Тема 3. Управління доступом до інформації

3.1. Поняття доступу до інформаційних ресурсів та його рівні

Повернутися до початку

Сучасний розвиток інформаційних технологій і комунікацій призвів до формування нового глобального середовища, в якому інформація стала одним із найцінніших ресурсів. Питання доступу до інформаційних ресурсів стало центральним у правовій, соціальній та економічній сферах життя. Це особливо актуально для країн, що знаходяться на різних етапах розвитку демократії та інформаційного суспільства. Доступ до інформації розглядається не лише як засіб для отримання знань, але й як фундаментальне право, що підтримує інші права людини, включаючи свободу вираження думок та доступ до правосуддя. У рамках цієї лекції буде розглянуто поняття доступу до інформаційних ресурсів та його рівні, а також аналіз нормативно-правових аспектів та приклади міжнародного досвіду.

Поняття доступу до інформаційних ресурсів

Доступ до інформаційних ресурсів можна визначити як можливість отримання, використання, поширення та управління інформацією, що необхідна для задоволення

соціальних, економічних і правових потреб. Інформаційні ресурси охоплюють широкий спектр даних і матеріалів, що можуть бути представлені в різних формах, включаючи цифрові, друковані та аудіовізуальні носії. З точки зору правових основ, доступ до інформації закріплений у міжнародних документах, таких як Загальна декларація прав людини (стаття 19) та Міжнародний пакт про громадянські і політичні права (стаття 19).

Національні законодавства різних країн також визнають право на доступ до інформації як важливий аспект демократичного управління. Зокрема, в Україні це право закріплено в Конституції (стаття 34), де зазначено, що кожен має право вільно збирати, зберігати, використовувати та поширювати інформацію усно, письмово або в інший спосіб.

Рівні доступу до інформаційних ресурсів

Доступ до інформаційних ресурсів можна розділити на декілька рівнів, залежно від ступеня відкритості та доступності інформації. Ці рівні можуть змінюватися залежно від політичного режиму, економічних умов та стану технологічного розвитку.

1. Вільний доступ

Вільний доступ передбачає відкритість інформації для всіх без винятку. Це стосується публічних документів, звітів державних органів, наукових досліджень та інших матеріалів, які мають важливе суспільне значення. Вільний доступ забезпечує прозорість діяльності державних органів, сприяє розвитку громадянського суспільства та зменшує рівень корупції. Однак для забезпечення такого доступу необхідні законодавчі механізми, що гарантують ефективне виконання цього права.

Прикладом є практика Скандинавських країн, де закони про свободу інформації є одними з найпрогресивніших у світі. Наприклад, у Швеції законодавство, що

регулює доступ до публічних документів, було прийняте ще у XVIII столітті.

В Україні публічна інформація у формі відкритих даних — це такі відомості у форматі, що дозволяє їх автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також їх подальше використання (ст.10^1 Закону України "Про доступ до публічної інформації").

Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних та на своїх веб-сайтах.

Публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення. Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації.

2. Обмежений доступ

Обмежений доступ має місце тоді, коли інформація може бути доступна тільки певним категоріям осіб або в окремих випадках. Це можуть бути документи, що містять персональні дані, комерційні таємниці, державні секрети чи інші види інформації, що підлягають спеціальному захисту. Обмеження доступу виправдані для забезпечення національної безпеки, захисту особистих прав і свобод громадян, а також збереження комерційних інтересів компаній.

Законодавство України визначає межі доступу до інформації через закони, такі як "Про доступ до публічної інформації" та "Про захист персональних даних". Наприклад, стаття 7 закону "Про доступ до публічної інформації" встановлює перелік випадків, коли доступ до інформації може бути обмежений.

Конфіденційна інформація — інформація, доступ до якої обмежено фізичною

або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Розпорядники, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди — лише в інтересах національної безпеки, економічного добробуту та прав людини.

3. Спеціалізований доступ

Спеціалізований доступ передбачає надання інформації лише тим особам, які мають відповідні повноваження або професійний інтерес. Це може стосуватися експертів, журналістів, науковців або представників державних органів. Спеціалізований доступ сприяє глибшому розумінню певних питань, що мають суспільне значення, але потребують професійного аналізу.

Важливим аспектом є надання доступу до наукових і дослідницьких даних для розвитку технологій та підтримки інновацій. У багатьох країнах реалізуються ініціативи з відкритого доступу до наукових публікацій, які сприяють покращенню рівня освіти та науки. Наприклад, Європейський Союз активно підтримує програму Open Access, що забезпечує доступ до результатів наукових досліджень, фінансованих за рахунок державних коштів.

Прикладом інформації зі спеціалізованим доступом може бути таємна або службова інформація (відповідно ст.8 та ст.9 Закону України "Про доступ до публічної інформації").

Таємна інформація — інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Службова інформація — це та, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; або зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Нормативно-правові аспекти доступу до інформаційних ресурсів

Доступ до інформаційних ресурсів регулюється як міжнародними, так і національними правовими актами. Найбільш значущими є Загальна декларація прав людини та Міжнародний пакт про громадянські і політичні права. Ці документи проголошують право на свободу вираження думок та доступ до інформації.

В Україні законодавчі основи доступу до інформації закладені в Конституції та спеціалізованих законах. Закон України "Про інформацію" визначає загальні принципи регулювання інформаційних відносин. Інші нормативні акти, як-от закон "Про доступ до публічної інформації", уточнюють механізми реалізації цього права та встановлюють правила роботи з інформацією.

Виклики та перспективи розвитку

Незважаючи на наявність законодавчих механізмів, забезпечення ефективного доступу до інформаційних ресурсів стикається з рядом викликів. Однією з головних проблем є технічні обмеження, такі як недостатня інфраструктура для зберігання та обробки великих обсягів даних. Іншим важливим аспектом є питання безпеки та захисту конфіденційної інформації, яке потребує дотримання суворих правил і протоколів.

