Лабораторна робота №10.

Моделювання підсистеми аудиту

Мета роботи

ознайомити студентів з місцем та задачами підсистеми реєстрації в системах захисту інформації від несанкціонованого доступу.

Теоретичні відомості

Підсистема реєстрації є сукупністю таких механізмів захисту, що здійснюють реєстрацію всіх подій в обчислювальній системі, які прямо чи опосередковано стосуються її безпеки. Використання механізмів реєстрації обумовлено такими чинниками:

1) оскільки обчислювальні системи складаються з великої кількості компонентів та мають дуже складну структуру, практично неможливо гарантувати відсутність помилок при їх розробці, а також адміністративних помилок під час їх експлуатації;
2) побудовані за допомогою криптографічних механізмів захисту системи є вразливими внаслідок можливості розкриття засобами криптоаналізу, а системи, що використовують паролі, – внаслідок можливості підбору паролю;
3) використання систем розмежування доступу обмежує користувачів системи певними правилами, дотримання яких не завжди можна забезпечити організаційними заходами;
4) навіть найдосконаліша система розмежування доступу є вразливою від дій користувачів, що зловживають своїми повноваженнями.

В якості прикладів подій, що реєструються, можна навести включення та виключення системи, вхід у систему та вихід з неї користувачів, невдалі спроби автентифікації, доступ суб'єктів до об'єктів, зміну повноважень суб’єктів по відношенню до об'єктів та інші. Реєстрація має відбуватися як на рівні системного (операційна система), так і на рівні прикладного (наприклад сервер бази даних) програмного забезпечення.

Для реєстрації подій створюється спеціальний файл (або група файлів), що носить назву **журналу реєстрації**. Журнал реєстрації, як правило, містить інформацію про час, дату, місце, тип та результати кожної зареєстрованої події. Система захисту інформації від несанкціонованого доступу повинна забезпечити захист своїх журналів реєстрації від несанкціонованого доступу, знищення або спотворення.

Хід роботи

1. Доповніть програму, розроблену в ході Лабораторних робіт № 7,8 механізмом реєстрації подій. Обов'язково повинні реєструватися вдалі та невдалі спроби автентифікації та вдалі і невдалі спроби доступу до об'єктів.
2. Відлагодьте програму та запротоколюйте її роботу у вигляді таблиці з двох стовпчиків. Перший має містити дії користувача, другий – їх відображення в журналі аудиту.
3. Оформіть звіт.

Звіт має містити

1) вихідні тексти серверної частини програми.
2) протоколи роботи програми.
3) блок-схему; діаграму класів або модулів, або data-flow diagram (на вибір) та діаграму прецедентів розробленого ПЗ (виконуються за допомогою UML – ПЗ);
4) висновок.

Контрольні запитання

1) Спробуйте ідентифікувати ознаки тих чи інших порушень безпеки, спираючись на отриманий вами журнал реєстрації. Охарактеризуйте труднощі, що виникають при рішенні цієї задачі.
2) Проаналізуйте взаємодію підсистеми реєстрації з підсистемами автентифікації та управління доступом в розробленій системі.
3) Оцініть рівень реєстрації в розробленій системі згідно НД ТЗІ 2.5-004-99. Що можна зробити, щоб його підвищити?