Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кібербезпека
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

Магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: **Методика захисту конфіденційності інформації в базах даних MS SQL та MySQL від sql-атак**

Виконав: студент (ка) 6 курсу, групи СБм
спеціальності (напряму підготовки) 125
Кібербезпека
(шифр і назва спеціальності (напряму підготовки))
(підпис) Осельський С. В. (прізвище та ініціали)

Керівник (підпис) Козак Р. О. (прізвище та ініціали)

Нормоконтроль (підпис) (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

м. Тернопіль – 2019

Зміст

Анотація

Пояснювальна записка: 96 сторінок, 20 рисунків,13 лістингів, 70 джерело.

Об’єкт дослідження: процес впровадження змін в базах даних несанкціонованими користувачами з метою порушення конфіденційності баз даних.

Мета роботи: підвищення рівня захисту конфіденційності інформації баз даних з метою протидії найпоширенішим типам кібератак.

Методи дослідження: методи індукції, порівняння, аналізу, синтезу, дедукції.

У роботі досліджено методи захисту інформації на рівні баз даних та авторизації. Проаналізовано основні принципи і методи захисту інформації. Запропоновано методи захисту баз даних від стороннього втручання. Розроблено метод захисту конфіденційності інформації в базах даних MS SQL.

В економічному розділі визначено економічну ефективність та окупності витрат необхідних для реалізації запропонованого методу.

Практичне значення роботи полягає у визначенні нових можливостей для захисту різних баз даних, оптимізації процесу написання запитів до баз даних, а також впровадження сучасних методів захисту конфіденційної інформації за допомогою надійних комплексних систем.

Результати проведеного дослідження можуть використовуватись для конфігурації серверів, зокрема розподілених серверів, для підвищення рівня конфіденційності інформації та її комплексного захисту.

Наукова новизна полягає в тому, що вперше розроблено комплексний метод захисту конфіденційної інформації в базах даних на основі елементів існуючих методів, а також запропонований інноваційний метод для розподілених серверів баз даних на основі технології блокчейн.

Ключові слова: SQL-ін’єкції, MS SQL, mySQL, конфіденційність, авторизації, блокчейн.

Abstract

Explanatory note: 92p., 20 figures, 70 sources.

The object of the research: the process of implementing the process of making changes to data by unauthorized users in the privacy of databases.

Purpose: To enhance the security of database information to counter the most common types of cyberattacks.

Research methods: methods of induction, comparison, analysis, synthesis, deduction.

The methods of data protection in databases at the level of databases and authorization are investigated. The basic methods of information protection are analyzed. Methods for protecting databases from third-party interference are suggested. A method of protecting the privacy of information in MS SQL databases has been developed.

The economic section identifies the cost-effectiveness and cost recovery required to implement the proposed method.

The practical importance of the work lies in identifying the capabilities to protect different databases, and streamlining the process of writing database queries, as well as implementing modern methods of protecting sensitive information through robust integrated systems. The findings of this study can be used to configure servers, in particular distributed servers, to enhance the confidentiality of information and its complex protection.

The scientific novelty is that a method based on elements of existing methods was first developed, as well as a proposed method for distributed database servers based on blockchain technology.

Key words: SQL-injection, MS SQL, mySQL, privacy, authorization, blockchain.

Вступ

Актуальність дослідження. Станом на 2019 рік діяльність організацій все більше залежать від комп'ютерних технологій, а відповідно і проблеми захисту інформації стають актуальними. Будь-який збій в системі роботи баз даних призводить до значних матеріальних втрат у кожній організації. Захист даних є однією з найактуальніших проблем у сфері сучасних комп'ютерних технологій.

Щоб забезпечити захист даних в мережах баз даних потрібно встановити певні правила, що можуть забезпечити комплексний захист. Бази даних - це основа для будь-якої комп'ютерної системи, що створює можливість для веб-ресурсів використовувати динамічний контент.

Основною проблемою для системних адміністраторів є забезпечення безпеки баз даних. Є ряд варіантів його вирішення: резервного копіювання, ускладнення паролів, створення ієрархії прав користувачів.

Метою магістерської роботи (проекту) є дослідження існуючих та нових методів захисту баз даних для створення єдиної методики для всестороннього захисту.

Завдання дослідження. Для досягнення зазначеної мети магістерської роботи поставлені такі завдання:

– дослідити вразливості баз даних MS SQL і mySQL на рівні баз;

– дослідити вразливості баз даних MS SQL і mySQL на рівні web-додатку;

– дослідити методи та практики захисту інформації на рівні баз даних;

– дослідити методи та практики захисту інформації на рівні web-додатку;

– на основі встановлених вразливостей та вимог сформувати комплексні методики захисту інформації в базах даних mySQL і MS SQL;

Об'єктом дослідження магістерської роботи є ефективна і безперебійна робота баз даних.

Предметом дослідження є методики захисту баз даних від будь-яких кібератак.

Методи дослідження. У роботі використано методи порівняння, дедукції, системного підходу, аналізу і синтезу;

При формуванні методики захисту конфіденційності інформації від SQL-ін'єкцій був використаний метод синтезу.

При наданні оцінки іншим методам та тестування експлуатації окремих методик було використано метод індукції, що передбачає перехід від конкретних до загальних принципів.

В економічному розділі обраховано вартість даної методи та строки її окупності.

Наукова новизна роботи. Полягає в тому, що вперше розроблено комплексний метод захисту конфіденційної інформації в базах даних на основі елементів існуючих методів, а також запропонований інноваційний метод для розподілених серверів баз даних на основі технології блокчейн.

Розділ 1. Принципи захисту інформації в базах даних та її основні загрози

Зі стрімкими темпами розвитку інформаційних технологій, збільшенням кількості загроз інформації, складності визначення ступенів їх виникнення і реалізації, а також із розвитком комплексних систем захисту інформації спеціалізованої спрямованості, завдання побудови системи принципів захисту інформації в базах даних та протидії її основним загрозам набуває актуальності.

1.1 Принципи захисту інформації

Під **захистом інформації** розуміють комплекс дій, направлених на виключення чи викрадення важливої інформації. Завдання захисту інформації полягає в підтриманні цілісності, доступності і конфіденційності інформації.

Захист інформації вимагає правову, організаційну і технічну базу виключити неправомірний доступ, зберігання конфіденційності і реалізацію права на доступ.

Існують три основні принципи захисту інформації у будь-якій організації. Порушення будь-якого з цих принципів свідчить про викрадення інформації.

1. **Конфіденційність.** Лице, знаюче певну конкретною інформацією, не має права передавати її третім особам без згоди правовласника цієї інформації. Варто відзначити, що конфіденційність інформації не є її властивістю.

2. **Цілісність.** Забороняються будь-які неправові зміни, як випадкові, так і вчинені з певним наміром.

3. **Достовірність.** Гарант, що інформація повинна бути отриманою з надійного джерела.

1.1.1 Основні потреби в захисті інформації

Для реалізації принципів інформації, система повинна відповідати певним вимогам:

1. **Централізованість.** Процес управління інформації завжди є централізованим, а система, яка потрібна для її реалізації, повинна підходити під структуру об'єкта, який відповідає за цю інформацію.
2. **Плановість.** Система захисту інформації повинна базуватись на взаємодії всіх підрозділів, направлених на реалізацію ухваленої політики безпеки.
3. **Конкретика і цілеспрямованість**. Під захист підпадають конкретні інформаційні ресурси, які потенційно можуть зацікавити конкурентів та зловмисників.
4. **Активність.** Важливими є засоби прогнозування, експертні системи та інші інструменти, спрямовані на реалізацію принципів "знайти і знешкодити".
5. **Надійність і універсальність**. Система захисту інформації повинна застосовувати відповідні методи і засоби для завчасного запобігання викраденню інформації.
6. **Економічний ефект.** Ресурси для захисту інформації не повинні перевищували розмір можливого збитку.

1.1.2 Рівні захисту інформації

Для належних результатів, необхідний комплексний підхід, щоб виконувати плани законодавства, адміністрації, здійснювати процедури та забезпечувати програмно-технічні характеристики. Відповідно існують три рівні організації захисту інформації на будь-якому заході, а саме:

- рівень, який стосується робочого місця користувача,
- рівень підрозділу
- рівень, який відноситься до всього підприємства.

Кожний наступний рівень захисту інформації у порядку його зростання вимагає складні механізми.

1.1.3 Закон про захист інформації

Закон “Про захист інформації в автоматизованих системах” від 1994 року спрямований на регулювання правових відносин по захисту інформації на рівні держави. У цьому законі також передбачені права власності людей на інформацію. Правовий захист інформації на законодавчому рівні поділяється на дві групи:

1. Методи, які допомагають організувати і підтримувати негативну реакцію стосовно порушення закону про захист інформації як на рівні компанії, так і у суспільстві загалом
2. Методи, які допомагають направляти і координувати заходи, спрямовані на збільшення обізнаності суспільства у сфері інформаційної безпеки.

1.1.4 Заходи захисту інформації

Існують чотири групи способів зберігання інформації:

1. **Технічні.** Апаратні методи захисту інформації, які закривають доступ до даних. Наприклад, за допомогою маскування, генератори шуму і мережеві екрани. Переваги цього способу: надійність, незалежність від суб’єктивних фактів і збільшену стійкості до модифікацій. Недоліками цього способу є: недостатня гнучкість, великий об’єм і маса цих пристроїв, а також їх висока вартість.
2. **Програмні**. Програми, які використовують для ідентифікації користувачів, а також контролю доступу до інформації і її шифрування. Перевагами є: універсальність, гнучкість, надійність, простота встановлення і можливість їх модифікації і розвитку. Недоліками є: обмежений функціонал, підвищена чутливість до змін, потенційна залежність від типу ПК.
3. **Змішані.** Апаратно-програмні методи, які володіють тими ж функціями, що програмні і технічні, але також включають проміжні варіанти.
4. **Організаційні.** Організаційно-технічні і організаційно-правові засоби. Перевагами є: вирішення різних проблем, їх легша

реалізація, а також швидкість реагування на небезпеку. Недоліками є: відносно висока залежність від впливу суб’єктивних факторів.

1.1.5. Захист інформації в інтернеті

Об’єктами атак зловмисників і хакерів є не тільки державні установи, банки і веб-сайти, а також і персональні інформація фізичних та юридичних осіб. Тому важливо захищати інформацію, яка знаходиться на будь-якому комп’ютері. Існує чотири основні способи захисту інформації в інтернеті:

1. **Надійні паролі**. Фахівці рекомендують використовувати комбінації з великих і маленьких латинських літер, цифр і символів. Вони повинні легко запам'ятовуватися, але не нести смислового навантаження.
2. **Шифрування даних**. У корпоративній і професійній версії Windows є інструмент BitLocker, механізм для шифрування даних на одному або декількох розділах жорсткого диска. Також для безпеки окремих файлів можна використовувати зашифровані архіви.
3. **Антивірусні програми**. Зломисники для отримання інформації застосовують допоміжне програмне забезпечення. Віруси перехоплюють дані під час їх руху, а тому потрібний антивірусний захист із обов’язково актуальною версією.
4. **Налаштування паролів на BIOS.** За допомогою цієї системи захисту унеможливлюється завантаження ПК із вбудованого чи зовнішнього носія інформації. Такі паролі варто встановлювати на жорсткий диск, до якого зловмисник не матиме доступу в руках зловмисника.

