ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ТЕМА 2. ЗАХИСТ ІНФОРМАЦІЇ НА РІВНІ ПРИКЛАДНОГО ТА СИСТЕМНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

План

1. Доступ до інформації та розмежування повноважень користувачів
2. Системи ідентифікації та автентифікації як інструменти забезпечення інформаційної безпеки досліджень
3. Аудит, моніторинг і логування дій користувачів: значення для доказування та відповідальності
4. Антивірусний та програмний захист у контексті забезпечення цілісності наукових даних

Доступ до інформації – фундаментальна категорія інформаційного права, кібербезпеки та управління організаційними системами. У сучасних цифрових екосистемах управління доступом розглядається як складова загальної архітектури інформаційної безпеки та корпоративного врядування.

У широкому значенні доступ до інформації – це регламентований правовими, організаційними та технічними механізмами процес надання суб'єктам можливості отримувати, використовувати, змінювати або передавати інформаційні ресурси відповідно до встановлених повноважень.

Методологічно концепція управління доступом базується на:

- теорії інформаційних потоків;
- принципах мінімальної достатності;
- концепції багаторівневої безпеки;
- ризик-орієнтованому підході;
- системному та процесному управлінні.

У науковому дискурсі управління доступом розглядається як інтеграційний механізм, що поєднує правові норми, організаційні регламенти та технічні інструменти контролю.

Класифікація інформації:

- публічна інформація;
- службова інформація;
- конфіденційна інформація;
- комерційна таємниця;
- персональні дані;
- інформація з обмеженим доступом;
- критична інформаційна інфраструктура.

Критерії класифікації інформації:

- за рівнем потенційної шкоди у разі несанкціонованого доступу;
- за стратегічним значення;
- за нормативним статусом;
- за економічною цінністю;
- за впливом на репутаційні та правові ризики.

Принципи інформаційної безпеки

Принцип мінімальних привілеїв (Least Privilege) – користувач отримує лише ті права, які необхідні для виконання службових функцій.
Принцип розподілу обов'язків (Segregation of Duties) – критичні процеси розподіляються між різними суб'єктами для запобігання зловживанням.
Принцип необхідності знання (Need-to-know) – доступ надається лише за умови обґрунтованої потреби.
Принцип багаторівневої перевірки (Multi-layered control) – створення кількох взаємодоповнюючих рівнів контролю (організаційного, процедурного, технічного), які забезпечують запобігання помилкам, зловживанням і ризикам на різних етапах процесу.
Принцип простежуваності та аудиту (Accountability and Auditability) – забезпечення можливості відстежити всі дії, рішення та операції в системі – із фіксацією відповідальних осіб, часу та змісту змін
У науковому вимірі ці принципи корелюють із концепціями внутрішнього контролю COSO та міжнародними стандартами ISO/IEC 27001.

Архітектурні моделі управління доступом:

DAC (Discretionary Access Control) – дискреційна модель, де власник ресурсу визначає права доступу.

MAC (Mandatory Access Control) – мандатна модель з централізованим контролем рівнів доступу.

RBAC (Role-Based Access Control) – рольова модель, де права надаються через ролі.

ABAC (Attribute-Based Access Control) – модель на основі атрибутів користувача, ресурсу та середовища.

Zero Trust Architecture – концепція нульової довіри, що передбачає постійну верифікацію доступу.

Організаційні механізми розмежування повноважень

Розмежування доступу включає:

- розробку внутрішніх положень та політик безпеки;
- створення матриці доступу;
- формалізацію посадових інструкцій;
- процедури ідентифікації та автентифікації;
- регламент управління життєвим циклом облікових записів.

Матриця доступу визначає відповідність:

користувач → роль → ресурс → рівень повноважень → строк дії доступу.

Особлива увага приділяється управлінню доступом у періоди:

- кадрових змін;
- реорганізації структури;
- кризових ситуацій;
- кіберінцидентів.

Технічні інструменти контролю доступу

Сучасні IT-рішення передбачають:

- системи IAM (Identity and Access Management);
- багатофакторну автентифікацію;
- системи журналювання та моніторингу;
- SIEM-платформи;
- контроль привілейованих користувачів (PAM);
- шифрування даних та сегментацію мережі.

У науковому контексті доцільно аналізувати ефективність цих інструментів через призму:

- зниження операційних ризиків;
- запобігання внутрішнім загрозам;
- мінімізації людського фактору;
- забезпечення комплаєнсу.

