23. Гасий Г. М. Трудоемкость монтажа сталежелезобетонных конструкций / Г. М. Гасий // Сучасне промислове та цивільне будівництво. – Макіївка: ДонНАБА, 2014. – Т. 10. – № 2. – С. 141–146.

24. Гасий Г. М. Эффективные конструктивные решения для пространственных сталежелезобетонных несущих элементов / Г. М. Гасий, О. С. Заболотский // ҚазБСҚА ХАБАРШЫСЫ. – Алматы: ҚазБСҚА, 2016. – № 3(61). – С. 94–103.

25. Гасій Г. М. Динаміка розвитку, сутність та галузь застосування просторових структурно-вантових сталезалізобетонних конструкцій / Г. М. Гасій // Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна. – Дніпро, 2017. – № 5(71). – С. 107–114.

26. Гасій Г. М. Можливості використання структурно-вантових систем в будівництві / Г. М. Гасій // Сталезалізобетонні конструкції: дослідження, проектування, будівництво, експлуатація. – № 12. – Полтава, 2016. – С. 71–75.

27. Гасій Г. М. Основи формотворення і проектування просторових покриттів із структурно-вантових сталезалізобетонних конструкцій / Г. М. Гасій // Строительство, материаловедение, машиностроение. – Дн-ск: ПГАСА, 2016. – № 87. – С. 48–53.

28. Гасій Г. М. Просторові структурно-вантові сталезалізобетонні конструкції: монографія / Г. М. Гасій – Полтава: ТОВ «АСМІ», 2018. – 347 с.

29. Стороженко Л. І. Великопролітні структурно-вантові сталезалізобетонні покриття для будівель і споруд аеропортів / Л. І. Стороженко, Г. М. Гасій // Проблеми розвитку міського середовища. – К.: НАУ, 2016. – № 2. – С. 72–79.

**Безносюк Л.О.**

*студент,*

*Одеська національна академія зв'язку імені О.С. Попова*

## ЗАХИСТ БАЗИ ДАНИХ ВІД АТАК І НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Зростаючий попит на інформацію приводить до виокремлення інформаційної діяльності, у результаті якої виникають нематеріальні об'єкти правовідносин, в окремий вид.

Побудована належним чином база даних забезпечує доступ до оновлених і точних відомостей. Оскільки правильна структура є необхідною умовою для досягнення поставленої мети під час роботи з

базою даних, доцільним буде вивчення принципів правильної побудови бази даних для конфіденційності та уникнення атак.

Були досліджені такі публікації як навчальний посібник Гайна Г.А. Основи проектування баз даних [1], де розглянуто головні концепції проектування і побудови баз даних, основні моделі баз даних, архітектури СУБД. В підручнику Пасічник В.В. Організація баз даних та знань [2] детально і ґрунтовно викладено основи класичної та сучасної теорії, а також важливі практичні аспекти організації баз даних та знань. Сутність безпеки баз даних розглянуто у книзі Пономаренко В.С. Інструментальні засоби розробки та підтримки баз даних розподілених інформаційних систем [3].

Безпека баз даних – стан захищеності життєво важливих інтересів корпорацій та підприємств, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Кожен збій роботи бази даних може паралізувати роботу цілих корпорацій, фірм, що призведе до великих матеріальних втрат.

Метою даної роботи є огляд питань теоретичного аналізу і практичних рекомендацій щодо збереження значних обсягів інформації (даних).

Зрозуміти що таке бази даних та якими засобами їх можна захистити від несанкціонованого доступу.

Дані в базах даних повинні зберігатися з гарантуванням безпеки та конфіденційності. Інформація не повинна бути загубленою або викраденої.

Модель загроз – фізичне, математичне, описову уявлення властивостей або характеристик загроз безпеки інформації.

Модель загроз безпеки персональних даних необхідна для визначення вимог до системи захисту. Без моделі загроз неможливо побудувати адекватну (з точки зору грошових витрат) систему захисту інформації, що забезпечує безпеку персональних даних.

Для того щоб СУБД була найбільш захищеною і забезпечувала гарантію того, що конфіденційна інформація не може бути отримана третьою стороною, необхідно розуміти її уразливості і постаратися мінімізувати або ліквідувати їх. Спроби атак на СУБД можуть бути зовнішніми і внутрішніми. Все залежить від ступеня обізнаності зловмисника.

На даний момент виділяють наступні атаки: PL / SQL-ін'єкції, SQL-ін'єкції, переповнення буфера, некоректна робота об'єднань і уявлень.

SQL-ін'єкція – це атака, в ході якої змінюються параметри SQL-запитів до бази даних. В результаті запит набуває зовсім інший зміст, і в разі недостатньої фільтрації вхідних даних здатний не тільки зробити висновок конфіденційної інформації, а й змінити / видалити дані.

Основні методи захисту, що реалізовані у більшості СУБД, полягають у наступному: використання паролю; розподілення прав доступу до складових чи інформації сховища або бази даних між користувачами; шифрування й криптографія даних та програмних модулів.

Захист від несанкціонованого доступу через використання паролю є одним з найпоширеніших та ефективних способів.

| ТИП АТАКИ | МЕТОД ЗАХИСТУ |
|---|---|
| Виконання коду (Command Execution) | Перевірка даних на достовірність |
| Парольні атаки | При використанні звичайних паролів намагайтеся придумати такий, який було б важко підібрати |
| Атаки на рівні додатків | Читайте лог - файли, підпишіться на послуги CERT |
| Зловживання довірою | Ризик зловживання довірою можна знизити за рахунок більш жорсткого контролю рівнів довіри в межах своєї мережі |
| Переадресація портів | Використання надійних моделей довіри (попередній пункт) |
| Захист від несанкціонованого доступу | Скорочення або повна ліквідація можливостей хакера з отримання доступу до системи за допомогою несанкціонованого протоколу |

**Рис. 1. Типи атак і методи захисту БД**

Паролі встановлюються користувачами або адміністраторами, а їх облік і зберігання забезпечується СУБД у зашифрованому вигляді в певних системних файлах. Незручність полягає у тому, що всі користувачі мають один пароль і за недбалого відношення він може стати надбанням третьої особи.

Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Сьогодні використовується шість основних способів захисту: перешкода, маскування, регламентація, управління, примус, спонукання.

Для вирішення зазначених проблем забезпечення інформаційної безпеки СУБД необхідно перейти від методу закриття уразливостей до комплексного підходу забезпечення безпеки сховищ інформації. Основними етапами цього переходу, повинні стати наступні положення:

– розробка комплексних методик забезпечення безпеки сховищ даних на підприємстві;

– оцінка і класифікація загроз і уразливостей СУБД;

– розробка стандартних механізмів забезпечення безпеки.

**Список використаних джерел:**

1. Гайна Г.А. Основи проектування баз даних: Навчальний посібник / Г.А. Гайна. − К.: КНУБА, 2005. – 204 с.

2. Пасічник В.В. Організація баз даних та знань / В.В. Пасічник, В.А. Резніченко. – К.: Видавнича група BHV, 2006. – 384 с.

3. Пономаренко В.С. Інструментальні засоби розробки та підтримки баз даних розподілених інформаційних систем / В.С. Пономаренко, Павленко Л.А. – Х.: Вид. ХДЕУ, 2001. – 132 с.