1.1.6 Захист інформації на підприємстві

Щоб забезпечити комплексний захист інформації, необхідно здійснити декілька етапів підготовки: проаналізувати і вибрати політику безпеки, впровадити відповідні засоби, розробити і застосувати організаційні заходи. Етапами підготовки системи захисту інформації на підприємстві є:

1. Підготовка нормативно-правових документів.
2. Визначення потенційних загроз і оцінка потенційних збитків по відношенню до кожної із загроз.
3. Створення спеціального підрозділу з безпеки для: захисту даних, запобігання несанкціонованому проникненню забезпечення цілісності інформації.
4. Безпосередній захист інформації. Цей етап передбачає застосування таких методів як: електронний підпис, криптографічний метод шифрування, паролі, система аудиту та протоколювання, а також електронні ключі.

1.1.7 Захист персональних даних

До персональної інформації відносять паспортні дані, паролі доступу до різних сервісів і електронних гаманців, номер телефону та інші дані, за допомогою яких можна отримати іншу важливу інформацію. В інтернеті людина сама вирішує надавати свої дані чи ні. Захист конфіденційної інформації проводиться з урахуванням таких порад:

1. Не завантажуйте і не активуйте е програми, які є сумнівними.
2. Не записуйте важливу інформацію в легкодоступних місцях.
3. Не записуйте паролі у документи без захисту.
4. Не ігноруйте попередження в браузері про проблеми з сертифікатами та реєстрацією сайту.
5. Під час роботи на чужих комп’ютерах не зберігайте свої паролі і завжди виходьте із акаунтів на інших веб-сайтів.
6. Використовуйте антивірусні програми і перевіряйте усі завантажені файли.

1.1.8 Захист носіїв інформації

Для захисту носії інформації використовують три групи методів: програмні, апаратні та комбіновані. Важливо розуміти, що абсолютно надійного захисту як інформації, так і її носіїв не існує. Принципами найпопулярніших методів захисту носіїв інформації є:

1. Для всіх знімних носіїв використовувати фізичний захист. Наприклад, закриття у сейфі.
2. Програмне закриття доступу до певного носія або повністю до всього ПК. Наприклад, пароль CMOS.
3. Використання програмно-апаратного методу із застосуванням електронних ключів, які часто вставляю у COM-порт ПК. Якщо прилад не отримує правильну відповідь, то программа не запускається.

Отже, основними принципами захисту інформації є її конфіденційність, цілісність і достовірність. Захист інформації потребує централізованості, плановості, конкретики і цілеспрямованості, активності, надійності і універсальності, а також мати економічний ефект. Захист інформації існує на рівні робочого місця користувача, на рівні підрозділу і всього підприємства. Є чотири групи захисту інформації: технічні, програмні, змішані і організаційні. Найбільш вразливою є інформація в інтернеті, а тому рекомендується використовувати надійні паролі, шифрування даних, антивірусні програми, а також налаштовувати паролі на BIOS для її ефективного захисту.

1.2 Основні загрози безпеці інформації в базах даних

1.2.1 Поняття кіберзагрози

Стрімка інформатизація суспільства позитивно впливає на різні сфери економіки: фінанси, торгівлю, промисловість, охорону здоров'я, освіту, науку та інші. Сьогодні інформаційні технології – це невід'ємна частина не тільки успішного бізнесу, але і державної політики. Однак

зловмисники навчилися використовувати інформаційні технології у своїх неправомірних цілях, що дало початок протистоянню з фахівцями з інформаційної безпеки. Ця боротьба сприяє постійному вдосконаленню методів та інструментів, які використовують зловмисники, що у свою чергу неминуче породжує зростання числа кіберзагроз.

Кіберзагрози – це сукупність факторів та умов, що створюють небезпеку порушення інформаційної безпеки. У цьому дослідженні кіберзагроза розглядається з точки зору дій зловмисників у кіберпросторі, спрямованих на проникнення в інформаційну систему з метою крадіжки чи вилучення даних, коштів або з іншими намірами, які потенційно ведуть до негативних наслідків для держави, бізнесу або приватних осіб. Дії зловмисників можуть бути спрямовані як на IT-структуру компанії, робочі комп'ютери, мобільні пристрої, так і на інші технічні засоби, а також особисто і на саму людину як на елемент кіберпростору.

1.2.2 Тренди і прогнози розвитку кіберзагроз

Компанія Positive Technologies стежить за актуальними загрозами інформаційній безпеці. Кіберзлочинці швидко реагують на звістки про нові вразливості, адаптуються до змін і продовжують удосконалювати методи своїх атак.

За підсумками II кварталу 2019 року, Positive Technologies відзначають такі тенденції:

- Кількість унікальних кібер-інцидентів залишається високою і на 3% перевищує показник I кварталу.
- Цілеспрямовані атаки переважають над масовими, їх частка склала 59%, що на 12% більше, ніж у I кварталі.
- Абсолютна більшість усіх кіберзлочинів відбуваються з метою викрадення інформації. Пряма фінансова вигода цікавить зловмисників в 42% атак проти приватних осіб і в 30% атак проти юридичних осіб.
- Персональні дані є основним типом викраденої інформації в атаках на юридичні особи (29%). Приватні особи найчастіше ризикують

обліковими записами та даними своїх банківських карт (44% і 34% відповідно від усього обсягу інформації, вкраденої у приватних осіб).

- Кількість атаки MageCart на онлайн-ресурси зростає. Фахівці відзначають шкідливі JavaScript-сніфери, у тому числі і на сайтах без функції оплати.
- Зростає частка заражень шкідливим ПЗ серед державних установ (62% у порівнянні щ 44% у I кварталі 2019 року). Державні установи найчастіше піддаються атакам троянів-шифрувальників.
- Угруповання RTM продовжує активно атакувати промисловий сектор як одну з слабо захищених галузей. З фінансовою мотивацією група RTM продовжує здійснювати спроби атак на фінансові організації.
- IT-компанії стають проміжною ланкою в атаках на організації з управління ланцюгом поставок (supply chain). Кібер-зловмисники використовують поштові адреси зламаних постачальників IT-послуг для фішингових розсилок.

1.2.3 Статистика кіберзагроз в Україні у II кварталі 2019 року

Викрадення інформації залишається пріоритетною завдання абсолютної більшості кібератак. Фінансову вигоду зловмисники переслідують в 30% і 42% атак на юридичні особи та приватних осіб відповідно. Висока частка фінансово мотивованих атак на приватних осіб пояснюється регулярними масовими ураженнями шкідливим ПЗ з нав'язливою рекламою, у тому числі на мобільних пристроях, зараженням майнерами та іншими вірусними програмними забезпеченнями на сумнівних сайтах, а також кампаніями, які вимагають гроші, у ході яких зловмисники загрожують поширити компрометуючу персональну інформацію.

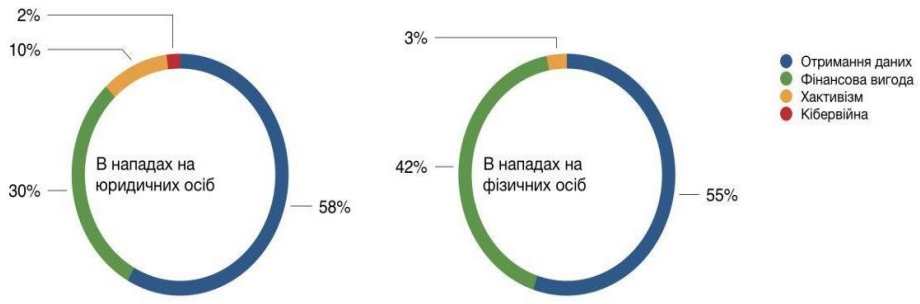


Рисунок 1.2.3.1 Мотиви кіберзловмисників

Персональні та облікові дані найчастіше цікавлять зловмисників при атаці на юридичних осіб. Це пояснюється тим, що компаніях зберігаються великі бази як персональних, так і облікових даних клієнтів. Крім того, зловмисники можуть бути зацікавлені в облікових даних співробітників компанії-жертви.

Під загрозою перебувають і облікові записи у соціальних мережах, особливо якщо персональний аккаунт популярний, тобто має велике число послідовників. Користувачі, у свою чергу, нехтують безпекою особистих акаунтів: використовують нестійкі і однакові паролі, вводять облікові дані, не впевнившись у надійності ресурсу, публікують інформацію про себе, яка може допомогти підібрати пароль. Це пояснює високу частку викрадених облікових даних (44%) в атаках на приватних осіб.

Наприклад, до категорії людей, що входять в зону підвищеного ризику атак з боку хакерів, відносять любителі комп'ютерних ігор. У II кварталі зловмисники заманювали користувачів Steam на веб-ресурси, де наче безкоштовно можна отримати нову гру, ввівши облікові дані від аккаунта в Steam. Крім того, попастися на приманку зловмисників геймери можуть і на спеціалізованих форумах. Таким чином під виглядом

чит-кодів, упакованих в ZIP-архів, багато веб-ресурсів поширювали вірус троян для майнингу криптовалюти TurtleCoin.

Дані банківських карт і платіжна інформація клієнтів, як правило, захищені криптографічними методами, тому зловмисникам простіше дізнатися їх за допомогою методів соціальної інженерії безпосередньо у клієнта. Як наслідок, 34% вкрадених в результаті атак на приватних осіб даних – це дані їх банківських карт.

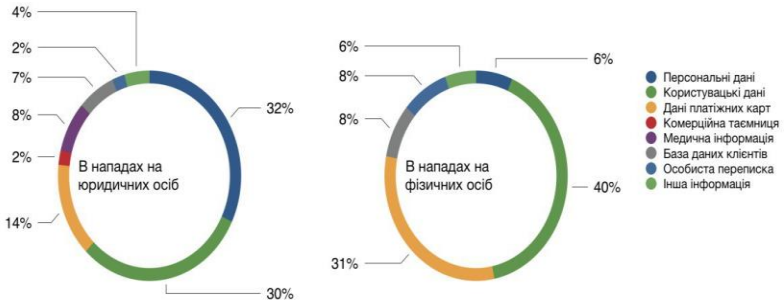


Рисунок 1.2.3.2 Типи вкрадених даних

У II кварталі 2019 року частка цілеспрямованих атак зросла у порівнянні з I кварталом і становила 59% (у I кварталі – 47%). Частка кібер-інцидентів, в результаті яких постраждали приватні особи, становила 24%. Серед юридичних осіб (див. Малюнок 3) зловмисники найчастіше атакують державні організації, промислові компанії, медичні організації, банки та інші організації фінансової сфери. У II кварталі відзначають атаки на організації з управління ланцюгами поставок (supply chain) на великі IT-компанії з клієнтами з різних галузей економіки.

