи даних у системі повинні підтримуватися дійсними від одного стану системи до наступного, і визначає можливості різних принципалів у системі. Модель використовує мітки безпеки для надання доступу до об'єктів за допомогою процедур трансформації та моделі обмеженого інтерфейсу.

Модель була описана в статті 1987 року (*Порівняння комерційної та військової політики комп'ютерної безпеки*) Девіда Д. Кларка та Девіда Р. Вілсона. У статті розроблено модель як спосіб формалізації поняття цілісності інформації, особливо порівняно з вимогами до систем багаторівневої безпеки (MLS), описаними в Помаранчевій книзі. Кларк і Вілсон стверджують, що існуючі моделі цілісності, такі як Biba (читання/запис), краще підходили для забезпечення цілісності даних, а не конфіденційності інформації. Біба-моделі є більш корисними, наприклад, у системах банківської класифікації, щоб запобігти ненадійній модифікації інформації та спотворенню інформації на вищих рівнях класифікації. Навпаки, **Кларка–Вілсона** більш чітко можна застосувати до

бізнес-процесів і галузевих процесів, у яких цілісність інформаційного вмісту має першочергове значення на будь-якому рівні класифікації (хоча автори підкреслюють, що всі три моделі, очевидно, корисні як урядовим, так і промисловим організаціям).

Основні принципи

Відповідно до навчального посібника CISSP Стюарта та Чеппла, *шосте видання*, модель Кларка–Вілсона використовує багатогранний підхід для забезпечення цілісності даних. Замість визначення формального кінцевого автомата, модель визначає кожен елемент даних і дозволяє модифікувати лише невеликий набір програм. Модель використовує зв'язок із трьох частин суб'єкт/програма/об'єкт (де програма взаємозамінна з транзакцією), відомий як *трійка* або *трійка контролю доступу.* У межах цього відношення суб'єкти не мають прямого доступу до об'єктів. Доступ до об'єктів можливий лише через програми. Подивіться тут, щоб побачити, чим це відрізняється від інших моделей контролю доступу.

Правила застосування та сертифікації моделі визначають елементи даних і процеси, які є основою для політики цілісності. Ядро моделі базується на понятті транзакції.

– Добре сформована транзакція – це серія операцій, які переводять систему з одного узгодженого стану в інший узгоджений стан.

– У цій моделі політика цілісності стосується цілісності транзакцій.

– Принцип розподілу обов'язків вимагає, щоб засвідчувач транзакції та виконавець були різними особами.

Модель містить ряд базових конструкцій, які представляють як елементи даних, так і процеси, які працюють з цими елементами даних. Ключовим типом даних у моделі Кларка–Вілсона є обмежений елемент даних (CDI). Процедура перевірки цілісності (IVP) гарантує, що всі CDI в системі дійсні в певному стані. Транзакції, які забезпечують дотримання політики цілісності, представлені процедурами перетворення (TP). TP приймає як вхідні дані CDI або Unconstrained Data Item (UDI) і створює CDI. TP має перевести систему з одного дійсного стану в інший. UDI представляють вхідні дані системи (наприклад, дані, надані користувачем або зловмисником). TP має гарантувати (через сертифікацію), що він перетворює всі можливі значення UDI на «безпечний» CDI.

Правила

В основі моделі лежить поняття зв'язку між автентифікованим принципалом (тобто користувачем) і набором програм (тобто TP), які працюють з набором елементів даних (наприклад, UDI та CDI). Компоненти такого відношення, взяті разом, називають *трійкою Кларка–Вілсона.* Модель також має гарантувати, що різні сутності відповідають за маніпулювання зв'язками між принципалами, транзакціями та елементами даних. Як короткий приклад, користувач, здатний сертифікувати або створювати відношення, не повинен мати можливість виконувати програми, вказані в цьому відношенні.

Модель складається з двох наборів правил: правил сертифікації (C) і правил виконання (E). Дев'ять правил забезпечують зовнішню та внутрішню цілісність елементів даних. Перефразовуючи це:

– C1 – коли виконується IVP, він повинен забезпечити дійсність CDI.

– C2 – для певного пов’язаного набору CDI TP має перетворити ці CDI з одного дійсного стану в інший.