Неналежне управління повноваженнями призводить до:

- витоку персональних та комерційних даних;
- фінансових зловживань;
- маніпуляцій з бухгалтерськими показниками;
- саботажу інформаційних систем;
- порушення законодавства щодо захисту даних.

Особливо небезпечними є:

- накопичення надлишкових прав;
- несанкціоноване делегування доступу;
- відсутність періодичного аудиту прав.

Правове регулювання доступу до інформації

Правові основи формуються на рівні:

- конституційних гарантій права на інформацію;
- законодавства про захист персональних даних;
- нормативів кібербезпеки;
- галузевих регуляторних вимог (банківська, страхова, фінансова сфери);
- міжнародних стандартів та директив.

Регуляторні вимоги передбачають:

- фіксацію повноважень;
- обов’язковий аудит;
- відповідальність посадових осіб;
- санкції за порушення режиму доступу.

Доступ до інформації в умовах цифрової трансформації

Цифровізація змінює парадигму доступу:

- перехід до хмарних сервісів;
- дистанційна робота;
- інтеграція великих масивів даних;
- використання штучного інтелекту;
- розвиток відкритих даних.

Це створює нові виклики:

- трансграничний обіг інформації;
- складність контролю розподілених систем;
- необхідність автоматизованого моніторингу;
- зростання кількості кіберзагроз.

Інформаційна безпека наукових досліджень передбачає забезпечення конфіденційності, цілісності та доступності даних (CIA-модель) на всіх етапах життєвого циклу дослідження: формування гіпотези, збору емпіричних даних, обробки, зберігання, публікації та архівації.
Ідентифікація – процес встановлення унікальності суб'єкта в інформаційній системі.
Автентифікація – процес перевірки достовірності заявленої ідентичності.

У науковому середовищі ці механізми мають особливе значення через:

- роботу з великими масивами даних (Big Data);
- обробку персональних даних респондентів;
- міжнародну колаборацію;
- використання хмарних платформ;
- міжінституційну інтеграцію дослідницьких інфраструктур.

Ідентифікація та автентифікація формують базовий рівень кіберзахисту дослідницької екосистеми.

Система управління ідентичністю (IdM) – комплекс організаційних та технічних засобів, що забезпечують:

- створення цифрової ідентичності;
- керування атрибутами;
- перевірку доступу;
- аудит дій користувачів;
- управління життєвим циклом облікових записів.

Теоретичні підходи до управління ідентичністю:

- централізована модель (єдиний каталог користувачів);
- федеративна модель (Federated Identity);
- децентралізована модель (Self-Sovereign Identity);
- Zero Trust Identity Architecture.

У контексті досліджень особливого значення набуває інтеграція ORCID, Scopus Author ID, Google Scholar ID як елементів академічної ідентифікації.

Автентифікація базується на трьох основних групах факторів:
Що користувач знає (пароль, PIN-код).
Що користувач має (токен, смарт-карта, мобільний пристрій).
Що у користувача є (біометрія: відбиток пальця, розпізнавання обличчя, голос).

Розширені фактори автентифікації:

- поведінкова біометрія;
- геолокаційний фактор;
- аналіз контексту доступу.

Для наукових досліджень критичною є багатофакторна автентифікація (MFA), особливо при доступі до:

- репозиторіїв даних;
- результатів експериментів;
- державних наукових реєстрів;
- фінансової звітності грантових проєктів.

Порівняння факторів автентифікації

Критерій	Знання	Володіння	Біометрія
Рівень безпеки	Середній	Високий	Дуже високий
Вразливість до фішингу	Висока	Середня	Низька
Зручність	Висока	Середня	Висока
Вартість впровадження	Низька	Середня	Висока
Доцільність у дослідженнях	Базовий рівень	Рекомендовано	Для критичних даних

Архітектура систем автентифікації у наукових установах

1	**Каталог користувачів (LDAP / Active Directory)**	**централізована служба зберігання, структурування та адміністрування облікових записів, груп, ролей і політик доступу.**
2	Сервер автентифікації	сервер автентифікації здійснює перевірку достовірності облікових даних користувача та підтверджує його цифрову ідентичність
3	Система MFA (Multi-Factor Authentication)	це механізм багатофакторної автентифікації, що передбачає використання щонайменше двох незалежних факторів підтвердження особи:
4	Журналювання (логування)	процес автоматичної фіксації подій у системі: входів і виходів, змін прав доступу, спроб несанкціонованого доступу, адміністративних операцій, змін конфігурацій тощо.
5	Система моніторингу (SIEM — Security Information and Event Management)	платформа централізованого збору, кореляції та аналізу подій безпеки з різних джерел: серверів, мережевого обладнання, застосунків, систем доступу.
6	Модуль контролю доступу до дослідницьких ресурсів	спеціалізований компонент, який реалізує політики авторизації щодо наукових баз даних, електронних архівів, лабораторних систем, хмарних обчислювальних середовищ та інших дослідницьких інфраструктур.

