ТЕМА 2

Завдання 1. Порівняти моделі контролю доступу (DAC, MAC, RBAC, ABAC) у контексті захисту наукових інформаційних систем.

Необхідно:

– визначити переваги та обмеження кожної моделі;

– оцінити їх придатність для університетських дослідницьких середовищ;

– запропонувати оптимальну модель для багаторівневого наукового проєкту.

Завдання 2. Проаналізувати типові сценарії витоку або несанкціонованого доступу до наукових даних (людський фактор, соціальна інженерія, внутрішні загрози).

Сформувати:

– карту загроз;

– класифікацію ризиків;

– систему превентивних заходів.

Завдання 3: Розробити модель розподілу ролей у дослідницькій групі (керівник, дослідник, аналітик, IT-адміністратор, зовнішній партнер).

Потрібно:

– визначити права доступу до даних;

– встановити рівні модифікації;

– передбачити механізми аудиту.

Завдання 4: Сформувати внутрішній регламент щодо:

– багатофакторної автентифікації;

– управління паролями;

– використання електронного підпису;

– доступу до хмарних сервісів.

Завдання 5: Дослідити:

- однофакторну автентифікацію;
- двофакторну (2FA);
- багатофакторну (MFA);
- біометричні системи;
- SSO (Single Sign-On).

Оцінити їх ефективність для захисту наукових баз даних.

Завдання 6: Проаналізувати сучасні підходи до захисту:

- від шкідливого ПЗ;
- ransomware;
- атак типу phishing;
- шкідливих макросів у наукових документах.

Окремо оцінити вплив кіберінцидентів на цілісність наукових результатів.

Завдання 7: Проаналізувати, як сприяють забезпеченню академічної відповідальності в дослідженнях:

- контроль доступу,
- аудит,
- логування,
- цифрові сліди

Завдання 8: Дискусія на тему:

1. Чи може надмірний контроль доступу обмежувати академічну свободу?
2. Чи допустимий повний моніторинг дій дослідників?
3. Чи є багатофакторна автентифікація обов'язковою умовою сучасної науки?
4. Чи повинні журнали дій користувачів зберігатися необмежений час?

Завдання 9: Створити повну модель безпеки, що включає:

- політику доступу;
- систему автентифікації;
- журналювання;
- резервне копіювання;
- антивірусний захист;
- план реагування на інциденти.

Окремо описати механізми відповідальності.

Теми для доповідей

1. Моделі контролю доступу в інформаційних системах наукових установ.
2. Роль автентифікації у забезпеченні достовірності наукових результатів.
3. Логування як інструмент цифрового доказування.
4. Інформаційна безпека досліджень у добу хмарних технологій.
5. Багатофакторна автентифікація: сучасні стандарти та перспективи.
6. Антивірусні рішення для захисту наукових даних.
7. Zero Trust архітектура в наукових інформаційних системах.
8. Кіберзагрози для наукових баз даних: аналіз сучасних кейсів.
9. Правове регулювання захисту інформації в науковій діяльності.
10. Баланс безпеки та академічної свободи в цифровому середовищі.
11. Відповідальність за порушення інформаційної безпеки у наукових установах.
12. Вплив кібератак на цілісність наукових досліджень.
13. Внутрішні загрози як фактор ризику наукової діяльності.
14. Аудит інформаційної безпеки як елемент системи управління якістю.

Тестові завдання:

1. Яка модель контролю доступу передбачає надання прав користувачем-власником ресурсу?

а) MAC
б) RBAC
в) DAC
г) ABAC

2. Який механізм найбільш ефективно мінімізує ризик компрометації пароля?

а) Часта зміна логіну;

б) Використання однакових паролів;

в) Багатофакторна автентифікація;

г) Відключення журналювання

3. Логування дій користувачів необхідне насамперед для:

а) прискорення роботи системи;

б) архівування програм;

в) доказування фактів порушення;

г) шифрування трафіку

4. Zero Trust архітектура базується на принципі:

а) повної довіри внутрішній мережі;

б) відсутності перевірки користувача;

в) постійної перевірки доступу;

г) відмови від автентифікації

5. Основною загрозою для цілісності наукових даних при ransomware-атаці є:

а) повільне з’єднання;

б) шифрування файлів з вимогою викупу;

в) видалення антивірусу;

г) блокування електронної пошти

6. Дослідник передав свій пароль колезі для тимчасового доступу до бази даних. Який принцип безпеки порушено?

а) принцип мінімальних привілеїв;

б) принцип унікальної ідентифікації;

в) принцип шифрування;

г) принцип резервування

7. Університет зазнав витоку дослідницьких даних через фішингову атаку. Який захід міг би мінімізувати наслідки?

а) вимкнення антивірусу;

б) використання MFA;

в) зменшення обсягу даних;

г) скасування логування

8. Під час аудиту встановлено відсутність журналів доступу до критичних даних. Це унеможливлює:

а) резервне копіювання;

б) доведення відповідальності;

в) автентифікацію;

г) шифрування

9. Який із наведених механізмів найбільше відповідає концепції забезпечення академічної доброчесності?

а) тотальний моніторинг без згоди користувача;

б) розмежування доступу та аудит змін у файлах;

в) відсутність журналювання;

г) одноразові паролі без фіксації подій

10. Який підхід є найбільш ефективним для захисту цілісності великих наукових масивів даних?

а) лише антивірус;

б) лише резервне копіювання;

в) комплексний підхід (контроль доступу + аудит + резервування + антивірус);

г) блокування зовнішніх носіїв