Оскільки ми повинні переконатися, що ці TP сертифіковані для роботи на конкретному CDI, ми повинні мати E1 і E2.

– E1 – система повинна підтримувати список сертифікованих зв’язків і гарантувати, що тільки TP, сертифіковані для роботи на CDI, змінюють цей CDI.

– E2 – система повинна пов’язати користувача з кожним TP і набором CDI. TP може отримати доступ до CDI від імені користувача, якщо це "легально".

– E3-Система повинна ідентифікувати особу кожного користувача, який намагається виконати TP.

Це вимагає відстеження трійок (користувач, TP, {CDI}), які називаються «дозволеними зв’язками».

– C3 – Дозволені стосунки мають відповідати вимогам «розподілу обов’язків».

Нам потрібна автентифікація, щоб відстежувати це.

– C4 – усі TP повинні додати до журналу достатньо інформації для реконструкції операції.

Коли інформація надходить у систему, їй не потрібно довіряти чи обмежуватись (тобто вона може бути UDI). Ми повинні відповідним чином поставитися до цього.

– C5 – будь-який TP, який приймає UDI як вхідні дані, може виконувати лише дійсні транзакції для всіх можливих значень UDI. TP або прийме (перетворить на CDI), або відхилить UDI.

Нарешті, щоб запобігти людям отримати доступ через зміну кваліфікації TP:

– E4. Лише сертифікатор TP може змінити список об’єктів, пов’язаних із цим TP.

CW-lite

Варіантом Кларка-Вілсона є модель CW-lite, яка послаблює початкову вимогу формальної перевірки семантики TP. Семантичну перевірку відкладено до окремої моделі та загальних формальних інструментів доказу.

11.3. Резервування інформації та компонентів інформаційно-телекомунікаційних системах

Згідно закону України «Про захист інформації в інформаційно-комунікаційних системах» власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:

– **створюють резервні копії** державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх **захисту, цілісності та конфіденційності**;

– **забезпечують створення резервних копій** державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), **протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування**.

Також згідно цього закону вводяться наступні поняття:

– **Резервна копія державних інформаційних ресурсів** – копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

– **Резервування державних інформаційних ресурсів та систем** – сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах, а також інсталяційних копій програмного забезпечення та операційних систем (та/або їх образів), в яких здійснюється їх обробка. Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання, визначається Кабінетом Міністрів України.

На цей час окрім організаційних заходів із планування відновлювальних робіт задля забезпечення неперервності функціонування своїх ІКС організації можуть застосовувати низку рішень із арсеналу аварійностійких (катастрофостійких) технологій. За своєю суттю ці технології передбачають *резервування ресурсів інформаційної системи* та *резервне зберігання даних*.

Можна виділити кілька рівнів резервування ресурсів інформаційної системи залежно від її значимості для діяльності організації, а також від чутливості діяльності до часу простою ІКС:

– Прикладом найнижчого рівня резервування для ІКС другорядного значення може бути просто серверна площадка, обладнана необхідними інженерними системами й підготовлена для установки серверного устаткування. Такий підхід дозволяє відновити роботу системи протягом декількох днів.

– Для більш важливих інформаційних систем відокремлений обчислювальний центр повинен містити все необхідне устаткування, щоб у випадку катастрофи можна було швидко запустити резервну систему (холодне резервування).

– А для найбільш критичних систем додатково необхідні системи реплікації даних і плани аварійного відновлення, що забезпечують збереження даних і безперервність функціонування ІКС (гаряче резервування).

Іншою складовою аварійностійких технологій, що стосується інформаційних ресурсів є резервування даних. У надзвичайних ситуаціях найбільший збиток організації наносять не тимчасова неможливість доступу до критичних даних, а цілковита їх втрата. Мінімізація цього ризику досягається за рахунок резервного копіювання й реплікації даних. На рис. 7.1 наведено класифікацію методів резервування даних.

