Огляд моделей захисту інформації в інформаційних системах

Савчук С.О.
Науковий керівник – к.т.н.,доц. Тітова В.Ю.
Хмельницький національний університет

В сучасному суспільстві комп'ютерні системи активно впроваджуються у фінансові, юридичні, промислові, торгові та соціальні галузі. У зв'язку з цим швидко зростає інтерес до проблем збереження та захисту інформації.

Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виняткове право певної держави [1]. Проте в останні роки збільшилися спроби несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів різних країн.

Згідно з оглядами міжнародних агентств з інформаційної безпеки, можна констатувати таке [2-3]:

- метою створення шкідливих програм і проведення атак стає, крім отримання грошового прибутку, крадіжка і подальше використання будь-якої можливої інформації
- з'являється новий клас шкідливих програм, націлений як на крадіжку персональної інформації користувачів, так і на тотальну крадіжку всіх інших даних.

А тому однією з актуальних на сьогоднішній день задач є вирішення питань ефективного захисту інформації, як від зовнішніх, так і від внутрішніх загроз, за рахунок створення та впровадження систем захисту інформації в автоматизованих системах підприємств, установ та організацій [2-3], що, серед іншого, потребує формалізації задачі захисту інформації для її наступної реалізації програмними та іншими засобами.

Відносно інформаційних систем застосовують наступні категорії безпеки [2-3]:

- надійність - гарантія того, що система працює в нормальному та позаштатному режимах так, як заплановано;
- точність - гарантія точного та повного виконання всіх команд;
- контроль доступу - гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;
- контрольованість - гарантія того, що в будь-який момент може бути зроблена повноцінна перевірка будь-якого компонента програмного комплексу;
- контроль ідентифікації - гарантія того, що клієнт, підключений у цей момент до системи, є саме тим, за кого себе видає;
– стійкість до навмисних збоїв - гарантія того, що при навмисному внесенні помилок у межах заздалегідь обговорених норм система буде

працювати так, як обговорено заздалегідь.

На основі зазначених категорій було розроблено кілька моделей інформаційної безпеки інформаційних систем.

Однією з перших моделей була модель Біба (рис.1) [2-3]. Відповідно до неї всі суб'єкти та об'єкти попередньо поділяються на декілька рівнів доступу, а потім на їх взаємодії накладаються наступні обмеження: 1) суб'єкт не може викликати на виконання суб'єкти з більш низьким рівнем доступу; 2) суб'єкт не може модифікувати об'єкти з більш високим рівнем доступу. Фактично, ця модель дуже нагадує обмеження, введені в захищеному режимі мікропроцесорів Intel 80386+ щодо рівнів привілеїв.

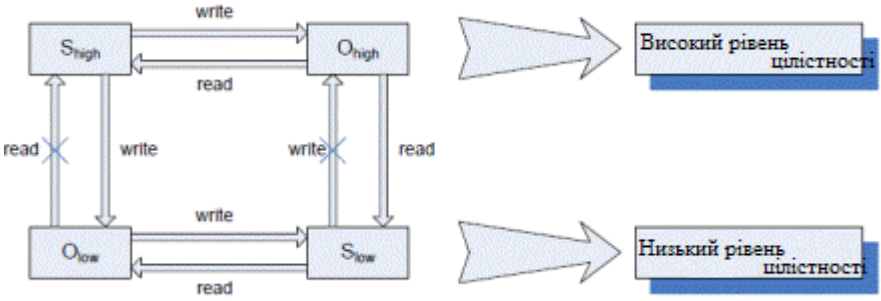

Рисунок 1 – Модель інформаційної безпеки Біба

Модель Гогена-Мезигера заснована на теорії автоматів [2-3]. Відповідно до неї система може при кожній дії переходити тільки з одного дозволеного стану в декілька інших. Суб'єкти та об'єкти в даній моделі захисту розбиваються на групи - домени і перехід системи з одного стану в інший виконується тільки відповідно до так званої таблиці дозволів, у якій зазначено, які операції може виконувати суб'єкт, скажімо, з домена C над об'єктом з домена D. У даній моделі при переході системи з одного дозволеного стану в інший використовуються транзакції, що забезпечує загальну цілісність системи.

