Запорізький національный університет

Основи безпеки інформаційних систем

І.В.Козін

Задачі лекції

1. Стандарти і специфікації в області ІБ
2. Механізми безпеки
3. Класи безпеки
4. Інформаційна безпека розподілених систем

. Стандарти і специфікації в області ІБ

- оціночні стандарти, спрямовані на класифікацію інформаційних систем і засобів захисту за вимогами безпеки;
- технічні специфікації, що регламентують різні аспекти реалізації засобів захисту.

Ступінь довіри

1. Політика безпеки - набір законів, правил і норм поведінки, що визначають, як організація обробляє, захищає і поширює інформацію. Зокрема, правила визначають, у яких випадках користувач може оперувати конкретними наборами даних. Чим вище ступінь довіри системі, тим суворіше і різноманітніше повинна бути політика безпеки. В залежності від сформульованої політики можна вибирати конкретні механізми забезпечення безпеки. Політика безпеки - це активний аспект захисту, що включає в себе аналіз можливих загроз і вибір заходів протидії.

2. Рівень гарантованості - міра довіри, яка може бути надана архітектурі і реалізації ІС. Довіра безпеки може виникати як з аналізу результатів тестування, так і з перевірки (формальної чи ні) загального задуму і реалізації системи в цілому і окремих її компонентів. Рівень гарантованості показує, наскільки коректні механізми, що відповідають за реалізацію політики безпеки. Це пасивний аспект захисту.

Приклад Політика безпеки

1. Загальні положення
1.1. Мета і призначення цієї Політики
1.2. Область застосування цієї Політики
2. Вимоги та рекомендації
2.1. Відповідальність за інформаційні активи
2.2. Контроль доступу до інформаційних систем
2.2.1. загальні положення
2.2.2. Доступ третіх осіб до систем Компанії
2.2.3. Віддалений доступ
2.2.4. Доступ до мережі Інтернет
2.3. захист обладнання
2.3.1. Апаратне забезпечення
2.3.2. Програмне забезпечення
2.4. Рекомендовані правила користування електронною поштою
2.5. Повідомлення про інциденти інформаційної безпеки, реагування та звітність
2.6. Приміщення з технічними засобами інформаційної безпеки
2.7. управління мережею
2.7.1. Захист і збереження даних
2.8. Розробка систем і управління внесенням змін

Механизми безпеки

- довільне керування доступом;
- безпеку повторного використання об'єктів;
- мітки безпеки;
- примусове управління доступом.

Класи безпеки

Всього є шість класів безпеки - C1, C2, B1, B2, B3, A1. Щоб у результаті процедури сертифікації систему можна було віднести до деякого класу, її політика безпеки і рівень гарантованості повинні задовольняти заданим вимогам, з яких ми згадаємо лише найважливіші.

Клас С1

- довірена обчислювальна база повинна управляти доступом іменованих користувачів до іменованих об'єктів;
- користувачі повинні ідентифікувати себе, перш ніж виконувати будь-які інші дії, контрольовані довіреної обчислювальної базою. Для аутентифікації повинен використовуватися захисний механізм, наприклад паролі. Аутентифікаційна інформація повинна бути захищена від несанкціонованого доступу;
- довірена обчислювальна база повинна підтримувати область для власного виконання, захищену від зовнішніх впливів (зокрема, від зміни команд і / або даних) і від спроб стеження за ходом роботи;
- повинні бути в наявності апаратні і / або програмні засоби, що дозволяють періодично перевіряти коректність функціонування апаратних і мікропрограмних компонентів довіреної обчислювальної бази;
- захисні механізми повинні бути протестовані на предмет відповідності їх поведінки системної документації. Тестування повинне підтвердити, що у неавторизованого користувача немає очевидних способів обійти або зруйнувати засоби захисту довіреної обчислювальної бази;
- повинні бути описані підходи до безпеки, використовувані виробником, і застосування цих підходів при реалізації довіреної обчислювальної бази.

Клас С2

- права доступу повинні гранульований з точністю до користувача. Всі об'єкти повинні піддаватися контролю доступу;
- при виділенні що зберігається об'єкта з пулу ресурсів довіреної обчислювальної бази необхідно ліквідувати всі сліди його використання;
- кожен користувач системи повинен унікальним чином ідентифікуватися. Кожне реєстроване дія повинна асоціюватися з конкретним користувачем;
- довірена обчислювальна база повинна створювати, підтримувати і захищати журнал реєстраційної інформації, що відноситься до доступу до об'єктів, контрольованим базою;
- тестування повинне підтвердити відсутність очевидних недоліків у механізмах ізоляції ресурсів і захисту реєстраційної інформації.