Крім того, важливим є питання цифрового розриву, коли різні верстви

населення мають неоднаковий доступ до сучасних інформаційних технологій. Для вирішення цієї проблеми необхідні як урядові ініціативи, так і підтримка приватного сектора та міжнародних організацій. Програми підвищення цифрової грамотності, доступу до інтернету в сільських та віддалених районах є важливими для забезпечення рівноправного доступу до інформаційних ресурсів.

Поняття доступу до інформаційних ресурсів є складним і багатогранним. Воно включає в себе як правові, так і технічні аспекти, що впливають на його реалізацію. Різні рівні доступу — вільний, обмежений та спеціалізований — відображають потребу в балансі між відкритістю та захистом інформації. Ефективна реалізація права на доступ до інформації потребує чіткого законодавчого регулювання, розвитку інфраструктури та забезпечення інформаційної безпеки.

На шляху до побудови інформаційного суспільства важливо враховувати не лише технічні та правові питання, але й соціальні фактори, що сприяють рівному доступу до інформаційних ресурсів для всіх громадян. Лише комплексний підхід дозволить забезпечити стале і демократичне управління інформаційними потоками, що, у свою чергу, сприятиме розвитку суспільства.

3.2. Системи управління доступом (СУД)

Повернутися до початку

У сучасному цифровому світі обсяг та складність інформації, що використовується та обробляється, зростають з кожним роком. Це призводить до необхідності забезпечення її захисту від несанкціонованого доступу, модифікації чи знищення. Системи управління доступом дозволяють регулювати права доступу до даних та забезпечують їх безпеку, захищаючи від можливих загроз.

Поняття системи управління доступом

Система управління доступом (СУД) визначається як набір технологій та процедур, що забезпечують контроль за доступом користувачів до інформаційних ресурсів. Вона складається з таких основних елементів:

1. **Аутентифікація** — процес перевірки особи користувача, що надає можливість системі переконатися в його правомірності.
2. **Авторизація** — визначення прав доступу, тобто, які ресурси можуть бути використані користувачем та у якому обсязі.
3. **Моніторинг та аудит** — відстеження активності користувачів для виявлення підозрілих дій та недопущення порушень.
4. **Адміністрування** — управління ролями, правами доступу та обліковими записами.

Різноманітні системи управління доступом можна класифікувати за типами доступу та методами управління:

1. **Дискреційні системи управління доступом (DAC — Discretionary access control systems)** У дискреційних системах доступ до ресурсів визначається власником ресурсу. Користувачі можуть самостійно надавати іншим користувачам права на використання ресурсів. DAC-системи є гнучкими, але мають обмеження з точки зору безпеки, оскільки користувачі можуть випадково або навмисно надати доступ невідповідним особам.
2. **Мандатні системи управління доступом (MAC — Mandatory access control systems)** У мандатних системах управління доступом права доступу встановлюються централізовано та базуються на політиках безпеки. Користувачі не мають можливості змінювати рівні доступу. MAC-системи зазвичай застосовуються у середовищах, де безпека є критично важливою, таких як військові та урядові установи.

3. **Рольові системи управління доступом (RBAC — Role-based access control systems)** У ролевих системах права доступу визначаються на основі ролей, які виконують користувачі. Кожна роль має певні права доступу, і користувачам надаються ці права залежно від їх ролі. RBAC-системи дозволяють спрощувати управління доступом у великих організаціях, де кожна роль чітко визначена.
4. **Атрибутивні системи управління доступом (ABAC — Attribute-based access control systems)** Атрибутивні системи надають доступ на основі набору атрибутів (наприклад, роль, місцезнаходження, час доби). Це дозволяє більш детально контролювати доступ та враховувати різні обставини при прийнятті рішення.

Архітектура систем управління доступом. Системи управління доступом складаються з кількох основних компонентів:

1. *Інтерфейс користувача* — забезпечує зручний доступ до системи для адміністраторів та користувачів.
2. *Модуль аутентифікації* — відповідає за підтвердження особи користувача.
3. *Модуль авторизації* — визначає рівень доступу та дозволи.
4. *База даних користувачів та прав доступу* — містить інформацію про облікові записи, ролі та їхні права.
5. *Модуль моніторингу та аудиту* — забезпечує запис дій користувачів та аналіз подій для виявлення потенційних загроз.

Моделі контролю доступу. Існують різні моделі контролю доступу, які застосовуються залежно від специфіки організації:

1. **Bell-LaPadula Model** — використовується для захисту конфіденційності даних і базується на принципах “нечитання зверху” та “незаписування вниз”.
2. **Biba Model** — зосереджена на забезпеченні цілісності даних і базується на

протилежних принципах: “нечитання знизу” та “незаписування вгору”.

3. **Clark-Wilson Model** — акцентує увагу на підтриманні внутрішнього контролю через встановлення обмежень для транзакцій.
4. **Модель мандатного управління доступом** — базується на розмежуванні доступу згідно з рівнями секретності та потребує жорсткого дотримання політики безпеки.

Модель Bell-LaPadula (BLP) — це формальна модель безпеки, що застосовується для контролю доступу до інформаційних ресурсів, зокрема в середовищах з високими вимогами до захисту інформації, таких як урядові та військові системи. Вона була розроблена в 1973 році, і її основною метою є забезпечення конфіденційності даних.

Модель була розроблена на основі двох основних принципів: *“не читай вище” (no read up, “NRU”)* і *“не записуй нижче” (no write down, “NWD”)*. Ці принципи дозволяють обмежити доступ до інформації таким чином, щоб мінімізувати ймовірність витоку конфіденційних даних.