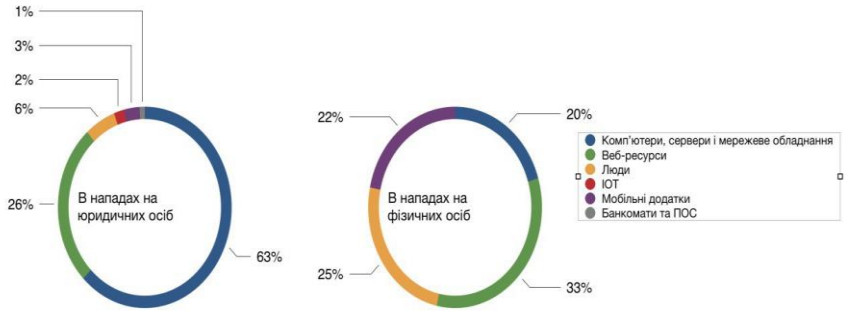


Рисунок 1.2.3.3 Об'єкти атак

1.2.2 Види загроз інформаційній безпеці

Серед найпоширеніших загроз інформаційній безпеці є: використання шкідливого ПЗ, соціальна інженерія, хакінг, експлуатація веб-вразливостей, відбір облікових даних (Брут). У цьому підрозділі роглядемо детальніше кожний вид загроз інформаційній безпеці із статистичними даними за I і II квартали у 2019 році.

1.2.2.1 Використання шкідливого ПЗ

Частка багатофункціональних троянів на фоні усіх інших видів кіберзагроз зростає. Наприклад, модульний троян DanaBot, про який писали у I кварталі, тепер здатний виконувати роль шифрувальника. Активність одного з найпоширеніших шифрувальників GandCrab, навпаки, почала спадати, і його оператори заявили про завершення шкідливої кампанії. Через декілька тижнів після новини про припинення розвитку трояна-”здирника” фахівці з кібербезпеки отримали доступ до серверів GandCrab, а разом з ним і ключі шифрування, завдяки чому була створена програма-дешифрувальник для останньої версії GandCrab, що дозволяє відновлювати зашифровані ними файли.

Незважаючи на ці події, частка атак троянів-вимагачів залишається високою. Це пояснюється тим, що для створення простого шифрувальника не потрібно розробляти унікальний код. Більшість нових

екземплярів вимагачів дуже схожі на своїх попередників, оскільки часто кіберзлочинці не розробляють шифрувальник з нуля, а отримують готовий код або підписку (ransomware as a service) у даркнеті. Таким чином, при мінімальному стартовому капіталі шифрувальники можуть приносити власникам високий дохід.

З квітня 2019 років періодично з'являються повідомлення про атаки нового крипто-вимагача Sodinokibi, від якого постраждали три провайдера IT-послуг. Кіберзлочинці використовували інструменти віддаленого адміністрування (Webroot і Kaseya) для зараження шифрувальником компаній-клієнтів скомпрометованих постачальників IT-послуг. Однак атаки у сфері управління ланцюгом поставок (supply chain) не є єдиним вектором поширення Sodinokibi. Троян поширюється також через уразливості в MS SQL WebLogic Server і фішингові листи.

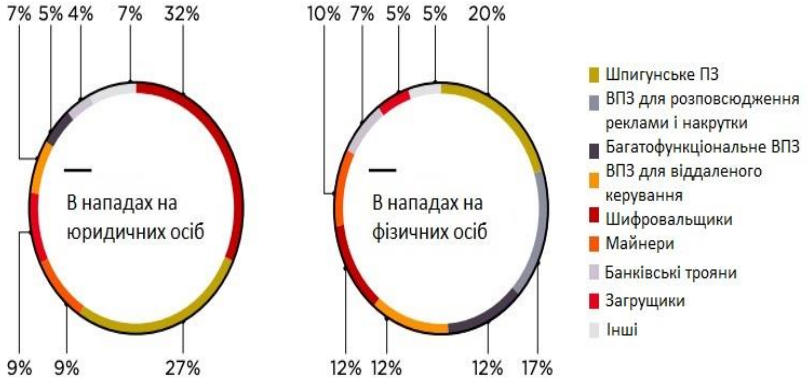


Рисунок 1.2.2.1.1 Типи шкідливого ПО

Найбільш популярним способом доставки шкідливого ПЗ залишається **електронна пошта**. У II кварталі фахівці відзначають, що частішими стали випадки поширення троянів за допомогою файлів у форматі ISO (цифрових образів компакт-дисків). Наприклад, так поширюються AgentTesla, LokiBot, NanoCore. ISO-образи часто не виявляються антивірусними рішеннями, оскільки можуть бути включені у білі списки. Однак проблему можна запідозрити за розміром файлу,

оскільки шкідливе вкладення має розмір не більше 2 МБ, у той час як легітимний ISO-образ, як правило, більший ніж 2 МБ.

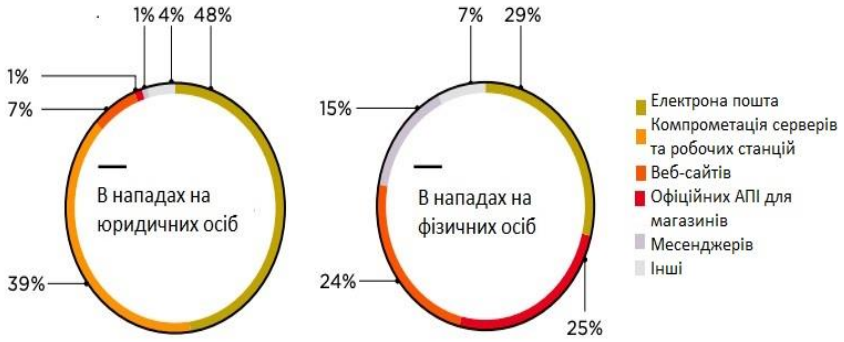


Рисунок 9. Способи поширення ШПЗ

У другому кварталі 2019 роки відзначають повернення інтересу зловмисників до криптоджекінгу. Курс біткойнів впевнено зростає, і зловмисники продовжують розвивати ПЗ для прихованого майнінгу. Таким чином, фахівці Sucuri виявили зразок Майнера з поліпшеними механізмами для закріплення в інфраструктурі: спеціальний cron-скрипт (сценарій для виконання певних дій за розкладом) дозволяє відновити процес майнингу навіть в разі, якщо основний модуль ВПЗ був виявлений і вилучений із зараженої системи.

У II кварталі зловмисники активно поширювали інфостилер AZORult. Наприклад, у квітні експерти Positive Technologies Expert Security Center (PT ESC) відзначали, що угруповання RTM стала використовувати AZORult замість Pony. Крім того, троян AZORult поширюється через веб-сайти під виглядом різних утиліт (наприклад, під виглядом утиліти для очищення і оптимізації роботи ОС G-Cleaner або VPN-клієнта Pirate Chick).

1.2.2.2 Соціальна інженерія

У II кварталі кіберзлочинці активно використовували набір сервісів Azure App Service для різного роду шахрайства із застосуванням методів соціальної інженерії. Наприклад, сервіс Azure задіюється для швидкого розгортання фішингових сторінок з підробленими формами аутентифікації і для створення підроблених сторінок служби технічної підтримки Microsoft зі спливаючими повідомленнями про те, що комп'ютер користувача сайту нібито заражений вірусом.

Крім того, зловмисники розсилають листи, в яких пропонують завантажити файл, авторизувавшись через підроблену форму, попередньо розміщену на платформі Azure Blob Storage. Масштабом і успіху подібного роду шахрайських операцій сприяє домен windows.net в адресному рядку і діючий SSL-сертифікат Microsoft. Однак схема крадіжки облікових даних не є новою, і існують спеціальні інструкції для користувачів, які допомагають налаштувати автоматичне блокування подібних фішингових листів.

Як уже зазначалося, стрімке зростання курсу біткойнів в II кварталі 2019 років призвів до зростання інтересу до криптовалюта, з чого зловмисники намагаються отримати вигоду. Наприклад, кіберзлочинці використовують поширену схему, коли нібито від імені відомих людей або організацій оголошують грошові призи з єдиною умовою: для отримання винагороди необхідно зробити попередній грошовий переказ під приводом верифікації адреси одержувача нагороди. Наприклад, «призи» у криптовалюті були оголошені нібито від імені Джона Макафі та Ілона Маска.

У зв’язку з популярністю платформи YouTube, відеоканали стають привабливим майданчиком для розміщення шкідливих посилань. У ході однієї з таких шахрайських компаній глядачам пропонувалися до перегляду відеоролики, що нібито навчають роботі з безкоштовним генератором біткойнів, посилання на який розміщували в описі під відео. Насправді ж клік по посиланню ініціював завантаження

інфостилера Qulab. У результаті іншої аналогічної кампанії через YouTube поширювалося ШПЗ для віддаленого управління njRAT.

1.2.2.3 Хакінг

У II кварталі 2019 року кібер-зловмисники націлені на експлуатацію: CVE-2017-11882; CVE-2019-0708; CVE-2019-0604; CVE-2019-2725; CVE-2019-10149; CVE-2019-3396. Хакери активно експлуатують вразливість у поштовому сервері Exim (CVE-2019-10149), яка дозволяє віддалено виконувати команди операційної системи (ОС) з правами адміністратора. Одне з хакерських угруповань використовує цю вразливість для впровадження бекдор, завантажуючи на поштові сервери shell-скрипти і додаючи SSH-ключ до облікового запису root.

Крім того, зловмисники незаконно завантажують на вразливі сервери ПЗ для майнингу криптовалюті. Вразливість була усунена розробниками Exim у лютому 2019 року. Однак випуск поновлення ПЗ виробником не завжди нейтралізує загрозу, і через несвоєчасне оновлення ПЗ хакери успішно експлуатують вразливості навіть п'ятирічної давності.

Найбільш обговорення набула проблема безпеки у II кварталі з критично небезпечною RCE-вразливістю BlueKeep (CVE-2019-0708) у використанні RDS деяких старих версій Windows. Незважаючи на те, що 14 травня 2019 року компанія Microsoft випустила патч, більшість комп'ютерів по всьому світу залишаються під загрозою, в той час як зловмисники продовжують активно шукати вразливі вузли і розробляти експлойти.