Клас B1

• довірена обчислювальна база повинна управляти мітками безпеки, асоційованими з кожним суб'єктом і збереженим об'єктом;

• довірена обчислювальна база повинна забезпечити реалізацію примусового управління доступом всіх суб'єктів до всіх збереженим об'єктах;

• довірена обчислювальна база повинна забезпечувати взаємну ізоляцію процесів шляхом поділу їх адресних просторів;

• група фахівців, повністю розуміють реалізацію довіреної обчислювальної бази, повинна піддати опис архітектури, вихідні та об'єктні коди ретельному аналізу й тестуванню;

• повинна існувати неформальна або формальна модель політики безпеки, підтримуваної довіреної обчислювальної базою.

Клас B2

• забезпечуватися мітками повинні всі ресурси системи (наприклад, ПЗУ), прямо або побічно доступні суб'єктам;

• до довіреної обчислювальної базі повинен підтримуватися довірений комунікаційний шлях для користувача, що виконує операції початкової ідентифікації і аутентифікації;

• повинна бути передбачена можливість реєстрації подій, пов'язаних з організацією таємних каналів обміну з пам'яттю;

• довірена обчислювальна база повинна бути внутрішньо структурована на добре визначені, відносно незалежні модулі;

• системний архітектор повинен ретельно проаналізувати можливості організації таємних каналів обміну з пам'яттю і оцінити максимальну пропускну спроможність кожного виявленого каналу;

Клас В2

• повинна бути продемонстрована відносна стійкість довіреної обчислювальної бази до спроб проникнення;

• модель політики безпеки повинна бути формальною. Для довіреної обчислювальної бази повинні існувати описові специфікації верхнього рівня, точно і повно визначають її інтерфейс;

• в процесі розробки і супроводу довіреної обчислювальної бази повинна використовуватися система конфігураційного управління, що забезпечує контроль змін в описових специфікаціях верхнього рівня, інших архітектурних даних, реалізаційної документації, вихідних текстах, працюючої версії об'єктного коду, тестових даних і документації;

• тести повинні підтверджувати дієвість заходів щодо зменшення пропускної спроможності таємних каналів передачі інформації.

Клас В3

• для довільного керування доступом повинні обов'язково використовуватися списки управління доступом із зазначенням дозволених режимів;

• повинна бути передбачена можливість реєстрації появи або накопичення подій, що несуть загрозу політиці безпеки системи. Адміністратор безпеки повинен негайно сповіщатися про спроби порушення політики безпеки, а система, у разі продовження спроб, повинна присікати їх найменш болючим способом;

• довірена обчислювальна база повинна бути спроектована і структурована таким чином, щоб використовувати повний і концептуально простий захисний механізм з точно визначеною семантикою;

• процедура аналізу повинна бути виконана для тимчасових таємних каналів;

• повинна бути специфікована роль адміністратора безпеки. Отримати права адміністратора безпеки можна тільки після виконання явних, протоколюються дій;

• повинні існувати процедури та / або механізми, що дозволяють провести відновлення після збою чи іншого порушення роботи без ослаблення захисту;

• повинна бути продемонстрована стійкість довіреної обчислювальної бази до спроб проникнення.

Клас А1

• тестування має продемонструвати, що реалізація довіреної обчислювальної бази відповідає формальним специфікаціям верхнього рівня;

• крім описових, повинні бути представлені формальні специфікації верхнього рівня. Необхідно використовувати сучасні методи формальної специфікації і верифікації систем;

• механізм конфігураційного управління повинен поширюватися на весь життєвий цикл і всі компоненти системи, що мають відношення до забезпечення безпеки;

• має бути описано відповідність між формальними специфікаціями верхнього рівня і вихідними текстами.