Сазерлендська модель захисту наголошує на взаємодії суб'єктів та потоків інформації [2-3]. Так само як і у попередній моделі, тут використовується машина станів з множиною дозволених комбінацій станів і деяким набором початкових позицій. У даній моделі досліджується поведінка множинних композицій функцій переходу з одного стану в інший.

Важливу роль у теорії захисту інформації відіграє модель захисту Кларка-Уілсона (рис.2) [2-3]. Засновано дану модель на використанні транзакцій і ретельному оформленні прав доступу суб'єктів до об'єктів. В даній моделі вперше досліджена захищеність третьої сторони в даній проблемі - сторони, що підтримує всю систему безпеки. Цю роль в інформаційних системах відіграє програма-супервізор. Крім того, у моделі Кларка-Уілсона транзакції вперше були побудовані за методом верифікації,

тобто ідентифікація суб'єкта здійснюється не тільки перед виконанням команди від нього, але й повторно після виконання. Це дозволило зняти проблему підміни автора в момент між його ідентифікацією й самою командою.

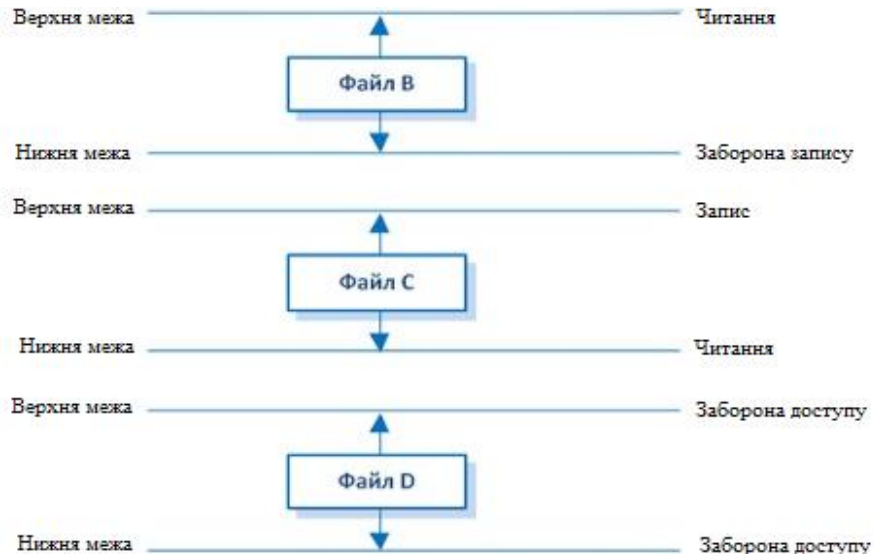

Рисунок 2 – Модель інформаційної безпеки Кларка-Уілсона.

Враховуючи переваги та недоліки наведених вище моделей, можна зробити висновки, що модель Кларка-Уілсона є однією із найкращих відносно підтримки цілісності інформаційних систем, а тому саме її доцільно взяти за основу для системи захисту інформації, описаній у [4].

Перелік посилань

1. Про державну таємницю [Електрон. ресурс] : закон України// Відомості Верховної Ради (ВВР). – 1994. – №16, ст. 93. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3855-12

2. Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие / Е.К. Баранова, А.В. Бабаш. – М.: РИОР: ИНФРА-М, 2017. – 322 с. – ISBN: 978-5-369-01450-9

3. Бирюков А.А. Информационная безопасность. Защита и нападение/ А.А. Бирюков. – М. : ДМК-Пресс, 2017. – 434 с. – ISBN: 978-5-97060-435-9

4. Тітова В.Ю. Концептуальна модель системи захисту інформації в сучасних компютерних системах/ В.Ю. Тітова, С.О. Савчук, В.Ю. Черниш// Вісник ХНУ. - Хмельницький: ХНУ, 2019. - №3. - с. 164-168.