Основні компоненти та принципи моделі Bell-LaPadula:

1. *Рівні безпеки (Security Levels):* У моделі Bell-LaPadula всі ресурси і користувачі мають рівні безпеки. Наприклад, це можуть бути рівні “Top Secret” (Топ-секретно), “Secret” (Секретно), “Confidential” (Конфіденційно) і “Unclassified” (Не класифіковано). Користувачі мають доступ до інформації лише на основі своїх рівнів безпеки.
2. *Маркери (Labels):* Кожен об’єкт (файл, документ) в системі має маркер або мітку, що вказує на його рівень безпеки. Користувачі мають мітки доступу, які визначають, до яких рівнів безпеки вони мають доступ.

Модель Bell-LaPadula описує два ключових правила:

1. *Правило "не читай вище" (no read up, NRU):* Користувач може читати лише ті дані, рівень безпеки яких є рівним або нижчим за рівень доступу користувача. Це запобігає тому, щоб користувач із нижчим рівнем безпеки випадково або навмисно отримав доступ до більш конфіденційної інформації.

Приклад: Користувач з рівнем безпеки "Confidential" не зможе прочитати документи, які мають маркер "Top Secret", навіть якщо ці документи доступні для читання іншими користувачами.

2. *Правило "не записуй нижче" (no write down, NWD):* Користувач може записувати (модифікувати) інформацію лише в об'єкти з рівнем безпеки, який є рівним або вищим за його рівень доступу. Це правило запобігає можливості випадкового або навмисного запису конфіденційної інформації в менш захищену частину системи, що може призвести до її витоку.

Приклад: Користувач з рівнем "Top Secret" не може записувати дані в документ, який позначений як "Confidential", оскільки це може призвести до витоку конфіденційної інформації.

Важливі характеристики моделі Bell-LaPadula:

1. *Фокус на конфіденційності:* Модель Bell-LaPadula орієнтована на забезпечення конфіденційності даних. Вона контролює доступ до інформації на основі рівнів безпеки, але не надає механізмів для забезпечення інших аспектів безпеки, таких як цілісність або доступність даних.
2. *Обмеження для зниження ризику витоку інформації:* Правила «не читай вище» і «не записуй нижче» допомагають зменшити ймовірність витоку конфіденційних даних, оскільки користувачі не можуть отримати доступ до більш високих рівнів безпеки та не можуть записувати на більш низькі рівні.
3. *Не підтримує принципи "не читай нижче" або "не записуй вище":* Важливо зазначити, що модель Bell-LaPadula не підтримує принцип "не читай нижче" або

“не записуй вище”, що означає, що користувач може читати або записувати дані на рівнях, що є нижчими за його рівень безпеки.

Приклад використання моделі Bell-LaPadula:

У військових або урядових інформаційних системах модель Bell-LaPadula може бути використана для контролю доступу до документів на різних рівнях безпеки. Наприклад:

- Користувач з рівнем доступу “Top Secret” може читати і писати документи, позначені як “Top Secret», “Secret”, “Confidential”, але не може отримати доступ до документів, позначених як “Unclassified”.
- Користувач з рівнем “Confidential” може читати лише документи рівня “Confidential” або “Unclassified” і не може записувати їх у документ з рівнем “Top Secret”.

Обмеження моделі Bell-LaPadula:

- *Цілісність даних:* Модель Bell-LaPadula не враховує цілісність даних. Вона фокусується лише на контролі доступу для забезпечення конфіденційності.
- *Доступність:* Вона також не орієнтована на забезпечення доступності даних. Модель не має механізмів для захисту від відмови в обслуговуванні або порушення доступу.
- *Гнучкість:* Модель може бути занадто обмеженою для деяких випадків, оскільки не дозволяє гнучко надавати доступ до інформації для користувачів, які мають неповний доступ до деяких ресурсів.

Отже, розглянута модель Bell-LaPadula є важливою теоретичною основою для контролю доступу в інформаційних системах, орієнтованих на *конфіденційність*. Вона застосовується в середовищах, де забезпечення конфіденційності є критично важливим, таких як військові, урядові чи спеціалізовані комерційні системи. Однак,

через свою орієнтацію тільки на конфіденційність, вона не є універсальним рішенням для всіх типів систем безпеки.

Модель Biba — це одна з формальних моделей безпеки, що була розроблена для забезпечення *цілісності даних* в інформаційних системах. Вона була запропонована Кеном Біба в 1977 році як противага до моделі Bell-LaPadula, яка фокусується на конфіденційності. Основна *мета моделі Biba* — це захист від несанкціонованих змін даних, забезпечення їх цілісності і запобігання спробам модифікації даних без належного дозволу.

Основні принципи моделі Biba:

Модель Biba використовує принципи, які дозволяють уникати несанкціонованих змін даних, зокрема це два ключових правила:

1. *Правило "не читай нижче" (No Read Down, "NRD"):* Користувач може читати лише ті дані, які мають рівень цілісності, рівний або вищий за рівень доступу користувача. Це правило забезпечує захист від зчитування даних низької цілісності, що може призвести до отримання або використання неправильних або ненадійних даних.

Приклад: Користувач з рівнем цілісності "Medium" може читати дані, які мають рівень "High" або "Medium", але не може читати дані з рівнем "Low", оскільки ці дані можуть бути неякісними або зміненими несанкціоновано.

2. *Правило "не записуй вище" (No Write Up, "NWU"):* Користувач може записувати (змінювати) дані лише в об'єкти, рівень цілісності яких є рівним або нижчим за його рівень. Це правило запобігає можливості того, щоб менш надійні (нижчі) дані були записані в більш захищені (вищі) об'єкти, що могло б призвести до компрометації цілісності даних.

Приклад: Користувач з рівнем цілісності "Medium" не може записувати дані в об'єкти

з рівнем “High”, оскільки зміна даних особою з нижчим рівнем доступу може вплинути на більш надійні і важливі для системи дані.