Таблица 1. Классы безопасности в "Оранжевой книге"

Требования	Классы					
	C1	C2	B1	B2	B3	A1
1 Требования к политике безопасности						
1.1 Произвольное управление доступом	+	+	=	=	+	=
1.2 Повторное использование объектов	-	+	=	=	=	=
1.3 Метки безопасности	-	-	+	+	=	=
1.4 Целостность меток безопасности	-	-	+	+	=	=
1.5 Принудительное управление доступом	-	-	+	+	=	=
2 Требования к подотчетности						
2.1 Идентификация и аутентификация	+	+	+	=	=	=
2.2 Предоставление надежного пути	-	-	-	+	+	=
2.3 Аудит	-	+	+	+	+	=
3 Требования к гарантированности						
3.1 Операционная гарантированность						
3.1.1 Архитектура системы	+	+	+	+	+	=
3.1.2 Целостность системы	+	=	=	=	=	=
3.1.3 Анализ тайных каналов передачи информации	-	-	-	+	+	+
3.1.4 Надежное администрирование	-	-	-	+	+	=
3.1.5 Надежное восстановление	-	-	-	-	+	=
3.2 Технологическая гарантированность						
3.2.1 Тестирование	+	+	+	+	+	+
3.2.2 Верификация спецификаций архитектуры	-	-	+	+	+	+
3.2.3 Конфигурационное управление	-	-	-	+	=	+
3.2.4 Надежное распространение	-	-	-	-	-	+

Інформаційна безпека розподілених систем

Аутентифікація. Даний сервіс забезпечує перевірку автентичності партнерів по спілкуванню і перевірку автентичності джерела даних. Аутентифікація партнерів по спілкуванню використовується при встановленні з'єднання і, бути може, періодично під час сеансу. Вона служить для запобігання таких загроз, як маскарад і повтор попереднього сеансу зв'язку. Аутентифікація буває односторонньою (зазвичай клієнт доводить свою справжність сервера) і двосторонньої (взаємної).

Управління доступом. Забезпечує захист від несанкціонованого використання ресурсів, доступних через мережу.

Конфіденційність даних. Забезпечує захист від несанкціонованого отримання інформації. Окремо згадаємо конфіденційність трафіку (це захист інформації, яку можна отримати, аналізуючи мережеві потоки даних).

Цілісність даних підрозділяється на підвиди залежно від того, який тип спілкування використовують партнери - з встановленням з'єднання або без нього, захищаються Чи всі дані або тільки окремі поля, чи забезпечується відновлення в разі порушення цілісності.

Неспростовності (неможливість відмовитися від вчинених дій) забезпечує два види послуг: неспростовності з підтвердженням автентичності джерела даних і неспростовності з підтвердженням доставки. Побічним продуктом неспростовності є автентифікація джерела даних.

Інформаційна безпека розподілених систем

	1	2	3	4	5	6	7
Аутентифікація	-	-	+	+	-	-	+
Управління доступом	-	-	+	+	-	-	+
Конфіденційність з'єднання	+	+	+	+	-	+	+
Конфіденційність поза з'єднання	-	+	+	+	-	+	+
Виборча конфіденційність	-	-	-	-	-	+	+
Конфіденційність трафіку	+	-	+	-	-	-	+
Цілісність з відновленням	-	-	-	+	-	-	+
Цілісність без відновлення	-	-	+	+	-	-	+
Виборча цілісність	-	-	-	-	-	-	+
Цілісність поза з'єднання	-	-	+	+	-	-	+
Неспростовності	-	-	-	-	-	-	+