Поширення шкідливого ПЗ за допомогою експлуатації BlueKeep може досягти масштабу WannaCry, тому настійно рекомендується встановлювати оновлення ПЗ.

Протягом II кварталу зловмисники шукали публічно доступні Docker API, скануючи інтернет у пошуках вузлів з відкритим портом 2375. Невірно сконфігуровані контейнери Docker використовуються у різних цілях. Наприклад, виявивши працює контейнер, хакери

встановлюють в нього троян Dofloo . Цей троян зловмисники доставляють на вузли зі встановленим ПЗ Atlassian Confluence, експлуатуючи вразливість CVE-2019-3396. Зловмисники Dofloo використовують обчислювальні потужності жертв для DDoS-атак і прихованого майнингу криптовалюти.

1.2.2.4 Експлуатація веб-вразливостей

У II кварталі 2019 року зловмисники експлуатували веб-вразливості у 18% атак на юридичні особи. Хвиля атак на веб-ресурси з можливістю онлайн-платежів, що розпочалася у I кварталі, набирає обертів. Таким чином, атакам з використанням JavaScript-сніфферів MageCart (шкідливих скриптів, спрямованих на крадіжку даних платіжних карт) цього разу атакували Forbes, Puma і деякі інтернет-магазини. Кіберзлочинці, що стоять за атаками MageCart, регулярно оновлюють шкідливі скрипти.

Небезпека JavaScript-сніфферів полягає в тому, що відвідувачі заражених сайтів не можуть розпізнати загрозу, оскільки дія шкідливих скриптів непомітна для користувачів. Однак один з нових способів крадіжки даних MageCart містить ознаки, за якими можна розпізнати загрозу. Зловмисники впроваджують форму для введення даних карти на веб-сторінках сайтів, у той час як цей інтерфейс повинен бути доступний тільки після перенаправлення на захищену сторінку провайдера платіжних систем. Необхідність двічі вводити реквізити карти (безпосередньо на сайті і на сторінці платіжного провайдера) повинна насторожити онлайн-покупців.

У другому кварталі фахівці Malwarebytes Labs виявили JavaScript-сніфери MageCart в бібліотеках, які розробники сайтів розміщували у закритих репозиторіях CDN на базі Amazon CloudFront. Крім того, з початку квітня зловмисники впроваджують JavaScript-сніфери MageCart в файли, що зберігаються в Amazon S3, що вже призвело до компрометації 17 тис. сайтів. Не всі скомпрометовані ресурси містять форму для введення платіжної інформації, з чого експерти роблять висновок, що

хакери впроваджують JavaScript-сніфери в ході масових атак в техніці spray and pray.

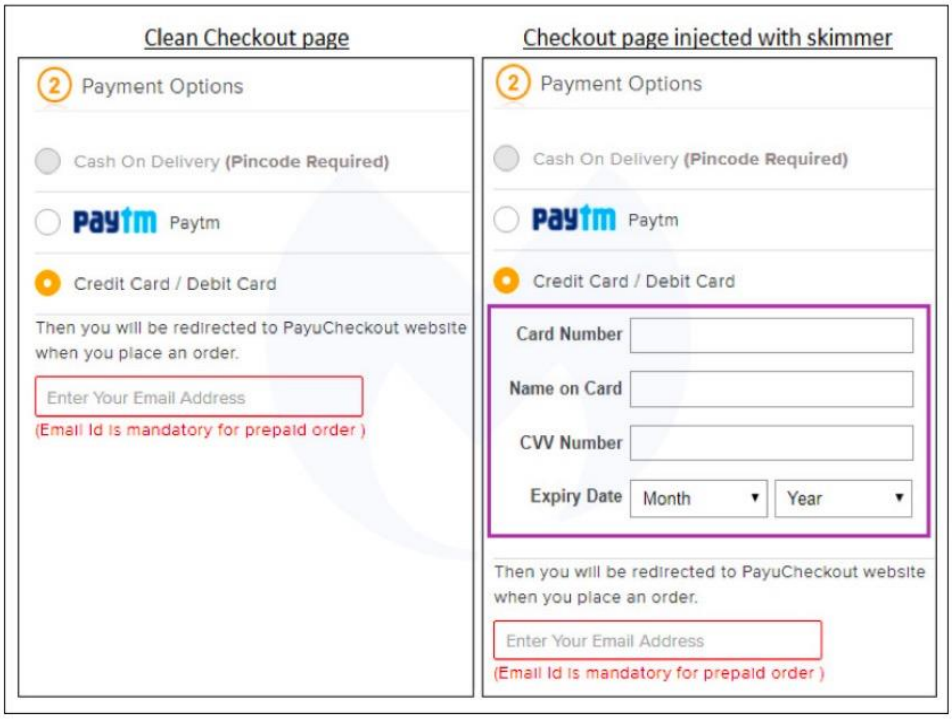


Рисунок 11. Форма MageCart для крадіжки даних платіжних карт

Очевидно, що зловмисників приваблюють не тільки ті сайти, на яких є можливість здійснювати онлайн-платежі. У червні був взламаний форум Social Engineered, розроблений на базі ПЗ MyBB. Хакери скористалися XSS-вразливістю в MyBB, про котру стало відомо за декілька днів до інциденту. У результаті атаки в руки хакерів потрапили 55 тисяч облікових записів користувачів форуму і їх особисті повідомлення.

1.2.2.5 Підбір облікових даних

Слабкі паролі залишаються однією з основних проблем безпеки. Паролі 300 співробітників агентства Information Network Security Agency в Ефіопії, основною метою якого є забезпечення безпеки інформації, мали слабку стійкість, через що потрапили у руки

зловмисників і опинилися у відкритому доступі. 142 паролі з 300 були поєднанням символів p @ $$ w0rd, а ще 60 – поєднання цифр 123.

Як і раніше актуальні атаки типу credential stuffing (спроби доступу до системи з використанням вкраденої бази облікових даних). У II кварталі від цих атак постраждали близько півмільйона користувачів двох інтернет-магазинів – бренди Uniqlo і GU.

Протягом II кварталу фахівці фіксують атаки нового ботнету GoldBrute, спрямовані на підбір паролів для доступу по RDP. Атакам піддалися вже більше 1,5 млн пристроїв під управлінням Windows. Цілі зловмисників поки невідомі, але з великою ймовірністю вони планують продавати викрадені облікові записи в дарквебі. Нерідко подібних масових атак, спрямованих на підбір облікових даних, піддаються і IoT-пристрої. У червні стало відомо про шкідливі програми Silex, які націлені на підбір стандартних паролів на пристроях IoT. Після успішного підбору паролів Silex виводить пристрої з ладу. Станом на 2019 рік налічується понад дві тисячі пристроїв, які постраждали від деструктивного впливу Silex.

1.2.3 Категорії жертв кіберзагроз

У цьому пункті ми розглянемо категорії жертв, які підпадають під кібератаки та приклади таких атак у різних сферах економічного і суспільного життя. Є п’ять основних категорії жертв кіберзагроз: державні організації, промислові компанії, медичні заклади, фінансові організації та IT-компанії.

1.2.3.1 Державні організації

У II кварталі 2019 роки спостерігається значне зростання частки заражень шкідливим ПХ серед державних організацій (62% у порівнянні з 44% в I кварталі).

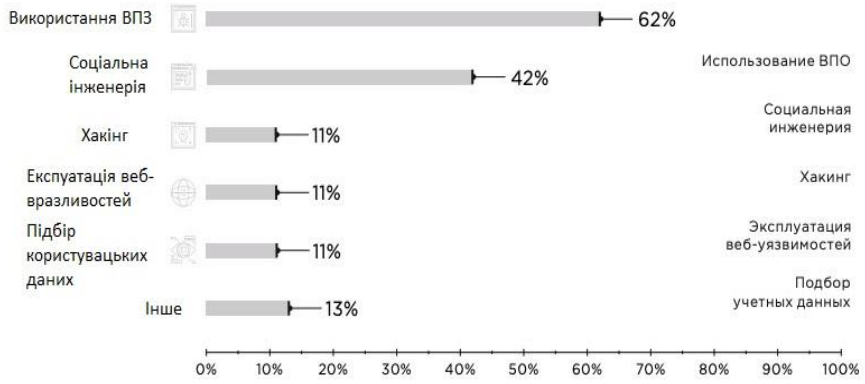


Рисунок 1.2.3.1.1 Методи атак на державні організації в Q2 2019

Найчастіше державні установи піддаються атакам шифрувальників. На початку травня уся IT-інфраструктура міста Балтимор (США) була заблокована на декілька тижнів через атаки шифрувальника RobinHood. Влада міста оцінили збиток від атаки більш ніж в 18 млн дол. США. Балтимор став не першою жертвою трояна RobinHood: у квітні шифрувальником були заражені інформаційні системи міста Грінвілл (США).

Порушення працездатності інформаційних систем змушує адміністрації постраждалих населених пунктів йти на угоду з вимагачами і платити викуп. Ця проблема особливо актуальна у невеликих містах із слабо розвиненою IT-інфраструктурою. Так, в уряді міста Рів'єра-Біч в штаті Флорида одноголосно прийняли рішення заплатити викуп в 65 біткойнів (600 тис. Дол. США), оскільки у IT-фахівців не виявилося резервних копій, необхідних для відновлення уражених систем.

На початку червня атаці трояна-шифрувальника підпало і інше місто Флориди, Лейк-Сіті. Міські інформаційні системи були заражені у ході масштабної шкідливої кампанії Triple Threat, про яку у квітні вперше розповіли фахівці Cybereason. Кампанія отримала назву через потрійне «корисну навантаження»: за допомогою фішингових листів на комп'ютери жертв доставляються три трояна: Emotet, TrickBot і Ryuk. Незважаючи на те що заражені пристрої були максимально швидко

відключені від мережі міста, зараженими виявилися більшість телефонних і поштових систем. Уряд також ухвалив рішення заплатити викуп вимагачам у розмірі 42 біткойнов (530 тис. Дол. США), після чого звільнили IT-директора з його посади.

Однак на цьому атаки троянів-вимагачів на населені пункти Флориди не закінчилися, і в кінці червня 2019 року черговою жертвою став Кі-Біскейн. Однак цього разу влада міста відмовилися платити викуп.

У Росії також були зафіксовані атаки троянів-шифрувальників. На Південному Уралі у II кварталі зафіксовані спроби заражень, і в Увельський районі Челябінської області вони виявилися успішними.

Великі фінансові втрати державні установи можуть понести і в результаті фішингової атаки. У результаті однієї з таких атак чиновники канадського міста Берлінгтон перевели на рахунок зловмисників 503 тис. дол США.

Крім того, тривають атаки на урядові веб-ресурси. Хакери зламали три веб-сайту Національної академії ФБР і виклали у відкритий доступ персональні дані чотирьох тисяч федеральних агентів і співробітників правоохоронних органів.