Ключові концепції моделі Biba:

1. *Цілісність даних:* Модель Biba націлена на забезпечення *цілісності* інформації в інформаційних системах. Це означає, що система повинна забезпечити, щоб дані не були змінені неправомірно або несанкціоновано. Цілісність має важливе значення для забезпечення точності, надійності та коректності даних.
2. *Рівні цілісності:* Подібно до моделі Bell-LaPadula, в моделі Biba дані та користувачі мають рівні цілісності. Дані позначаються мітками, які вказують на рівень їх надійності чи точності. Користувачі мають рівні доступу, які визначають, які дані вони можуть змінювати або зчитувати.

Приклад використання моделі Biba:

Розглянемо приклад для вищої навчальної установи, яка зберігає важливі дослідницькі дані. У цій системі є різні рівні цілісності даних:

High — Дані, які знаходяться на фінальному етапі дослідження і були перевірені;

Medium — Чернетки досліджень, що можуть містити деякі незавершені елементи;

Low — Початкові дослідження або необроблені дані.

За допомогою моделі Biba:

- Користувачі з рівнем доступу *Medium* не можуть змінювати дані на рівні *High,* оскільки їхні дослідження можуть бути не точними, і це може пошкодити результати більш надійних досліджень.
- Користувачі з рівнем *High* не можуть зчитувати дані з рівня *Low*, щоб не використовувати ненадійні або неперевірені дані, що можуть призвести до помилок.

Обмеження моделі Biba:

- *Цілісність без конфіденційності:* Модель Biba не забезпечує конфіденційність даних, і її можна застосовувати тільки в тих середовищах, де цілісність є пріоритетом, а не конфіденційність.
- *Складність реалізації:* Модель Biba може бути складною в реалізації для великих та складних систем, де потрібно дотримуватися суворих вимог щодо зміни рівнів цілісності та доступу до даних.

Таким чином, модель Biba є важливою для організацій, які фокусуються на забезпеченні *цілісності* даних. Вона дозволяє запобігти несанкціонованим змінам та помилковому доступу до важливих даних, підтримуючи їх точність та надійність. Хоча вона не вирішує проблеми конфіденційності, вона є важливою складовою частиною систем безпеки, де цілісність даних є критично важливою.

Різниця між моделями Bell-LaPadula та Biba:

- ✓ **Модель Bell-LaPadula** зосереджена на забезпеченні **конфіденційності**, тоді як модель Biba націлена на **цілісність** даних. У той час як Bell-LaPadula запобігає витоку конфіденційної інформації, Biba фокусується на забезпеченні правильності даних і запобігає їх модифікації.
- ✓ **Bell-LaPadula** використовує принципи **“не читай вище” (no read up)** і **“не записуй нижче” (no write down)**, що гарантує, що менш захищена інформація не потрапить до більш захищених рівнів. Натомість **Biba** використовує принципи **“не читай нижче” (no read down)** і **“не записуй вище” (no write up)**, що забезпечує, що дані низької цілісності не будуть доступні для зчитування або модифікації на більш високих рівнях.

Системи управління доступом є важливою складовою безпеки інформаційних ресурсів. Правильна реалізація СУД дозволяє забезпечити захист даних, знижуючи ризики несанкціонованого доступу та порушення конфіденційності. Різні методи та моделі управління доступом забезпечують різні рівні захисту та відповідають специфічним потребам організацій. Однак, ефективність таких систем залежить від їх інтеграції з іншими елементами кібербезпеки та постійного вдосконалення політик управління доступом.

3.3. Аутентифікація, авторизація та облік в СУД

Повернутися до початку

Сучасний світ цифрових технологій значно ускладнив процеси доступу до інформації та забезпечення її захисту. З розвитком мережевих технологій, Інтернету та численних веб-додатків питання безпеки даних набули критичної важливості. У цьому контексті важливими поняттями є аутентифікація, авторизація та облік (AAA), які разом утворюють основу сучасних систем управління доступом до ресурсів.

Аутентифікація, авторизація та облік (англ. authentication, authorization, and accounting — AAA) є базовими механізмами контролю доступу до інформаційних ресурсів і систем. Ці процеси використовуються для ідентифікації користувачів, перевірки їх прав доступу та ведення журналу дій користувачів у системі. Далі розглянемо кожне з цих понять детальніше, а також їх важливість у забезпеченні інформаційної безпеки.

Аутентифікація: основні принципи

Аутентифікація є процесом встановлення особистості користувача. Це перший крок у будь-якому процесі управління доступом, який допомагає переконатися, що

особа, яка намагається отримати доступ до системи або ресурсу, є тим, за кого себе видає. У більшості випадків аутентифікація передбачає використання облікових даних, таких як ім’я користувача та пароль.

Типи аутентифікації:

1. **Що знає користувач (паролі та PIN-коди)** Це найбільш поширений метод аутентифікації. Паролі повинні бути складними та регулярно змінюватися для забезпечення безпеки.
2. **Що має користувач (смарт-картки, токени)** Фізичні пристрої, такі як смарт-картки або апаратні токени, використовуються для підтвердження особистості користувача.
3. **Хто є користувач (біометрія)** Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя або сканування райдужки ока, забезпечує високий рівень безпеки.
4. З розвитком технологій з’явилися нові способи аутентифікації, такі як одноразові паролі (OTP), аутентифікація за допомогою мобільних додатків (наприклад, Google Authenticator або Duo), а також аутентифікація через соціальні мережі або сторонні сервіси (OAuth).

Аутентифікація — це процес перевірки справжності або підтвердження особи користувача, пристрою чи іншого об’єкта, що взаємодіє з інформаційною системою. У контексті інформаційних технологій це механізм, який забезпечує доступ до систем, сервісів або даних тільки тим суб’єктам, які мають відповідні права доступу. Аутентифікація допомагає захистити конфіденційну інформацію від несанкціонованого доступу.

