Міністерство освіти і науки україни

Київський національний університет будівництва і архітектури

Кафедра кібербезпеки та комп'ютерної інженерії

Графічний матеріал до Бакалаврської кваліфікаційної роботи Короткої Мілени Сергіївни

На тему:
«Управління доступом під час реалізації компонентів інформаційно-комунікаційних систем»

Науковий керівник:
к.т.н. доц. Ізмайлова О.В.

Київ 2026

Актуальність напряму

1. Стрімкий розвиток інформаційних технологій у XXI столітті суттєво трансформує всі сфери суспільного життя, зокрема інформаційно-комунікаційні системи, які стають основою функціонування сучасних організацій.
2. Зміни в інформаційному середовищі зумовлюють необхідність удосконалення теоретико-методологічних підходів до управління доступом, що дозволяє своєчасно реагувати на загрози, мінімізувати ризики несанкціонованого доступу та забезпечувати належний рівень захисту інформаційних ресурсів.
3. Особливого значення набуває впровадження сучасних моделей управління доступом, які враховують специфіку інформаційно-комунікаційних систем, їхню архітектуру та динамічний характер функціонування.

Мета, об’єкт та предмет дослідження

- **Метою роботи** є дослідження теоретико-методологічних основ управління доступом в інформаційно-комунікаційних системах.
- **Об’єктом дослідження** є процес управління доступом в інформаційно-комунікаційних системах.
- **Предметом дослідження** є теоретико-методологічні засади, методи та підходи до управління доступом в інформаційно-комунікаційних системах.

Нормативно-правова база

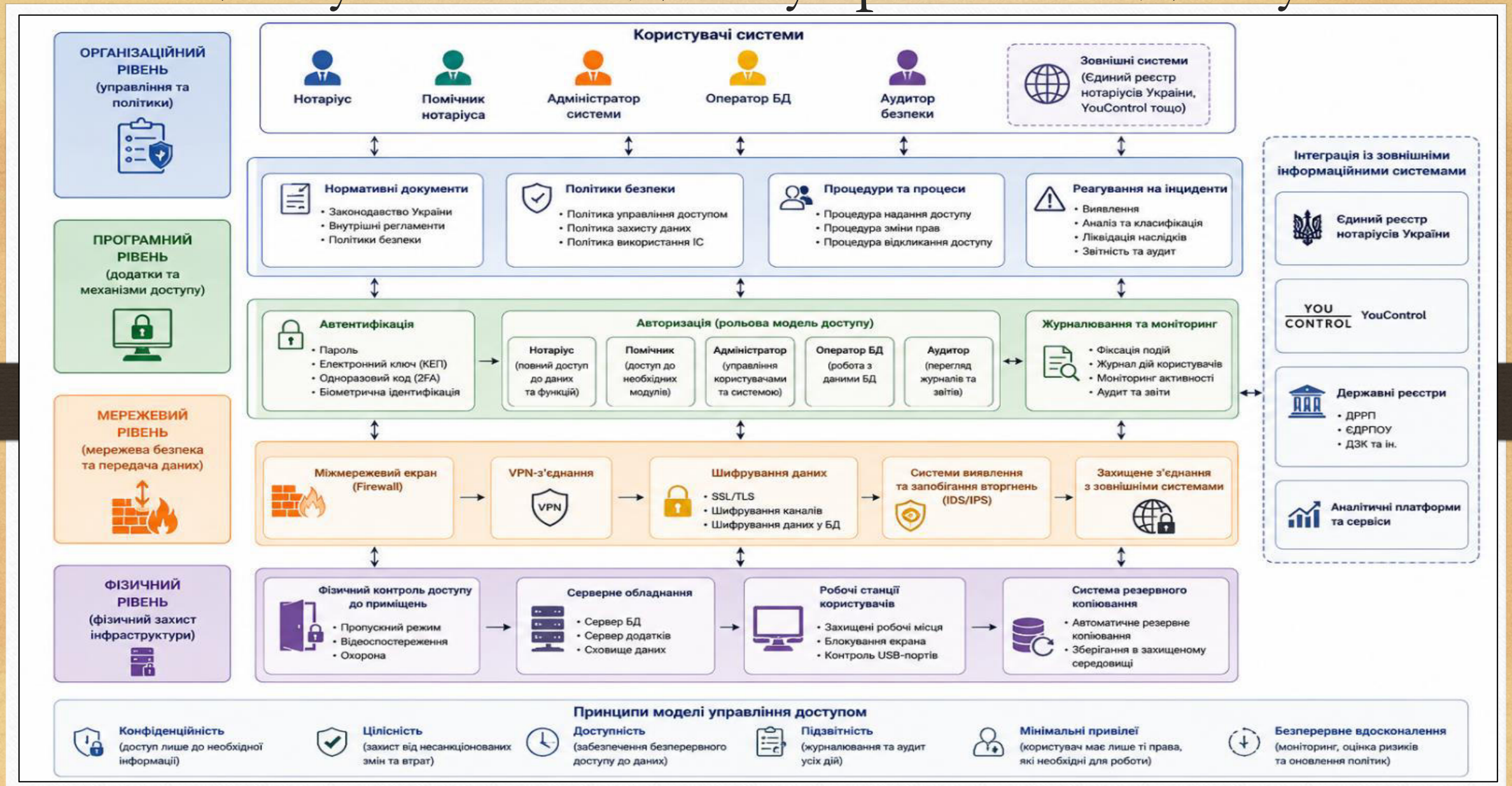
Управління доступом є ключовим механізмом забезпечення конфіденційності, цілісності та доступності інформації в інформаційно-комунікаційних системах.