1.2.3.2 Промислові компанії

Майже усі атаки на промислові підприємства (96%) у II кварталі 2019 року відбувалися з використанням шкідливого ПЗ. Активні спроби проникнення у внутрішню IT-інфраструктуру промислових компаній робить угруповання RTM. Протягом другого кварталу фахівці PT ESC зафіксували 26 шкідливих емейл-розсилок цієї групи. У списку адресатів, крім фінансових установ, більше десятка промислових організацій в Росії і СНД. Усі електронні листи складені російською мовою і мають схожу тематику: як правило, вони містять нібито фінансові документи (акти, рахунки та ін.) З проханнями перевірити, підписати документи або здійснити оплату.

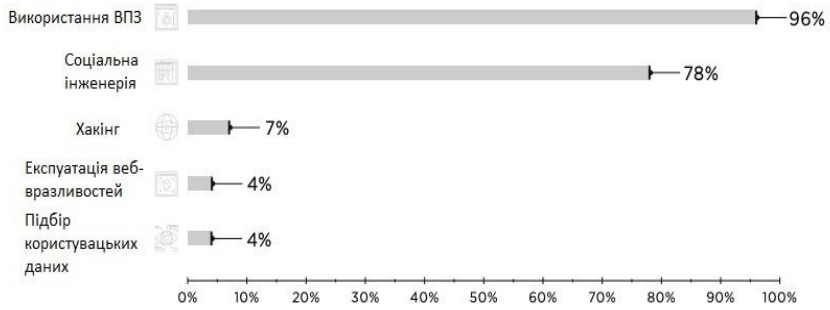


Рисунок 1.2.3.2.1. Методи атак на промислові компанії в Q2 2019

Троян RTM відноситься до категорії шпигунських: він викрадає облікові записи, записує відео, робить знімки екрану і передає їх на сервер зловмисників. У червні група змінила спосіб отримання IP-адреси контрольного сервера. Тепер адреса виходить за допомогою логічних операцій (AND і циклічний зсув вправо) над сумою транзакції, отриманої на певний гаманець Bitcoin.

У II кварталі фахівці PT ESC зафіксували атаки групи TaskMasters, спрямовані на промислові підприємства Росії. Цікаво, що в цих атаках група використовувала VMProtect для захисту трояна від детектування антивірусним ПЗ. Після публікації дослідження про групу TaskMasters, а також доповіді на конференції PHDays 9, присвяченого діяльності групи, зловмисники перевели більшість доменів на IP-адреси 127.0.0.1, запобігаючи тим самим передачу трафіку за межі комп'ютера жертви. Це свідчить про те, що група знає про її виявлення і, ймовірно, припинила свої дії.

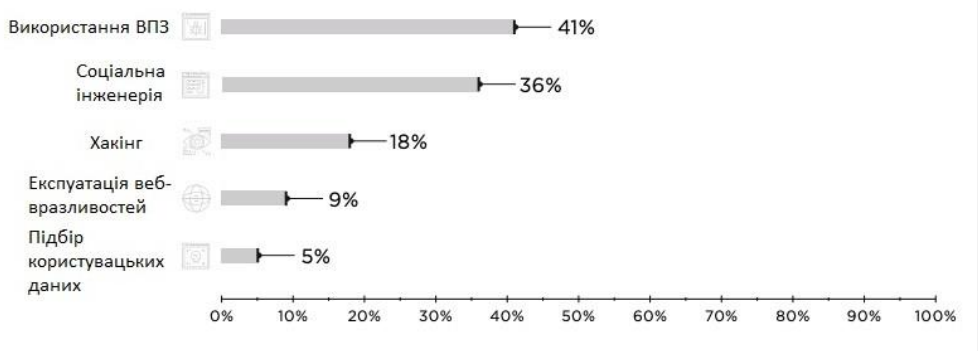
Тривають атаки на промисловість з боку шифрувальників. У II кварталі жертвами троянів-вимагачів стали, наприклад, виробник спецобладнання для утримання аеропортів Aebi Schmidt і один з найбільших виробників запчастин для авіаційної техніки ASCO.

Хакери атакують і веб-ресурси промислових підприємств. Так, зловмисники зламали сайт компанії Uniden для розміщення на ньому трояна Emotet. Сайт нафтогазової компанії Petrobangla був

двічі зламаний протягом доби. Хакер, який атакував сайт Petrobangla, намагався таким чином продемонструвати власникам веб-ресурсу наявні проблеми з безпекою.

1.2.3.3 Медичні заклади

Шкідливе ПЗ, що порушує працездатність систем організації, становить особливу загрозу для закладів охорони здоров'я, де подібного роду інциденти можуть дорого обійтися як для самої компанії, так і її пацієнтів. У квітні 2019 року жертвою атаки шифрувальника стала офтальмологічна клініка JFJ Eyecare, в результаті інциденту зашифрованими виявилися персональні дані пацієнтів.



Малюнок 1.2.3.3.1. Методи атак на медичні установи в Q2 2019

Співробітники медичних організацій нерідко піддаються фішинговим атакам. Працівник організації охорони здоров'я в Новій Шотландії (Канада) отримав лист нібито від співробітника IT-департаменту з проханням ввести дані свого облікового запису, щоб запобігти її блокування. У результаті успішної атаки в руки зловмисників потрапили логін і пароль співробітника, а дані близько трьох тисяч пацієнтів опинилися під загрозою.

Однак зловмисникам зламувати медичні організації з метою отримання відомостей не тільки про пацієнтів, а й про співробітників. Наприклад, за 500 дол. США в дарквебі продавалися

пакети документів лікарів: дипломи про медичну освіту, рекомендації, ліцензії на медичну діяльність.

1.2.3.4 Фінансові організації

У II кварталі фішингові розсилки проводили відразу декілька груп, орієнтованих на фінансову галузь. Угруповання Cobalt продовжує атакувати: протягом II кварталу експерти PT ESC відзначили дві атаки. Під час другої атаки група перейшла від традиційних COM-DLLDropper і JavaScript-бекдор, які використовувалися зловмисниками з кінця минулого року, до використання модифікованого CobInt, який відзначився в їх арсеналі з серпня по листопад 2018 року.

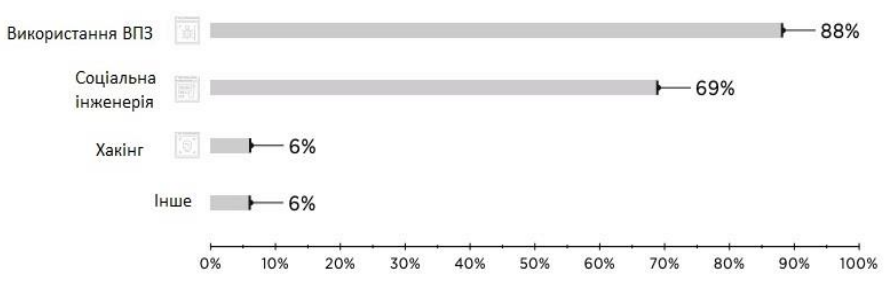


Рисунок 1.2.3.4.1. Методи атак на фінансові організації в Q2 2019

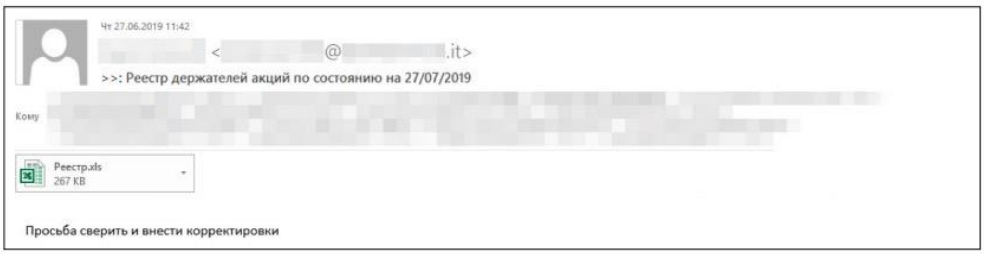


Рисунок 1.2.3.4.2. Фішингових лист угруповання Cobalt

У червні фахівці PT ESC виявили фішингову розсилку угруповання Silence нібито від імені клієнта банку:

Рисунок 1.2.3.4.3. Фішингових лист Silence

У травні спеціалістами PT ESC були виявлені фішингові листи з зашифрованими архівами, в яких знаходився файл у форматі LNK. При запуску цього файлу на комп'ютері жертви завантажується скрипт PowerShell, що збирає системну інформацію і відправляє її зловмисникам. За цією інформацією зловмисники визначали, який вірусний засіб застосувати у скомпроментованій системі. Мережева інфраструктура ідентифікувала цю злочинну групу як FinTeam.

Рисунок 1.2.3.4.4. Фішингових розсилка невідомої групи (ймовірно FinTeam)

Крім того, в II кварталі 2019 року жертвами хакерів стали щонайменше три банки в Бангладеш: Dutch Bangla Bank Limited (DBBL), NCC Bank і Prime Bank. Відомо, що в результаті кібератаки банк DBBL втратив 3 млн. дол. США. За словами представників двох інших банків, вони не понесли фінансових втрат.

1.2.3.5 IT-компанії

У першій половині квітня хакери отримали доступ до інфраструктури компанії Matrix, розробника децентралізованої платформи обміну повідомленнями, скориставшись вразливостями в застарілої версії Jenkins. В результаті вторгнення в руки зловмисників потрапили не зашифровані повідомлення, хеш-кодування паролів користувачів і маркери доступу.

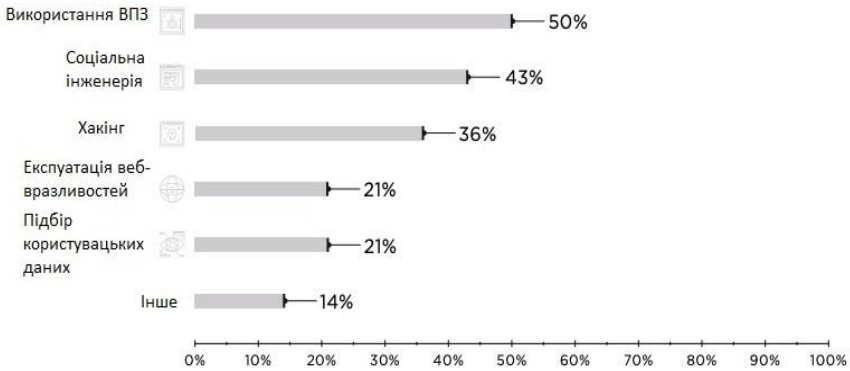


Рисунок 1.2.3.5.1 Методи атак на IT-компанії в Q2 2019

IT-компанії нерідко стають жертвами атак у сфері управління ланцюгами поставок (supply chain). Хакери зламали одного з найбільших індійських постачальників IT-послуг,компанію Wipro, клієнтами якої є організації сфери охорони здоров'я, телекомунікацій та фінансової галузі. У результаті злому інфраструктури Wipro від фішингових атак постраждали не менше десятка компаній-клієнтів, які отримали електронні листи з шкідливими вкладеннями нібито від співробітників Wipro. За думку експертів Flashpoint, які проводили розслідування інциденту, однією з цілей зловмисників стала шахрайська операція з подарунковими картками (gift card fraud).