Процес аутентифікації зазвичай складається з таких основних етапів:

1. Пред’явлення ідентифікатора (наприклад, ім’я користувача або ID).
2. Представлення доказів справжності (наприклад, пароля або іншого способу перевірки).
3. Перевірка системою наданих даних.
4. Надання доступу або відмова в разі успішної чи невдалої аутентифікації.

Аутентифікація може здійснюватися різними способами, залежно від рівня захисту, що потрібен:

1. *Однофакторна аутентифікація (1FA):* використовується лише один фактор для перевірки. Це найпростіший вид аутентифікації, наприклад, введення пароля при вході в систему. Її недолік полягає в тому, що у разі коли пароль зламаний або вкрадений, система стає вразливою.
2. *Двофакторна аутентифікація (2FA):* використовується два різні фактори для перевірки справжності, що підвищує безпеку, наприклад, введення пароля та додаткова перевірка через SMS-код або мобільний додаток. Перевагою цього виду є те, що його складніше обійти, навіть якщо один з факторів скомпрометований.
3. *Багатофакторна аутентифікація (MFA):* залучає два або більше незалежних факторів перевірки для досягнення найвищого рівня безпеки, наприклад, вхід за допомогою пароля, відбитка пальця та додаткового коду з мобільного пристрою. Перевагою є максимальна захищеність інформаційного ресурсу.

<u>Приклади використання аутентифікації:</u>

- Інтернет-банкінг: використовує 2FA або MFA для перевірки особи клієнта при вході в акаунт. Наприклад, введення пароля та додаткова аутентифікація через SMS.

- ❖ Корпоративні мережі: для доступу до внутрішніх систем компанії співробітники можуть використовувати комбінацію пароля та відбитка пальця.
- ❖ Соціальні мережі: застосовують двофакторну аутентифікацію для підвищення безпеки облікових записів користувачів.

Аутентифікація є ключовим елементом захисту інформаційних систем. Використання більш складних методів аутентифікації, таких як 2FA або MFA, значно підвищує безпеку, зменшуючи ризик несанкціонованого доступу. Організації повинні ретельно підбирати методи аутентифікації, виходячи з рівня захисту, вимог безпеки та зручності для користувачів. Найкращим варіантом, який здатен підвищити рівень безпеки до максимального рівня буде поєднання декількох методів аутентифікації:

1. *Паролі* — один з найпоширеніших методів, який базується на знанні користувачем певної інформації.
2. *Біометричні дані* — використовують фізичні або поведінкові характеристики, такі як відбитки пальців, розпізнавання обличчя або голосу.
3. *Смарт-карти та токени* — фізичні пристрої, що забезпечують додатковий рівень безпеки.
4. *Двофакторна аутентифікація (2FA)* — комбінує два різних методи для підвищення надійності.
5. *Одноразові паролі (OTP)* — забезпечують додатковий захист, оскільки використовуються лише один раз і мають обмежений термін дії.

Авторизація — це процес надання або обмеження доступу користувача до певних ресурсів або функцій після його успішної аутентифікації. Після того як система перевірила особу користувача (аутентифікація), наступним кроком є визначення його прав доступу до певних даних або дій. Авторизація відповідає на питання: *“Що дозволено робити користувачеві?”*.

Аутентифікація та авторизація тісно пов’язані, але вони не є синонімами:

- Аутентифікація: Перевіряє, чи є користувач тим, за кого себе видає (ідентифікація особи).
- Авторизація: Визначає, які права та рівні доступу має цей користувач у системі після аутентифікації.

Наприклад, після успішного входу в корпоративну систему (аутентифікація), користувач може мати доступ лише до певних файлів або функцій залежно від своєї ролі (авторизація).

Як працює авторизація?

1. Аутентифікація користувача: Спершу користувач підтверджує свою особу, використовуючи обраний метод аутентифікації (пароль, біометрія тощо).
2. Перевірка прав доступу: Система перевіряє, до яких саме ресурсів або функцій має доступ аутентифікований користувач.
3. Доступ до ресурсів: В залежності від визначених прав, користувачеві надається або обмежується доступ до різних компонентів системи.

Основні моделі авторизації:

1. Модель контролю доступу на основі ролей (Role-Based Access Control, RBAC):
   - Характеристика: Авторизація базується на ролях користувачів у системі. Користувачам призначаються певні ролі (наприклад, “адміністратор”, “редактор”, “читач”), і кожна роль має чітко визначені права доступу.
   - Приклад: У корпоративному середовищі адміністратори мають доступ до налаштувань системи, тоді як звичайні співробітники можуть лише переглядати певні дані.
2. Дискреційний контроль доступу (Discretionary Access Control, DAC):
   - Характеристика: Власник ресурсу може самостійно визначати права доступу до нього для інших користувачів.
   - Приклад: Користувач, який створює документ у текстовому редакторі, може

надати доступ іншим співробітникам на перегляд чи редагування.

3. Обов’язковий контроль доступу (Mandatory Access Control, MAC):
   - Характеристика: Використовується для систем з високими вимогами безпеки. Доступ до об’єктів визначається політиками безпеки, а не власником ресурсу.
   - Приклад: В урядових або військових системах використовується така модель, де доступ до документів залежить від рівня секретності користувача.
4. Атрибутний контроль доступу (Attribute-Based Access Control, ABAC):
   - Характеристика: Доступ визначається на основі множини атрибутів, що можуть включати інформацію про користувача, його місцезнаходження, час доби тощо.
   - Приклад: Система може надавати доступ до певних функцій лише користувачам, які працюють у певному офісі під час робочих годин.