Напрям дослідження	**Основні результати**
Мета управління доступом	Захист інформаційних ресурсів, надання користувачам лише необхідних прав доступу.
Основні принципи	Мінімальні привілеї, розмежування повноважень, автентифікація, авторизація, моніторинг доступу.
Моделі управління доступом	DAC, MAC, RBAC, ABAC; найбільш поширена – **RBAC**, перспективна – **ABAC**.
Нормативне забезпечення	Законодавство України та стандарти **ISO/IEC 27000**.
Практичне значення	Підвищення рівня інформаційної безпеки та вдосконалення захисту від сучасних кіберзагроз.

Досліджувана система забезпечує базовий рівень захисту, проте потребує модернізації механізмів управління доступом відповідно до сучасних вимог кібербезпеки.

Напрям аналізу	Основні результати
База дослідження	Система «Нотаріус» поєднує відкритий та обмежений доступ до інформаційних ресурсів.
Технології управління доступом	Автентифікація, авторизація, IAM, MFA, SSO, PAM, концепція Zero Trust.
Особливості реалізації	Комбінований доступ: публічні дані – відкриті, внутрішні ресурси – обмежені.
Виявлені недоліки	Статичні моделі доступу, недостатній захист автентифікації, обмежений моніторинг дій користувачів.
Напрями вдосконалення	Впровадження MFA, контекстного контролю доступу, журналювання та поведінкового аналізу користувачів.

Концептуальна модель управління доступом



Основні фактори багатофакторної автентифікації

Фактор	Характеристика	Приклади
Фактор знання	Інформація, яку знає користувач	Пароль, PIN-код
Фактор володіння	Об’єкт, яким володіє користувач	Токен, смартфон, електронний ключ
Біометричний фактор	Унікальні фізіологічні характеристики	Відбиток пальця, розпізнавання обличчя

Розподіл ролей користувачів у системі

Роль користувача	Основні функції	Рівень доступу
Нотаріус	Робота з документами, реєстрами, підписання документів	Повний доступ
Помічник нотаріуса	Підготовка документів, обробка заяв	Обмежений доступ
Адміністратор системи	Технічне обслуговування системи	Адміністративний доступ
Аудитор безпеки	Контроль журналів подій, аудит безпеки	Доступ до звітів

Рекомендовані механізми підвищення безпеки автентифікації

Механізм захисту	Призначення	Результат
Багатофакторна автентифікація	Додаткова перевірка особи користувача	Зниження ризику несанкціонованого доступу
Електронний цифровий підпис	Підтвердження автентичності документів	Захист електронних документів
Біометрична ідентифікація	Унікальна перевірка користувача	Підвищення точності автентифікації
Апаратні токени	Захист облікових записів	Неможливість віддаленого перехоплення доступу

Рекомендації щодо захисту мережевої інфраструктури

Захід безпеки	Функціональне призначення
VPN-з’єднання	Захист віддаленого доступу
SSL/TLS шифрування	Захист передачі даних
Firewall	Контроль мережевого трафіку
IDS/IPS системи	Виявлення кібератак
Сегментація мережі	Обмеження поширення загроз

Комплекс рекомендацій щодо підвищення безпеки доступу

Напрям удосконалення	Основні рекомендації
Автентифікація	Багатофакторний захист
Авторизація	Рольова модель доступу
Моніторинг	Автоматичне журналювання
Мережевий захист	VPN та криптографія
Фізична безпека	Контроль доступу до обладнання
Навчання персоналу	Підвищення цифрової грамотності
Аудит безпеки	Регулярна перевірка системи

Висновки

Концептуальна модель безпеки нотаріального кабінету передбачає комплексний багаторівневий захист даних на організаційному, програмному, мережевому та фізичному рівнях для надійного забезпечення їх конфіденційності, цілісності та доступності.

Основу системи становить рольове управління доступом за принципом мінімальних привілеїв та обов'язкове впровадження багатофакторної автентифікації (пароль, ЕЦП, OTP), що повністю нівелює недоліки застарілого парольного захисту. Ефективність адміністрування та стійкість до кіберзагроз підвищується завдяки автоматизації моніторингу, безперервному журналюванню подій та системам миттєвого блокування підозрілої активності користувачів. Стійкість інфраструктури додатково гарантується використанням сучасних криптографічних засобів, VPN-з'єднань, резервного копіювання, фізичним захистом серверів та регулярним навчанням персоналу методам протидії фішингу та мінімізації людського фактора.

Дякую за увагу!