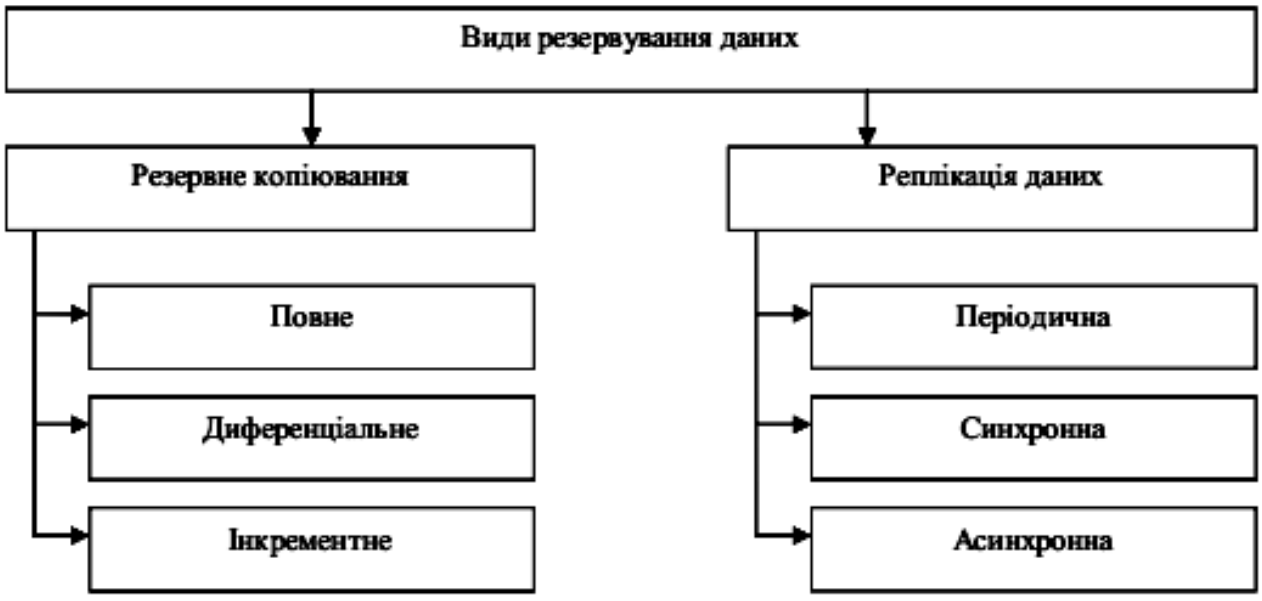

Рисунок 11.1 – Рівні резервування інформаційних систем

Резервне копіювання (*англ. backup*) – процес створення копії даних на спеціальних носіях (стримерах, матрицях дисків і т. д.), призначений для відновлення даних в основному місці їх розташування в разі їх пошкодження або руйнування. Резервне копіювання необхідне для швидкого і недорогого відновлення інформації (документів, програм) у випадку втрати робочої копії інформації з будь-якої причини. Важливо зберігати носії з резервними копіями окремо від оригінальних даних.

Повне резервування (*full backup*) зазвичай зачіпає всю операційну систему і всі дані. Створення щотижневих, щомісячних і щоквартальних архівів передбачає повне резервування. Перше щотижневе архівування повинно бути повним резервуванням, що зазвичай виконується по п'ятницях або упродовж вихідних, і передбачає копіювання всіх бажаних файлів. Подальші резервування, які проводять з понеділка по четвер аж до наступного повного резервування, можуть бути інкрементними або диференціальними, щоб заощадити час і місце на носії. Повне резервування слід проводити, принаймні, щотижня.

Диференціальне або *різницеве резервування* (*differential backup*) передбачає копіювання кожного файлу, зміненого з моменту останнього повного резервування. Диференціальне резервування прискорює процес відновлення і для відновлення вимагає лише останню повну і останню диференціальну резервні копії. Популярність диференціального резервування зростає, оскільки всі копії файлів виконуються в певні моменти часу, що, наприклад, дуже важливо при зараженні ІКС вірусами.

Інкрементне або *додаткове резервування* (*incremental backup*) передбачає копіювання тільки тих файлів, які були змінені з часу останнього повного або додаткового резервного копіювання. Подальше додаткове резервування додає тільки файли, які були змінені з моменту попереднього додаткового резервування. Таке резервування займає менше часу, оскільки копіюється менша кількість файлів. Однак, процес відновлення даних займає більше часу, тому що повинні бути відновлені дані останнього повного резервування, плюс дані всіх наступних додаткових резервувань. При цьому, на відміну від диференціального резервування нові або змінені файли не заміщають старі, а додаються на носій незалежно.