Біометричні системи в наукових центрах

Біометрія застосовується для:

- доступу до лабораторій;
- серверних приміщень;
- центрів обробки даних;
- обмежених архівів.

Переваги:

- висока точність;
- неможливість передачі іншій особі;
- мінімізація людського фактору.

Недоліки:

- етичні питання;
- ризик витоку біометричних даних;
- складність правового регулювання.

Загрози системам ідентифікації

Основні кіберзагрози:

1. Фішинг (Phishing) – метод шахрайства, за якого зловмисник маскується під надійне джерело (банк, державний орган, сервіс) з метою отримання конфіденційних даних – логінів, паролів, банківських реквізитів (найчастіше здійснюється через електронну пошту, підроблені сайти або повідомлення в месенджерах);

2. Brute force-атаки – атаки «грубою силою», що полягають у переборі великої кількості комбінацій паролів або ключів доступу до моменту знаходження правильного варіанта (ефективність таких атак зростає за використання слабких або коротких паролів);

3. Credential stuffing – тип атаки, за якого зловмисники використовують раніше викрадені пари «логін–пароль» (з інших сервісів) для автоматизованого входу в інші системи (ґрунтується на поширеній практиці використання однакових паролів на різних ресурсах);

4. Man-in-the-Middle (MITM) – зловмисник перехоплює та, за потреби, змінює інформацію, що передається між двома сторонами (наприклад, користувачем і сервером) (може здійснюватися через незахищені Wi-Fi-мережі або шляхом підміни сертифікатів безпеки);

5. Викрадення токенів (Token hijacking) – отримання зловмисником сесійного токена або іншого маркера автентифікації, що дозволяє йому діяти від імені користувача без повторного введення пароля (часто відбувається через XSS-уразливості або перехоплення незахищених з’єднань);

6. Соціальна інженерія (Social engineering) – маніпулятивні методи впливу на людину з метою отримання доступу до конфіденційної інформації або ресурсів (ґрунтується не на технічних уразливостях, а на психологічних механізмах – довірі, страху, авторитеті, терміновості тощо).

Особливість академічного середовища – висока відкритість та міжінституційна взаємодія

Аудит, моніторинг і логування є ключовими механізмами забезпечення підзвітності (accountability) в інформаційних системах. Вони формують доказову базу для встановлення:

- факту доступу до інформації;
- зміни або видалення даних;
- перевищення повноважень;
- порушення політик безпеки;
- умисних або необережних дій користувачів.

Логування – автоматична фіксація подій у системі.

Моніторинг – безперервний аналіз подій у реальному часі.

Аудит – систематизована перевірка відповідності діяльності встановленим нормам і політикам.

У науковому та державному середовищі ці інструменти мають не лише технічне, а й процесуально-правове значення.

Логування створює так звані “цифрові сліди” (digital footprints), які можуть використовуватися як:

- докази в дисциплінарних провадженнях;
- матеріали службових розслідувань;
- джерела судових доказів;
- інструменти внутрішнього контролю.

Основні типи логів:

- системні журнали;
- журнали доступу;
- журнали змін баз даних;
- журнали мережевої активності;
- журнали адміністративних дій.

Ключові параметри, що фіксуються:

- ідентифікатор користувача;
- дата та час події;
- IP-адреса або пристрій;
- тип дії;
- результат операції.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Таблиця: Види логів та їх доказове значення

Вид журналу	Що фіксує	Доказове значення
Access log	Вхід/вихід	Встановлення факту присутності
Audit log	Зміни даних	Доказ модифікації
System log	Системні події	Аналіз збоїв
Security log	Спроби порушення	Виявлення злочинних дій

Види логів та їх доказове значення

Вид журналу	Що фіксує	Доказове значення
Access log	Вхід/вихід	Встановлення факту присутності
Audit log	Зміни даних	Доказ модифікації
System log	Системні події	Аналіз збоїв
Security log	Спроби порушення	Виявлення злочинних дій

Моніторинг як механізм превентивного контролю передбачає:

- аналіз подій у режимі реального часу;
- виявлення аномалій;
- автоматичне реагування на інциденти;
- формування сигналів тривоги.