У середині травня від атаки у сфері управління ланцюгами поставок (supply chain) постраждав і постачальник хмарних рішень PCM. Зловмисники отримали доступ до облікового запису

адміністратора, який використовується в PCM для управління обліковими записами клієнтів в Office 365. Метою зловмисників стала крадіжка інформації для її використання як незаконного отримання подарункових карт.

Висновки до першого розділу

У цьому розділі було проведена така робота, як огляд літератури та збір даних. Аналітика про кібератаки за кінець 2019 року розповідає про необхідність створення методики захисту інформації в базах даних та дотримання стандартів безпечного програмування систем web-додатків інтернет-суспільством.

Отже, основними принципами захисту інформації є її конфіденційність, цілісність і достовірність. Захист інформації потребує централізованості, плановості, конкретики і цілеспрямованості, активності, надійності і універсальності, а також мати економічний ефект. Захист інформації існує на рівні робочого місця користувача, на рівні підрозділу і всього підприємства. Є чотири групи захисту інформації: технічні, програмні, змішані і організаційні. Найбільш вразливою є інформація в інтернеті, а тому рекомендується використовувати надійні паролі, шифрування даних, антивірусні програми, а також налаштовувати паролі на BIOS для її ефективного захисту.

Кіберзагрози –- це сукупність факторів і умов, що створюють небезпеку порушення інформаційної безпеки. Цілеспрямовані атаки переважають над масовими і становлять 59% усіх атак. Більшість з них спрямована на викрадення інформації у фізичних чи юридичних осіб для отримання фінансової вигоди. Серед найпоширеніших загроз інформаційній безпеці варто відзначити використання шкідливого ПЗ, соціальну інженерію, хакінг, експлуатації веб-вразливостей, підбір облікових даних.

Наведені приклади показують гостру актуальність обраної проблеми та які наслідки за собою вона має. Проблема захисту інформації розгалужена та багатогранна.

У наступному розділі будуть розглянуті приклади атак та способи захисту від них.

Розділ 2. Методи кібератак на конфіденційність інформації та її захисту в базах даних

2.1 SQL-ін’єкції як основний метод порушення конфіденційності інформації в базах даних

2.1.1 Причини виникнення SQL-ін’єкції

SQL ін'єкція – це техніка введеня коду, яка використовується для атаки неправильно написані запити і вставляють інші значення для досягнення своїх цілей.

SQL-запити є повноцінною програмою з операторами, змінними і стрічковими літералами. Ця програма збирається динамічно. На відміну від PHP-скриптів, які написані раз і назавжди, і не змінюються на основі даних які отримуються, SQL-запит кожен раз динамічно формується спочатку. Як наслідок, неправильно відформатовані дані можуть деформувати запит або навіть змінити його, підставивши не передбаченні оператори. Цей процес називається ін’єкцією.

Серверна обробка плейсхолдерів. У програму постійно вносяться змінні. Плейсхолдери – це звичайні змінні, які прописані в SQL-запиті і не міняються в залежності від отриманих даних. Самі дані йдуть на сервер окремо від запиту, і ніколи з ними не пересікаються. Тільки після того, як запит буде виконаний, дані будуть використані на етапі виконання.

На практиці це виглядає так: при виклику prepare() на запит йде на сервер в такому вигляді – з плейсхолдерами/змінними, сервер його парсить і дає сигнал. Якщо все в порядку, сервер готовий отримувати дані або повідомляє про помилку. Після цього, при виконанні, на сервер йдуть дані та приймають участь безпосередньо у виконанні.

2.1.2 Атака SQL ін'єкції з метою отримання доступу до баз даних MSSQL

Взлом MS SQL починається з збирання інформації про сервер та пошук безпосередньо серверу SQL. Для цього потрібно прослухати порти 1433 (безпосередньо MS SQL) та 1434 UDP (SQL Browser). Для цього достатньо використати Nmap з скриптом ms-sql-info. Коли MS SQL знайдено, необхідно отримати доступ до сервера. MS SQL підтримує два способи аутентифікації:

1. **Windows Authentication** (trusted connection), дозволяє виконувати в якості користувача Windows, який перевірений на рівні ОС.
2. **Змішаний режим** – автентифікація засобами SQL Server.

За замовчуванням стоїть режим автентифікації Windows, але змішаний режим набагато гнучкіший. Деякі плюси змішаного режиму:

1. Дозволяє SQL Server підтримувати старі версії застосунків, а також стороннім виробникам ПО.
2. Дозволяє підтримувати інші середовища з декількома ОС, в яких не проходять перевірку Windows.
3. Дозволяє скласти ієрархію в дозволах звертанням до бази даних.

Зазвичай на такому етапі немає доступу в корпоративну мережу, тобто неможливо використовувати автентифікацію Windows. Однак існує відкритий порт 1433, в такому випадку на SQL Server присутній користувач SA(System Administrator) і є можливість спробувати підібрати пароль під неї.

Якщо отримано доступ до SA, виникає найпростішим способом отримання даних. Як правило такий доступ не розповсюджений, оскільки дуже простий для взлома. Якщо ж доступ до SA не отримано, зловмисники використовують sql-ін’єкції у запити, щоб отримати доступ до БД. Для прикладу,простий sql-запит, який відбирає дані. Нам

необхідно використати процедуру xp_cmdshell, але для неї необхідні права адміністратора БД.

Використовуючи простий SELECT, виконуємо sql-ін’єкцію. Нам потрібно створити БД та додати користувача:

```
CREATE DATABASE dbmsq;

CREATE LOGIN msadmin WITH PASSWORD
= 'msadmin'
```

Лістинг 2.1.2.1

Наступним кроком робимо нашого користувача sysadm,

```
USE dbmsq
ALTER LOGIN [msadmin] with
default_database = [dbmsq];
CREATE USER [bob] FROM LOGIN [bob];
EXEC sp_addrolemember [db_owner], [bob];
```

Лістинг 2.1.2.2

Тепер нам необхідно включити можливість персоналізації, та отримати права адміністратора:

```
ALTER DATABASE dbmsq SET TRUSTWORTHY ON

USE dbmsq
GO
CREATE PROCEDURE sp_lvlup
WITH EXECUTE AS OWNER
AS
EXEC sp_addsrvrolemember 'bob','sysadmin'
```

Лістинг 2.1.2.3

Процедура sp_lvlup створена від імені OWNER, что в даному випадку є користувачем sa. Це можливо завдяки тому, що база створенна від db_owner, а ця база є довіреною, тобто TRUSTWORTHY = On. Без цієї властивості не вдалось би виконати процедуру. Активована властивість TRUSTWORTHY – це не завжди погано. Проблеми починаються, коли адміністратори не контролюють привілеї власників баз. В результаті ми отримали доступ sysadmin.

Отримавши доступ до потрібних нам прав – потрібно дозволити використання cmdshell:

```
EXEC sp_configure 'show advanced options',1;
reconfigure;
‘exec sp_configure 'xp_cmdshell',1;
reconfigure
```

Лістинг 2.1.2.4

Для найпростішого взлому, використовують доступ по RDP (Remote Desktop Protocol):

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentCon
trolSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0 /f

exec master.dbo.xp_cmdshell 'net user root toor
```

Лістинг 2.1.2.5

У результаті, ми створили користувача в системі Windows, та відкрили доступ до сервера. Наступним кроком потрібно відкрити консоль mstsc, ввести дані, і ми отримали доступ на сервер з правами адміністратора.

2.2 Методи захисту баз даних від SQL-ін'єкцій

Правила які гарантують нам захист від ін’єкцій:

1) Дані необхідно використовувати в запитах тільки з використанням плейсхолдерів

2) Ідентифікатори і ключові слові підставляються з білого списку, загодя прописані в нашому коді.

Звичайно, практичне використання даних правил потребує більш детального опису. Плейсхолдери – це використання точних даних, всі дані повинні попадати в запит не напряму, а за допомогою свого роду представника.

2.2.1 Плейсхолдери як основний метод захисту від SQL-ін’єкцій

Більшість статей, присвячених ін’єкціям пропускають цей момент. Але реальність така, необхідно підставляти не тільки дані в запити, але й інші елементи, такі як ідентифікатори, елементи синтаксису, ключові

слова. Навіть такі незначні елементи як DESC чи AND, але потреба в безпеці таких підстав все рівно повинні бути не менш строгими.

Розберемо звичайний випадок. В нас є база товарів, яку необхідно вивести на екран користувачу в вигляді HTML таблиці. Особа яка використовує дану таблицю, може проводити будь-які дії відносно даних в таблиці, що приводить до значень які може використовувати користувач, а саме: атрибути та ідентифікатори. Використання даних значення на пряму в запит – це гарантована ін'єкція. Методи форматування до яких усі привикли тут не допоможуть. Підготовка вираження ні з яким ідентифікатором, ні з ключовим словом не приведуть до потрібного результату. Єдине правильне рішення в цій ситуації – це білий список.Це звичайне поняття і практично всі досвідченні розробники легко добавляють його у потрібні запити.

Для використання даного методу, нам необхідно щоб усі дані були прописані в коді в якості змінних, що унеможливлює ін'єкцію в даний запит.

Суть даного методу у тому, що всі можливі варіанти вибору повинні бути чітко прописані в нашому коді, і в запит попадатимуть тільки вони, на основі користувацького вводу.