Приклади авторизації:

- *Онлайн-банкінг:* після входу в систему користувач може переглядати залишок на рахунку, здійснювати платежі, але не має доступу до адміністративних функцій банківської системи.
- *Соціальні мережі:* авторизація дозволяє користувачам переглядати свої власні профілі та профілі друзів, публікувати дописи або коментарі, але обмежує доступ до панелі адміністратора, яка доступна лише модераторам.
- *Корпоративні системи:* співробітник може мати доступ до своєї електронної пошти та певних внутрішніх документів, але доступ до конфіденційних даних компанії матимуть лише працівники з відповідними правами.

Основні характеристики авторизації:

- Гнучкість: Система повинна дозволяти легко змінювати права доступу в

залежності від ролей та необхідності.

- ❖ Масштабованість: Можливість застосовувати авторизацію для великої кількості користувачів та різних рівнів доступу.
- ❖ Безпека: Ефективна авторизація забезпечує надійний захист ресурсів системи від несанкціонованого доступу.
- ❖ Прозорість: Система повинна бути зрозумілою користувачам, аби вони могли знати свої права та обов'язки.

Отже, авторизація є критичним компонентом захисту даних та інформаційних систем. Вона гарантує, що навіть після аутентифікації користувач отримує доступ лише до тих ресурсів, на які він має право. Застосування ефективних методів авторизації допомагає зберегти конфіденційність, цілісність і доступність даних, що є важливим аспектом безпеки сучасних інформаційних систем.

Важливе місце в забезпеченні безпеки інформаційних системах займає облік.

Облік (англ. accounting) забезпечує ведення журналу подій і дій, що виконуються користувачами у системі. Це важливо для аналізу діяльності користувачів, виявлення потенційних загроз, розслідування інцидентів безпеки та дотримання законодавчих вимог.

<u>Облік може включати:</u>

- ✓ Логи доступу до системи;
- ✓ Історію дій користувачів;
- ✓ Звіти про використання ресурсів.

Дані обліку використовуються для моніторингу та аудиту безпеки, а також для підвищення ефективності системи. Облік дозволяє адміністраторам вчасно реагувати на підозрілі активності та забезпечувати безпеку даних.

Системи аутентифікації, авторизації та обліку постійно еволюціонують через

зростання кіберзагроз і підвищення вимог до конфіденційності. Підходи до захисту інформації повинні включати багаторівневі механізми захисту, інтеграцію сучасних технологій (наприклад, штучного інтелекту для аналізу поведінки користувачів), та суворе дотримання міжнародних стандартів.

Аутентифікація, авторизація та облік є фундаментальними складовими інформаційної безпеки, що допомагають забезпечити захищений доступ до систем і даних. Використання багатофакторної аутентифікації, сучасних протоколів авторизації та надійних механізмів обліку сприяє збереженню конфіденційності, цілісності та доступності інформації.

3.4. Моніторинг, аудит та адміністрування в СУД

Повернутися до початку

Моніторинг та аудит в системі управління доступом до інформаційних ресурсів є важливими процесами для забезпечення безпеки у сучасних інформаційних системах. Вони служать для відстеження та контролю дій користувачів, аналізу логів і перевірки відповідності політикам безпеки.

Моніторинг — це процес безперервного спостереження за діями, які виконуються користувачами в інформаційних системах. Основна мета моніторингу — забезпечення оперативного відстеження активностей, виявлення підозрілих або несанкціонованих дій та забезпечення реакції на можливі інциденти.

Основні характеристики моніторингу:

1. *Реальний час:* Моніторинг зазвичай виконується в режимі реального часу, щоб швидко виявляти аномалії.
2. *Відстеження активності користувачів:* Моніторинг охоплює дії користувачів,

такі як входи в систему, спроби доступу до ресурсів, зміни конфігурацій тощо.

3. *Автоматизовані повідомлення:* Системи моніторингу часто мають функції автоматичного оповіщення у разі виявлення підозрілих дій або порушень політик безпеки.
4. *Збір логів:* Всі події зберігаються у вигляді логів, які можуть бути використані для подальшого аналізу.

Приклади використання моніторингу:

- *Інтернет-банкінг:* Моніторинг активності користувачів для запобігання шахрайським діям, таким як несанкціоновані перекази чи входи з підозрілих IP-адрес.
- *Корпоративні системи:* Спостереження за тим, хто і коли отримує доступ до конфіденційних файлів або змінює їх.

Технології моніторингу:

- *SIEM-системи (Security Information and Event Management):* Об'єднують моніторинг та управління безпекою, збирають і аналізують логи для виявлення загроз і порушень.
- *Інструменти для відстеження мережевої активності:* Наприклад, IDS/IPS (Intrusion Detection System/Intrusion Prevention System), які відстежують активність в мережі та сигналізують про можливі вторгнення.

Аудит — це процес ретельного аналізу та перевірки активностей, що вже відбулися, з метою оцінки дотримання встановлених політик і норм безпеки. Аудит може бути внутрішнім або зовнішнім і спрямований на виявлення недоліків в управлінні доступом.

Основні характеристики аудиту:

1. *Регулярність:* Аудити можуть проводитися регулярно або у відповідь на інциденти безпеки.
2. *Документування:* Результати аудиту фіксуються у звітах для подальшого аналізу та прийняття заходів.
3. *Перевірка політик:* Аудитори перевіряють, чи відповідають практики управління доступом внутрішнім та зовнішнім вимогам безпеки.
4. *Виявлення вразливостей:* Під час аудиту можуть бути виявлені потенційні слабкі місця в системах управління доступом.

Приклади використання аудиту:

- *Регулярний внутрішній аудит у банківських установах:* Перевірка дотримання політик доступу до конфіденційної інформації клієнтів.
- *Аудит у державних установах:* Оцінка дотримання нормативних актів щодо захисту даних, наприклад, відповідно до стандартів GDPR (General Data Protection Regulation)[1].