Реплікація даних – це віддалене резервне копіювання, що на відміну від звичайного резервного копіювання передбачає виділення таких додаткових ресурсів, як віддалені системи архівування, що з’єднані із ІКС організації каналами зв'язку. Розмаїтість схем і варіантів реплікації даних забезпечує можливість вибору найбільш ефективного й раціонального рішення для кожного конкретного завдання.

Періодична реплікація або *реплікація за розкладом* допомагає зберегти у відокремленому центрі копію даних на фіксований момент часу в минулому. Основний недолік цього методу – втрата актуальності даних за період часу, що дорівнює інтервалу між реплікаціями. Проте, реплікація за розкладом є доволі ощадливим рішенням для організацій, коли час відновлення не є критично важливим, а також допускається незначна втрата даних.

Синхронна реплікація гарантує найвищий рівень надійності, забезпечуючи ідентичність всіх копій даних. Висуваючи високі вимоги до каналів зв'язку, синхронна реплікація найчастіше застосовується для найбільш важливих застосувань, де необхідний максимальний захист даних.

Асинхронна реплікація забезпечує безперервність передачі даних, причому навіть в умовах нестабільності каналів зв’язку. Цей спосіб допомагає зберегти високу продуктивність інформаційних систем і контролювати завантаження каналів передачі даних, але не забезпечує настільки ж високий рівень актуальності даних, як синхронна реплікація.

Останнім часом часто застосовуються схеми множинної реплікації, коли дані передаються з основного обчислювального центра відразу до кількох резервних центрів. Нерідко в цих випадках навіть застосовуються різні способи реплікації для більш надійного й комплексного захисту даних.

Реплікація даних має деякі переваги порівняно з традиційними методами резервного копіювання:

– віддалене копіювання не вимагає участі користувачів та забезпечує необмежене в часі зберігання даних;

– деякі віддалені резервні служби можуть працювати безперервно, копіюючи зміни у файлах. Проте реплікація має й кілька істотних недоліків:

– відновлення даних може бути повільним, за обмеженої смуги пропускання каналів зв’язку;

– постачальники послуг віддаленого резервного копіювання можуть не надавати гарантій конфіденційності, тому організації-клієнти повинні самостійно шифрувати дані для віддаленого зберігання, при цьому, якщо ключ шифрування буде втрачено, то відновлення даних стане неможливим;

– деякі постачальники послуг реплікації часто мають щомісячні ліміти, які внаслідок чого обсяги резервного копіювання для організацій можуть обмежуватися.

Надійне збереження дуже важливих даних у випадку виникнення надзвичайної ситуації забезпечується за допомогою розподілених мереж зберігання даних (англ. Storage Area Network – SAN), для роботи яких необхідні надійні й високопродуктивні канали передачі даних. Технологія SAN забезпечує відмовостійкий доступ серверів до ресурсів зберігання і дозволяє знизити сукупну вартість утримання IT-інфраструктури за рахунок оптимального онлайнового управління доступу серверів до ресурсів зберігання. Розподілені мережі зберігання даних складаються з серверів резервного копіювання, системи управління та комунікаційної інфраструктури, що забезпечує фізичний зв'язок між елементами мережі зберігання даних. Подібна архітектура дозволяє забезпечити безперебійне і безпечне зберігання даних, а також обмін даними між елементами мережі зберігання даних. В основі концепції SAN лежить можливість з'єднання будь-якого з серверів з будь-яким пристроєм зберігання даних, що працює за протоколом Fibre Channel. Зручні засоби адміністрування SAN дають можливість скоротити чисельність обслуговуючого персоналу, що знижує вартість зберігання даних.

Об'єднання SAN за допомогою IP-мереж має меншу продуктивність, але за рахунок широкої поширеності й низької вартості IP-каналів цей варіант є більш доступним. Мережі зберігання даних із застосуванням технологій DWDM (системи з хвильовим ущільненням каналів) забезпечують передачу даних на великі відстані з високою швидкістю. У рішеннях цього класу використовуються волоконно-оптичні лінії зв’язку, в тому числі існуючі мережі глобальних операторів зв’язку. Висока швидкість передачі даних по SAN (200 Мбайт/с) дозволяє в реальному часі переміщати дані, що змінюються, у віддалене сховище.