З метою моніторингу дій користувачів використовуються:

1. SIEM-системи (Security Information and Event Management) – платформи централізованого збору, зберігання та кореляції подій безпеки з різних джерел (сервери, мережеве обладнання, застосунки, системи доступу), які забезпечують:

- виявлення підозрілої активності в реальному часі;
- формування алертів про інциденти;
- аналітику історичних даних;
- підтримку аудиту та розслідування інцидентів.

2. Поведінкова аналітика (UEBA – User and Entity Behavior Analytics) – Інструмент аналізу поведінкових моделей користувачів і пристроїв на основі статистичних та аналітичних методів.

Дозволяє виявляти:

- внутрішні загрози (insider threats);
- компрометацію облікових записів;
- аномальні дії, що не відповідають ролі користувача.

3. Алгоритми машинного навчання – використовуються для автоматичного виявлення складних закономірностей у великих масивах даних журналювання.

Застосовуються для:

- класифікації подій безпеки;
- прогнозування ризиків;
- зменшення кількості хибнопозитивних спрацювань;
- адаптивного оновлення моделей загроз.

4. Системи реагування (SOAR – Security Orchestration, Automation and Response) – платформи автоматизації реагування на інциденти безпеки.

SOAR інтегрується з SIEM та іншими засобами моніторингу й забезпечує:

- автоматичне виконання сценаріїв реагування (playbooks);
- ізоляцію скомпрометованих облікових записів;
- блокування підозрілих IP-адрес;
- координацію роботи аналітиків SOC.

Аудит як інструмент відповідності та доказування

Види аудиту:

- внутрішній аудит;
- зовнішній аудит;
- ІТ-аудит;
- комплаєнс-аудит

У контексті доказування аудит:

- встановлює причинно-наслідкові зв’язки;
- оцінює відповідність політикам;
- формує висновки для притягнення до відповідальності;
- визначає рівень вини.

Аудиторський висновок може бути використаний у:

- дисциплінарному провадженні;
- цивільному процесі;
- кримінальному провадженні;
- адміністративному процесі.

Цифрові логи можуть визнаватися доказами за умови:

- цілісності даних;
- незмінності інформації;
- підтвердженої автентичності;
- дотримання процедури зберігання;
- забезпечення ланцюга збереження доказів (chain of custody).

Ключові вимоги:

- синхронізація часу (NTP);
- криптографічний захист логів;
- обмеження доступу до журналів;
- архівування з контрольними сумами.

Відповідальність користувачів та посадових осіб

Аудит і логування дозволяють встановити:

1. **Факт перевищення повноважень** (аналіз журналів доступу та дій користувачів дає змогу виявити випадки, коли посадова особа здійснювала операції поза межами наданих їй прав).
2. **Незаконний доступ** (логи дозволяють зафіксувати спроби або факти несанкціонованого входу в систему – використання чужих облікових даних, підбір паролів, доступ із нетипових геолокацій чи пристроїв).
3. **Службову недбалість** (журналювання допомагає встановити бездіяльність або неналежне виконання службових обов’язків).
4. **Умисне втручання в систему** (фіксація змін конфігурацій, видалення даних, встановлення несанкціонованого програмного забезпечення або маніпуляцій із журналами подій дозволяє виявити навмисні дії, спрямовані на порушення цілісності, конфіденційності чи доступності інформації).

Відповідальність користувачів та посадових осіб

Можливі види відповідальності:

1. **Дисциплінарна відповідальність** (настає у разі порушення внутрішніх правил організації або посадових інструкцій).
2. **Матеріальна відповідальність** (застосовується у випадку завдання майнової шкоди установі)
3. **Адміністративна відповідальність** (настає за порушення вимог законодавства у сфері захисту інформації, персональних даних або кібербезпеки)
4. **Кримінальна відповідальність** (застосовується у разі вчинення злочинів у сфері використання електронно-обчислювальних систем, несанкціонованого втручання, розголошення державної чи комерційної таємниці тощо)
5. **Цивільно-правова відповідальність** (виникає у разі порушення прав фізичних або юридичних осіб, що спричинило шкоду)

Принципи моніторингу дій користувача:

1. **Принцип пропорційності** (обсяг і глибина моніторингу повинні відповідати поставленій меті та рівню ризику);
2. **Принцип мінімізації втручання** (збір і обробка даних мають здійснюватися в мінімально достатньому обсязі)
3. **Принцип законності** (моніторинг повинен здійснюватися на підставі норм законодавства та внутрішніх нормативних актів, із належним інформуванням працівників)
4. **Принцип обґрунтованості** (запровадження та масштаби моніторингу мають бути документально обґрунтовані).