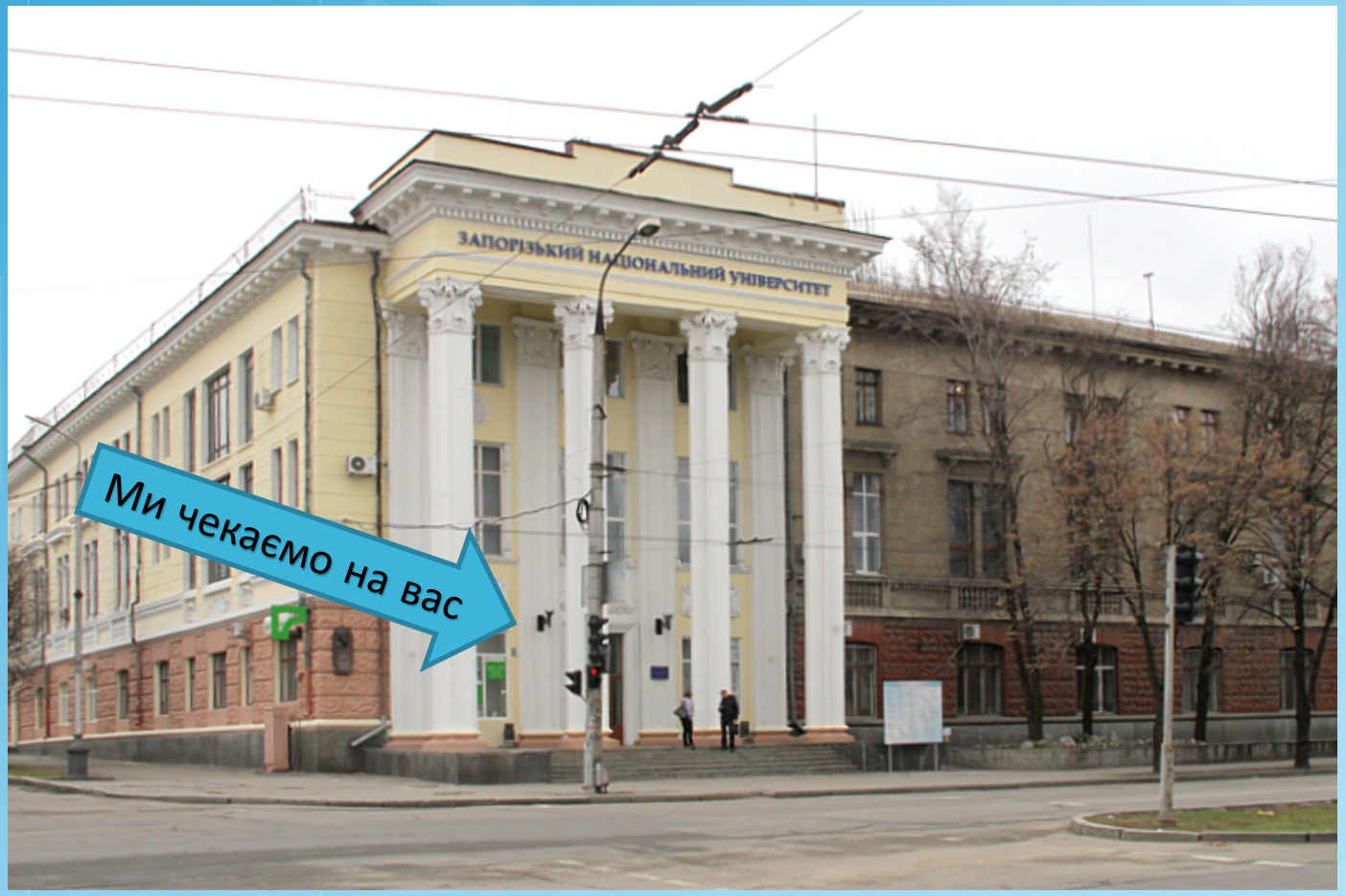
Мережеві механізми безпеки

- шифрування;
- електронний цифровий підпис;
- механізми управління доступом. Можуть розташовуватися на будь-який з точок, що беруть участь у спілкуванні сторін або в проміжній крапці;
- механізми контролю цілісності даних. У рекомендаціях X.800 розрізняються два аспекти цілісності: цілісність окремого повідомлення або поля інформації та цілісність потоку повідомлень або полів інформації. Для перевірки цілісності потоку повідомлень (тобто для захисту від крадіжки, переувпорядкування, дублювання та вставки повідомлень) використовуються порядкові номери, тимчасові штампи, криптографічне зв'язування або інші аналогічні прийоми;

Мережеві механізми безпеки

- механізми аутентифікації. Згідно з рекомендаціями X.800, аутентифікація може досягатися за рахунок використання паролів, особистих карток або інших пристроїв аналогічного призначення, криптографічних методів, пристроїв вимірювання та аналізу біометричних характеристик;
- механізми доповнення трафіку;
- механізми управління маршрутизацією. Маршрути можуть вибиратися статично або динамічно. Крайова система, зафіксувавши неодноразові атаки на певному маршруті, може відмовитися від його використання. На вибір маршруту здатна вплинути мітка безпеки, асоційована з переданими даними;
- механізми нотарізації. Служать для запевнення таких комунікаційних характеристик, як цілісність, час, особи відправника та одержувачів. Засвідчення забезпечується надійною третьою стороною, що володіє достатньою інформацією. Зазвичай нотарізація спирається на механізм електронного підпису.

А що буде далі…



..ну що, нарешті ...

Пора прощатися.

До побачення!