Ключові аспекти аудиту:

- *Повнота даних:* Переконання, що всі дії користувачів і системні події належним чином документуються.
- *Аналіз логів:* Перевірка логів на наявність слідів аномальних або несанкціонованих дій.
- *Звітність:* Формування звітів для керівництва і відповідних органів, які містять рекомендації щодо покращення політик доступу.

[1] Загальний регламент про захист даних, який був прийнятий Європейським Союзом (ЄС) і набрав чинності 25 травня 2018 року. Це законодавчий акт, що визначає правила обробки та захисту персональних даних осіб у межах ЄС та регулює їх передачу за межі ЄС.

GDPR встановлює високі стандарти захисту приватності, які впливають на всі організації, що обробляють персональні дані осіб у ЄС, незалежно від їхньої географічної локації. Його основна мета — забезпечити, щоб фізичні особи мали контроль над своїми персональними даними та щоб ці дані оброблялися прозоро, безпечно і законно.

Взаємозв'язок між моніторингом та аудитом:

Моніторинг і аудит доповнюють один одного:

- ✓ Моніторинг забезпечує своєчасне виявлення інцидентів та дозволяє реагувати на них у реальному часі.
- ✓ Аудит дозволяє ретроспективно оцінити ефективність моніторингу, виявити прогалини в системі безпеки та внести відповідні зміни до політик управління доступом.

Технологічні інструменти для моніторингу та аудиту:

- ➢ Splunk: Платформа для збору, аналізу та візуалізації логів.
- ➢ ELK Stack (Elasticsearch, Logstash, Kibana): Система для моніторингу та аналізу логів у реальному часі.
- ➢ Auditd: Інструмент для аудиту на базі Linux-систем, який фіксує дії користувачів та системних процесів.

Моніторинг та аудит є ключовими елементами системи управління доступом до інформаційних ресурсів. Вони допомагають виявляти порушення, забезпечувати дотримання політик безпеки та підтримувати високий рівень захисту даних. Ефективна інтеграція обох процесів дозволяє своєчасно реагувати на загрози та підвищувати загальний рівень безпеки організації.

Адміністрування в системі управління доступом до інформаційних ресурсів — це процес налаштування, управління та моніторингу доступу користувачів до інформаційних систем і ресурсів. Адміністратор системи доступу відповідає за визначення, підтримку та контроль за політиками доступу, управління правами користувачів і забезпечення безпеки доступу до чутливої інформації. Адміністрування включає налаштування параметрів безпеки, розподіл ролей, моніторинг активностей користувачів, а також аудит і підтримку належної

конфіденційності, цілісності та доступності даних.

Основні функції адміністрування в системі управління доступом:

1. Створення та управління обліковими записами користувачів:
   - ❖ Адміністратор системи створює нові облікові записи для користувачів, присвоює їм відповідні ролі та права доступу, а також забезпечує їх належну автентифікацію.

Приклад: В організації адміністратор створює обліковий запис нового співробітника в системі, визначає його роль (наприклад, співробітник, менеджер або адміністратор), встановлює рівень доступу до ресурсів (наприклад, доступ до документів чи тільки до електронної пошти).

2. Управління ролями та правами доступу:
   - ❖ Ролі визначають рівень доступу, який користувач отримує до різних системних ресурсів. Це включає в себе налаштування прав на перегляд, редагування, видалення або адміністрування ресурсів.

Приклад: У корпоративній інформаційній системі ролі можуть бути розподілені між різними користувачами, наприклад, співробітник може мати лише доступ до звітів, тоді як менеджер може також мати можливість їх редагувати та публікувати.

3. Забезпечення політик доступу та безпеки:
   - ❖ Визначення та впровадження політик доступу, що регулюють, хто має доступ до яких ресурсів і за яких умов. Це включає в себе правила для однофакторної або багатофакторної аутентифікації, визначення мінімальних вимог до паролів, обмеження доступу за IP-адресами або часом доби.

Приклад: У банківських системах адміністратор може вимагати від користувачів проходити двофакторну аутентифікацію для доступу до чутливих даних, таких як фінансові звіти.

4. Налаштування моніторингу та аудиту:
    - ❖ Адміністратор здійснює налаштування систем моніторингу і аудиту, щоб відстежувати діяльність користувачів і виявляти потенційні загрози або порушення політик безпеки.

Приклад: В системах корпоративного обліку адміністратор може налаштувати відстеження спроб несанкціонованого доступу або дій, які можуть порушити внутрішню політику безпеки, наприклад, спроби редагування документів без належних прав.

5. Обробка запитів на доступ та управління ролями:
    - ❖ Адміністратор відповідає на запити користувачів щодо зміни прав доступу, наприклад, надання доступу до нових ресурсів або зміна ролі в залежності від зміни посадових обов'язків.

Приклад: Керівник відділу може запросити доступ до фінансових звітів для своїх співробітників, і адміністратор системи переглядає запит і надає відповідні права доступу.

6. Підтримка політики безпеки та реагування на інциденти:
    - ❖ Адміністратор відповідає за своєчасне вжиття заходів у разі порушення безпеки, таких як втрата або компрометація облікових записів.

Приклад: Якщо виявлено, що один із співробітників зловживає своїми правами доступу або має ознаки несанкціонованого доступу до даних, адміністратор може змінити паролі, заблокувати обліковий запис та провести розслідування.

Характеристики адміністрування в системі управління доступом:

1. Централізоване управління:
    - ✓ У великих організаціях адміністрування доступом здійснюється централізовано через єдину систему керування доступом. Це дозволяє адміністратору ефективно керувати правами користувачів, ролями та

політиками безпеки на рівні всієї організації.

Приклад: Використання програмних рішень, таких як Active Directory для централізованого управління користувачами в організації.

2. Автоматизація:
   - ✓ Сучасні системи управління доступом забезпечують автоматизацію багатьох процесів адміністрування, таких як створення облікових записів, зміна прав доступу або моніторинг активностей.