Надмірне логування може створювати такі ризики:

1. **Порушення приватності** – збирання надлишкових даних (наприклад, про особисте листування або неслужбову активність) може порушувати право особи на повагу до приватного життя;
2. **Ризик витоку персональних даних** – чим більший обсяг зібраної інформації, тим вищий ризик її компрометації;
3. **Психологічний тиск** – постійний тотальний контроль може формувати атмосферу недовіри, знижувати мотивацію персоналу та створювати ефект «цифрового нагляду»;
4. **Правові спори** – непропорційний або непрозорий моніторинг може стати підставою для трудових конфліктів, судових позовів щодо захисту персональних даних або відшкодування моральної шкоди.

Інтеграція аудиту в систему управління ризиками

Аудит повинен бути інтегрований у:

- систему внутрішнього контролю;
- систему управління ризиками;
- політику кібербезпеки;
- комплаєнс-програми.

Принципи аудиту в системі управління ризиками:

1. **Превентивна функція** – спрямована на запобігання порушенням шляхом виявлення слабких місць у системі управління ще до настання негативних наслідків;
2. **Контрольна функція** – полягає у перевірці відповідності діяльності встановленим нормам, стандартам і процедурам;
3. **Доказова функція** – результати аудиту формують документально підтверджену інформацію, яка може використовуватися під час службових розслідувань, судових процесів або перевірок регуляторних органів;
4. **Управлінська функція** – аудит надає керівництву аналітичні висновки та рекомендації щодо вдосконалення процесів, оптимізації ресурсів і підвищення ефективності діяльності.
5. **Стратегічна функція** – сприяє формуванню довгострокової політики розвитку організації, підвищенню її стійкості до ризиків та зміцненню репутації.

Цілісність наукових даних як об’єкт інформаційної безпеки

Цілісність (Integrity) є ключовим компонентом тріади інформаційної безпеки (Confidentiality–Integrity–Availability). У контексті наукових досліджень цілісність означає:

- незмінність даних без санкціонованого втручання;
- захист від несанкціонованої модифікації;
- збереження достовірності результатів експериментів;
- відповідність даних первинним джерелам;
- відсутність прихованих змін або спотворень.

Порушення цілісності може призвести до:

- фальсифікації результатів;
- втрати грантового фінансування;
- дискредитації наукової установи;
- юридичної відповідальності;
- неможливості відтворення дослідження.

Антивірусний і програмний захист є базовим технічним механізмом підтримання цілісності даних у цифрових середовищах.

Загрози цілісності наукових даних

Шкідливе програмне забезпечення (malware):

Віруси – програми, які здатні самовідтворюватися та поширюватися на інші файли або системи (зазвичай завдають шкоди шляхом видалення, модифікації або блокування файлів);

Трояни (Trojan) – шкідливі програми, що маскуються під легітимні застосунки або файли (не саморозмножуються, але дозволяють зловмисникам отримати доступ до системи, викрадати дані, встановлювати інше шкідливе ПЗ або контролювати пристрій віддалено);

Ransomware – програми-вимагачі, які шифрують файли або блокують доступ до системи, вимагаючи викуп за відновлення доступу (часто поширюється через фішингові листи, шкідливі посилання або незахищені мережі);

Spyware – програмне забезпечення, призначене для таємного збору інформації про користувача та його активність: історію браузера, паролі, персональні дані (може працювати непомітно, передаючи зібрану інформацію зловмисникам для шахрайства, реклами або шантажу);

Rootkits – комплекси програм, що дозволяють зловмиснику приховати наявність інших шкідливих програм і отримати прихований контроль над системою (важко виявити, оскільки вони маскують свої процеси та файли від стандартних антивірусних засобів);

Несанкціонована модифікація баз даних;

Внутрішні загрози (інсайдерські ризики);

Помилки програмного забезпечення;

Атаки на хмарні середовища.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ДЯКУЮ ЗА УВАГУ!!!