Приклад: Автоматичне оновлення доступу до ресурсів після того, як користувач змінює свою роль у компанії, або автоматичне блокування облікового запису після кількох невдалих спроб входу.

3. Безпека:
   - ✓ Адміністрування має важливе значення для забезпечення безпеки інформаційних систем. Неправильне налаштування прав доступу або рольових обмежень може призвести до витоку чутливої інформації або несанкціонованого доступу до критичних ресурсів.

Приклад: Адміністратор може помилково надати доступ до фінансових даних звичайному співробітникові, що може призвести до серйозних наслідків для компанії.

4. Аудит та звітність:
   - ✓ Адміністрування системи доступу включає в себе не тільки налаштування доступу, а й регулярний аудит активностей користувачів та звітність про потенційні загрози чи порушення політик безпеки.

Приклад: Системи з контролем доступу часто генерують звіти про спроби несанкціонованого доступу, зміни в ролях користувачів або відхилення від стандартних процедур безпеки.

Приклади адміністрування в реальному житті:

1. Корпоративні інформаційні системи:
   - У великих компаніях адміністратор може надавати різні рівні доступу залежно від посадових обов'язків, управлінських прав та обмежень для кожного користувача (наприклад, обмеження доступу до бухгалтерії чи HR-системи для співробітників).
2. Медичні організації:
   - Адміністрування доступу до медичних записів пацієнтів для медичних працівників, де доступ до певних записів мають тільки лікарі, а інші співробітники можуть мати лише доступ до загальної інформації або адміністративних даних.

Адміністрування в системі управління доступом до інформаційних ресурсів є критично важливою складовою безпеки інформаційних систем. Це забезпечує не лише контроль за доступом користувачів до ресурсів, але й гарантує дотримання політик безпеки, ефективну роботу систем та своєчасне реагування на загрози. Компетентне адміністрування дозволяє зберегти цілісність, конфіденційність і доступність даних в організації.

3.5. Роль людського фактору в забезпеченні інформаційної безпеки

Повернутися до початку

Сучасний світ зазнає швидкого розвитку технологій, що обумовлює зростання уваги до інформаційної безпеки. Однак, забезпечення цієї безпеки залежить не тільки від технічних рішень, але й від людського фактору, що часто стає ключовим чинником

в цій сфері. Людський фактор виявляється як основним джерелом ризиків, так і неоціненним ресурсом для їх мітигації[2].

Задля кращого розуміння ролі людського фактору в системі інформаційної безпеки варто проаналізувати різні аспекти, серед яких помилки персоналу, соціальне маніпулювання, практики навчання та культура безпеки в організаціях.

Помилки персоналу та їх вплив на інформаційну безпеку

Один із найбільш поширених аспектів людського фактору в інформаційній безпеці — це помилки персоналу. Незалежно від рівня автоматизації систем, людська помилка може призвести до серйозних наслідків. Це може бути випадкове розголошення конфіденційної інформації, ненавмисне відкриття шкідливих файлів або нехтування протоколами безпеки. Статистичні дані свідчать, що значна частина кіберінцидентів пов’язана саме з помилками людей.

Основні типи помилок персоналу включають:

- *Фішинг та соціальна інженерія:* атаки, спрямовані на обман працівників шляхом маніпулювання інформацією для отримання доступу до системи.
- *Неналежне управління паролями:* використання слабких паролів, їх повторне використання або ненадійне зберігання.
- *Інші недоліки у безпековій поведінці:* нехтування оновленнями програмного забезпечення, робота з незахищеними мережами тощо.

Соціальне маніпулювання: методи та захист

Соціальна інженерія — це метод психологічного впливу на працівників з метою отримання доступу до конфіденційної інформації або систем. Основні методи включають телефонні дзвінки, підроблені електронні листи, а також пряме

[2] Зм’якшення, зменшення (сили), ослаблення

використання соціальних зв’язків для збору необхідних даних.

Захист від соціальної інженерії передбачає:

- *Навчання персоналу:* регулярне проведення тренінгів з кібербезпеки для підвищення обізнаності про сучасні методи атак.
- *Впровадження багатофакторної автентифікації (MFA):* додатковий рівень захисту, що робить проникнення зловмисників більш складним.
- *Розробка політик реагування:* наявність чітких інструкцій щодо дій у випадку підозрілих контактів чи повідомлень.

Навчання та підвищення обізнаності

Ефективне навчання персоналу — це один з ключових елементів успішної системи інформаційної безпеки. Організації повинні інвестувати в регулярне навчання працівників, що включає як базові знання про безпеку, так і спеціалізовані курси з виявлення потенційних загроз.

Основні переваги навчання:

- *Зменшення ризиків:* підвищення обізнаності про ризики знижує ймовірність помилок.
- *Підвищення ефективності реакції:* добре підготовлений персонал здатен швидко реагувати на загрози.
- *Формування культури безпеки:* створення середовища, де інформаційна безпека є спільною відповідальністю.

Культура безпеки в організаціях

Культура безпеки — це сукупність цінностей, норм та практик, що спрямовані на забезпечення інформаційної безпеки. Вона передбачає, що кожен працівник

розуміє важливість своєї ролі у забезпеченні захисту даних.

Елементи культури безпеки включають:

- *Підтримка з боку керівництва:* активна участь керівництва у питаннях безпеки формує приклад для інших співробітників.
- *Підтримка відкритої комунікації:* створення середовища, де працівники можуть повідомляти про загрози без страху перед покаранням.
- *Заохочення відповідальної поведінки:* мотивація працівників до дотримання безпекових норм.

Роль людського фактору в забезпеченні інформаційної безпеки є складною та багатогранною. Вона включає як можливість виникнення помилок, так і потенціал для захисту від загроз. Залучення співробітників, їх навчання та формування культури безпеки можуть значно зменшити ризики та підвищити загальний рівень захисту організації.