```
$order = isset($_GET['order']) ? $_GET['order'] : ''; //

$sort = isset($_GET['sort']) ? $_GET['sort'] : '';

$allowed = array("name", "price", "qty");

$key = array_search($sort,$allowed);

$orderby = $allowed[$key];

$order = ($order == 'DESC') ? 'DESC' : 'ASC';

$query = "SELECT * FROM `table` ORDER BY
```

Лістинг 2.2.1.1.

Раніше вважалось, що для ідентифікаторів достатньо плейсхолдерів, але тепер люди дійшли до висновку, що інснують наступні мінуси даної практики:

1) У випадку невірного імені запит видасть помилку.

2) Якщо використовувати імена полів без перевірки - ми отримаємо ін'єкцію іншого виду.

Так що тепер я використовую обидва методи: спочатку отримую ідентифікатор з білого списку, потім добавляю його через плейсхолдер – просто щоб не займатись форматуванням вручну. В принципі, цієї інформації достатньо щоб почати писати повністю безпечні запити, але в житті бувають різні нюанси, тому плейсхолдери потрібно розібрати детальніше.

2.2.1.1 Робота з плейсхолдерами

Насамперед потрібно зрозуміти, що існують два варіанти реалізації плейсхолдерів – серверні та клієнтські, а саме:

- В першому випадку запит і дані відправляються окремо. Обробка реалізується самою СУБД, на сервері.
- В другому випадку дані формуються і підставляються в стрічку запиту на місце плейсхолдерів прямо на клієнта, формуються класичні SQL-запити.

Кожен з цих способів має свої недоліки і переваги. Потрібно пам'ятати, що по замовчуванню працюють по-другому варіанту, імітуючи роботу по першому.

2.2.1.2 Перелік основних недоліки наявних бібліотек

На даному етапі розвитку захисту баз даних присутні такі недоліки бібліотек:

- багатослівність
- біндінг
- неможливість використання стандартних SQL запитів

- продуктивність

Багатослівність. При створенні класичного запиту вибірки значень з двовимірного масиву, нам необхідно використати довгий запит, оскільки в mysql не існує скороченого формату даної реалізації. У підсумку, для виконання даної задачі нам необхідний наступний запит:

```
$data  = array();

$query = "SELECT Name, Population, Continent
FROM Country WHERE Continent=? ORDER BY
Name LIMIT 1";
$stmt->prepare($query);
$stmt->bind_param("s", $continent);
$stmt->execute();
```

Лістинг 2.2.1.2.1

Даний запит можливо скласти без використання такої кількості частин, використавши усього лиш 2 рядки:

```
$query = "SELECT Name, Population, Continent
FROM Country WHERE Continent=? ORDER BY
Name LIMIT 1"; $data  = $db-
>getAll($query,$continent);
```

Лістинг 2.2.1.2.2

Біндінг. От є у мене змінна $ _GET ['id']; я хочу прив'язати її до плейсхолдеру. Відмінно, я можу це зробити прямо в execute () ... але тільки зробивши її масивом.

Недостатність функціонала. Оператор IN (). Для створення даного запиту необхідно використати наступний запит:

```
$conts = array('Europe','Africa','Asia','North America');

$query = "SELECT * FROM Country WHERE Continent IN(?) ORDER BY Name LIMIT 1";
$data  = $db->getAll($query,$conts);
```

Лістинг 2.2.1.2.3

Продуктивність. Зазвичай апологети серверних підготовлених виразів напирають на той факт, що парсинг запиту робиться тільки один раз.

На жаль, для веб-додатки це не працює. У підсумку виходить більше роботи там, де хотіли заощадити.

Ще одним потенційним виграшем в швидкості є кешування планів запитів. І навіть якщо ми робимо prepare() для кожного запиту, то БД може тримати в собі кешовані одні і ті ж дані для різних запитів. І отримати план виконання без парсинга, а простим порівнянням рядків. При реальних навантаженнях серверні готові запити програють у швидкості класичних запитам.

2.2.1.3 Самостійна реалізація плейсхолдеров

Взагалі, насправді ніхто не заважає нам поліпшити юзабіліті наявних бібліотек, які не витрачають час на плейсхолдери. Скажімо, написати обгортку над PDO, яка реалізує відсутній функціонал, використовуючи при цьому власні плейсхолдери PDO.

Як ми вже переконалися, в класичних бібліотеках недостатньо корисних плейхолдерів та серверні плейсхолдери можливо використовувати не в усіх можливих випадках.

2.2.1.4 Принципи форматування елементів SQL запиту

Створення власних плейсхолдерів не складна задача. Стандартний спосіб

існує в PHP. Все що потрібно - це розрізняти різні частини запиту. Правила створення запитів залежні від атрибутів, тому необхідно розуміти, який саме атрибут нам потрібен. Візьмемо, для прикладу, такий SQL запит:

```
INSERT INTO `db`.`table` as `t1`
VALUES('string',1,1.5,NOW());
```

Лістинг 2.2.1.4.1

Нам необхідні ідентифікатори та літерали з даного запиту, для точної підстановки в базу даних. В PDO це реалізується за допомогою стрічок - запит передає тільки стрічки, які парсяться у потрібний формат, але інколи це може призвести до помилок.

2.2.1.5 Форматування ідентифікаторів

Для ідентифікаторів існують всього два правила:

- Ідентифікатор має викликатись тільки в одинарних лапках (backticks)
- якщо такі лапки зустрічається в імені - вони повинні бути екрановані подвоєнням.

Треба чи не треба форматувати ідентифікатори? Адже в більшості випадків це не потрібно?
Якщо запит пишеться руками, то необхідність можна визначити на місці: працює запит - годі й форматувати; вилітає з помилкою на ідентифікатор - треба форматувати.
Якщо ж ми використовуємо плейсхолдер - тобто, додаємо ідентифікатор в запит динамічно - форматувати треба обов'язково, оскільки ми не знаємо, яке ім'я поля буде підставлена в запит, і, отже, потрібно чи йому форматування, чи ні. Значить, будемо форматувати все.
Саме використання плейхолдерів розуміється як правильне форматування

даних при підстановці їх в запит, і це допомагає нам захиститись від sql-ін’єкцій.

2.2.1.6 Форматування строкових літералів

Форматування стрічок в запитах мають свої правила:

- Використання лапок для рядка літералів
- В рядку мають виділятись спеціальні символи згідно правил.

Більшість людей їх не використовує, навіть в документації по PHP, в статті про mysql_real_escape_string () написано: «Якщо не користуватися цією функцією, то запит стає вразливим для злому за допомогою SQL-ін'єкцій. »- як ніби якщо її використовувати для чисел або ідентифікаторів, то це хоч якось допоможе.

3 Висновки до другого розділу (Захист від sql-ін’єкцій)

В даному розділі розглянуто типи атак на SQL сервер та їх приклади. Розлянуто базовий приклад вразливостей SQL-сервера завдяки якому можливо отримати повний адміністративний доступ до сервера.

Також розглянуто методику боротьби з sql-ін’єкціями засобами плейсхолдерів. Плейсхолдери - це змінні які чітко вказують що і як повино бути передано клієнтом на сервер, без можливості вставити в них ін’єкцію. В даному розділі описані правила користування плейхолдерами, випадки їх використання та переваги. Плейхолдери - це одна з найкращих методів захисту від sql-атак, але sql-ін’єкції - це не єдиний метод атаки на цілісність баз даних. Інші методи захисту від sql-атак будуть розглянуті в наступному розділі.

Розділ 3. Сучасні методи захисту конфіденційної інформації в базах даних Microsoft SQL Server та mySQL

3.1 Авторизація за допомогою алгоритму TOTP

На сьогоднішній день все більше компаній використовують одноразові паролі для збільшення рівню безпеки клієнтів та їх персональних даних. Ці компанії в основному використовують алгоритм HOTP - який створює хешованне значення використовуючи певні параметри, за рахунок чого досягається безпека. Але все більшої популярності отримує алгоритм TOTP - який використовує алгоритм HOTP з однією особливістю - він базується на часі.

Авторизація за допомогою алгоритму TOTP і HOTP є ефективними сучасними методами захисту конфіденційної інформації в базах даних. Їх основою є хеш-функція, яка дозволяє взяти дані будь-якої довжини і побудувати «цифровий відбиток пальця» за цими даними. Безпека алгоритмів TOTP і HOTP є засобами запобіганню двом найпоширенішим атакам: атака виду “людина посередині” і атака повторного відтворення. Їх функція полягає у застосуванні лічильника, який періодично змінює дані, які використовують для генерації одноразових паролів.

3.1.1 Хеш-функція

Хеш-функція дозволяє взяти дані будь-якої довжини і побудувати короткий «цифровий відбиток пальця» за цими даними. Довжина значення хеш-функції не залежить від довжини вихідного тексту; наприклад, у випадку використання алгоритму SHA-1 довжина цього відбитка становить 160 біт.

Це значення завжди має однакову довжину і не залежить від початкового тексту. Хеш-функцію порівнюють з виглядом кодового замка з коліщатками. Усі коліщатка виставляють в «нуль», потім йдемо

по текстом для кожної літери прокручують коліщатка відповідно до встановлених правил. Те число, яке виявиться на кодовому замку у кінці, і є значенням хеш-функції. Сюди належать такі засоби як: MD5, SHA-1.

Ідея хеш-функції в тому, що вона працює виключно в одному напрямку, що унеможливлює по вже готовому значенню хеш-функції знайти документ, який видасть таке ж значення. Це означає, що при зміні навіть однієї букви, хеш також змінюється.

3.1.2 Принцип роботи TOTP

Алгоритм TOTP базується на алгоритмі HOTP, в якому значення лічильника підставлено величиною, яка залежить від часу.

Формула складається з:

T – дискретне значення часу.

X – інтервал часу, протягом якого дійсний пароль.

T – проміжок часу, необхідний для синхронізації двох сторін.

K – публічний ключ.

Current Time – поточний час.

$$T = (CurrentTime - T_0)/X$$

$$\text{HOTP}(K, T) = Truncate(\text{HMAC-SHA-1}(K, T))$$

$$\text{TOTP} = \text{HOTP}(K, T)$$

3.1.3 Відмінність методів HOTP та TOTP

Основною відмінністю між двома алгоритмами є генерація пароля на основі мітки часу, яку використовують в ролі параметра TOTP-алгоритму. При цьому використовується не точне значення часу, а поточний інтервал, межі якого були встановлені заздалегідь (наприклад, 30 секунд).

HOTP - спирається на дві основні речі: загальний секрет і рухомий фактор . Як частина алгоритму HmacSHA1, рухомий фактор буде створюватись на основі секретного ключа. Цей алгоритм ґрунтується на подіях, тобто кожен раз, коли генерується новий OTP, рухомий фактор буде збільшуватися, отже, згенеровані паролі повинні бути різними.

TOTP - працює аналогічно HOTP, він також використовує загальний секрет та рухомий фактор, одна даний фактор створюється іншим способом. В TOTP рухомий фактор змінюється з використанням часу.

Основної ж відміністю даних способів полягає в тому, що паролі HOTP можуть бути дійсними протягом невизначеного періоду часу, а TOTP доступні тільки у короткі проміжки часу. Через це TOTP вважається безпечнішим.

3.1.4 Безпека алгоритм HOTP

Системи захисту, побудовані з використанням HOTP та TOTP стійкі до поширених криптографічних атак. Авторизація за допомогою алгоритму TOTP і HOTP є ефективними сучасними методами захисту конфіденційної інформації в базах даних. Їх основою є хеш-функція, яка дозволяє взяти дані будь-якої довжини і побудувати «цифровий відбиток пальця» за цими даними. Безпека алгоритмів TOTP і HOTP є засобами запобіганню двом найпоширенішим атакам: атака виду “людина посередині” і атака повторного відтворення. Їх функція полягає у застосуванні лічильника, який періодично змінює дані, які використовують для генерації одноразових паролів.

3.2 Застосування технології Blockchain для захисту інформації

3.2.1 Поняття технології Blockchain

У 2008 році вперше задокументували дизайн blockchain, а у 2009 році його вперше реалізували з відкритим кодом була розгорнута як невід'ємний елемент Bitcoin, першої децентралізованої цифрової валютної

системи для розповсюдження біткойнів за допомогою відкритого випуску програмного забезпечення “Bitcoin peer to peer”.

Система Bitcoin використовує блокчейн як розподілену загальну книгу, яка записує та перевіряє всі транзакції біткойна на відкритій мережевій системі. Інновація блокчейна полягає у його здатності запобігати подвійним витратам у транзакціях, якими торгуютьу повністю децентралізованій мережі без залучення зовнішнього довіреного центрального органу.

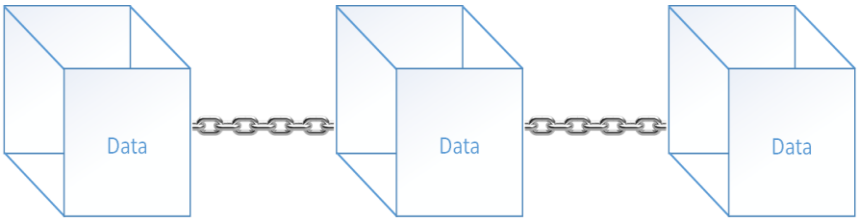


Рисунок 3.2.1.1 Схема роботи Блокчейн

Блокчейн організовує зростаючий перелік записів транзакцій в ієрархічно розширюваному ланцюгу блоків, захищеним методами криптографії, щоб забезпечити міцну цілісність своїх записів транзакцій. Нові блоки можуть бути задіяні у глобальну блок-ланцюзі лише після їх успішної конкуренції з децентралізованою процедурою взаємозгоди. Окрім інформації про записи транзакцій, блок також тримає у собі хеш-значення всього блоку, що може розглядатися як його криптографічне зображення, плюс хеш-значення попереднього блоку, який слугує криптографічним зв'язком з попереднім блок в блокчейн. Децентралізована процедура взаємозгоди застосовується мережею, яка контролює прийом нових блоків до ланцюга блоків, протокол зчитування для безпечної перевірки ланцюга блоків та узгодженість вмісту даних записів транзакцій, що містяться у кожній копії блокчейна та підтримуються на кожному вузлі. Як результат, блокчейн забезпечує те, що запис транзакцій буде доданий до блоку, а блок, у свою чергу, буде успішно створений та зафіксований у блокчейні.

Запис транзакцій не може бути змінено або порушено у ретроспективі. Цілісність вмісту даних у кожному блоці ланцюга гарантовано таким чином, що блоки, потрапивши в блокчейн, не можуть бути замінені жодним чином. У результаті, блок-ланцюг служить захистом для розподіленої книги, яка ефективно перевіряє усі операції між двома сторонами відкритої мережевої системи.

У контексті біткойн-систем блокчейн використовується як його захищений, приватний та надійний публічний архів для всіх транзакцій, які торгують біткойнами в мережі. Це гарантує, що всі транзакції з біткойнами записуються, організовуються та зберігаються в криптографічно захищених блоках, які є ланцюжками у певній та стійкій формі.

Blockchain – це головний захист біткойн-транзакцій від багатьох поширених атак. З розвитком технології blockchain, Bitcoin вплинув на його застосування в інших галузях, таких як охорона здоров'я, логістика, сертифікація освіти. Екосистема блокчейна стрімко зростає зі збільшенням інвестицій та інтересів промисловості, уряду та наукових установ у введенні децентралізованих систем баз даних.

3.2.2 Принципи роботи технології Blockchain

Блокчейн функціонально служить розподіленою та захищеною базою даних журналів транзакцій. Якщо у мережі Bitcoin клієнт A хоче надіслати деякі біткойни іншому клієнту B, він створить біткойн-транзакцію клієнтом A. Транзакція повинна бути затверджена майнерами до того, як вона буде виконана мережею Bitcoin.

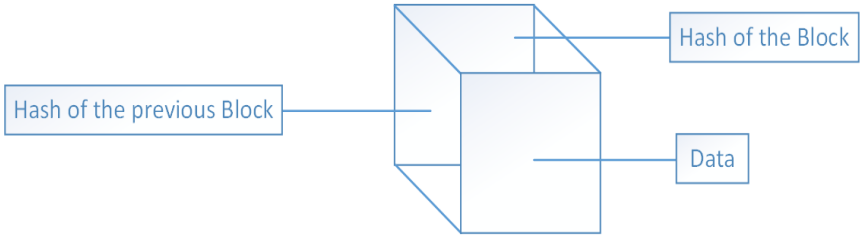


Рисунок 3.2.2.1Принцип роботи блокчейн

Майнери – це суб’єкти, які використовують ресурси власних ПК для добування певних значень хешу які не повторюються.

Для ініціювання процесу видобутку транзакція транслюється на кожний вузол мережі. Ті вузли, які є майнерами, збиратимуть транзакції в блок, перевірять транзакції в блоці та транслюватимуть блок для його перевірки, використовуючи протокол взаємозгоди для отримання схвалення від мережі. Коли інші вузли перевіряють, що всі транзакції, що містяться в блоці, є дійсними, блок додається до блокчейну. Тільки тоді, коли блок, що містить транзакцію, буде затверджений іншими вузлами та доданий до блокчейну, ця передача біткойна з A на B буде виконана та вважатиметься законною.

Три основні можливості, які підтримуються реалізацією блокчейна в Bitcoin:

1. Хеш-накопичувальне сховище (Hash Chained Storage).
2. Цифровий підпис.
3. Зобов'язання щодо додавання нового блоку до глобально ланцюгового сховища.

З правильним поєднанням набору відомих методів безпеки, таких як ланцюг Hash, дерево Merkle, цифровий підпис, з механізмами взаємозгоди, блокчейн може запобігти як проблемі подвійного витрачання біткойнів, так і не дозволити зміну будь-яких даних транзакцій в блоці іншою датою.

3.2.3. Хеш-накопичувальне сховище (Hash Chained Storage)

Показник Hash і дерево Merkle є двома основними будівельними блоками для реалізації блокчейна за допомогою хеш-ланцюгового сховища. Таким чином, хеш-показник використовують для перевірки того, чи дані сфальсифіковані. Блок ланцюга організований за допомогою хеш-показників для з'єднання блоків даних разом. За допомогою хеш-показника, що вказує на блок попередника, кожний блок вказує адресу, де зберігаються дані блоку попередника.

Хеш збережених даних може бути публічно перевірений користувачами, щоб довести, що збережені дані не були сфальсифіковані. Якщо зловмисник намагається змінити дані в будь-якому блоці у цілому ланцюгу, щоб замаскувати фальсифікацію, опонент повинен змінити хеш-показники усіх попередніх блоків. У результаті зловмисник припинить фальсифікацію, оскільки він не зможе підмінити дані основної частини ланцюга, яка генеруються після побудови системи. Цей початковий блок у ланцюзі називається блоком генезису.

3.2.4 Безпека та конфіденційність у ланцюзі Blockchain

Блокчейн стійкий до несанкціонованих дій. Користувачам дозволено повертатися до певного блоку та перевіряти його з початку ланцюга. Дерево Merkle є двійковим деревом пошуку з вузлами, пов'язаними між собою за допомогою хеш-показників. Така структура даних використовується для побудови блокчейна.

Ці вузли групують у роз'єднані групи, так що кожного разу два вузли на нижньому рівні згруповані в один на батьківському рівні, а для кожної пари вузлів нижчого рівня алгоритм побудови дерева Merkle створює новий вузол даних, який містить хеш-значення кожного з них. Цей процес повторюється до досягнення кореня дерева. Дерево Merkle має можливість запобігати фальсифікуванню даних шляхом проходження через хеш-показники до будь-якого вузла дерева.

Наприклад, коли зловмисник намагається підмінити дані на певному вузлі, це спричиняє зміну хеш-значення його батьківського вузла, і навіть якщо він продовжить підміняти верхній вузол, йому потрібно змінити усі вузли на шляху від низу до верху. Таким чином, можна виявити сфальсифіковані дані, оскільки хеш-показник кореневого вузла не збігається із збереженим хеш-показником.

Перевага дерева Merkle полягає в тому, що воно може ефективно довести приналежність до вузла даних, показавши цей вузол та всі його частини на його вихідному шляху до основного вузла. Приналежність до

дерева Merkle можна перевірити в логарифмічному часі, обчисливши хеші на шляху та перевіривши хеш-значення на наявність коренів.

3.2.5 Цифровий підпис

Цифровий підпис встановлює обгрунтованість частини даних за допомогою криптографічного алгоритму. Це також схема перевірки того, що фрагмент даних не є сфальсифікованим.

Існують три основні компоненти, які формують схему цифрового підпису. Перший компонент – це алгоритм генерації ключів, який створює два ключі, один використовується для підписання повідомлень і зберігається приватно, називається приватним ключем, а другий стає доступним для публіки і називається відкритим ключем, який використовується для перевірки того, чи повідомлення має підпис, підписаний відповідним приватним ключем.

Другий основний компонент – це алгоритм підписання. Він створює підпис на вхідному повідомленні, який підтверджений за допомогою даного приватного ключа.

Третій основний компонент – це алгоритм перевірки. Він приймає підпис, повідомлення і відкритий ключ як вхідні дані, та перевіряє підпис повідомлення за допомогою відкритого ключа, а також повертає булеве значення.

Правильно визначений і безпечний алгоритм підпису повинен мати дві властивості. Перша властивість є дійсною, коли підписи перевірені. Друга властивість є дійсною, коли підписи незмінні. Це означає, що зловмисник, у якого є відкритий ключ, не може підмінити підписи у цих повідомленнях.

3.2.6 Алгоритм цифрового підпису еліптичної кривої (ECDSA)

Блокчейн, який використовується в Bitcoin, приймає ECDSA як свою схему цифрового підпису для спільних транзакцій. Використовуючи ECDSA над стандартною еліптичною кривою “secp256k1”, для біткойн-блоку забезпечується 128 бітів безпеки. ECDSA є стійким до підробки

при атаці на обране повідомлення на основі загальної групи та його стійкості до певної атаки. Таким чином, схема цифрового підпису на зразок ECDSA є стійкою до атаки обраного повідомлення проти законного суб'єкта C, яка спрямована на фальсифікацію справжнього підпису на невидимому повідомленні M, після того, як опонент отримав підпис суб'єкта C у результаті надсилання набору вибраних запитів у відповідь на групу повідомлень (не включаючи повідомлення M).

Перевага використання цифрового підпису полягає в ефективному підтвердженні автентичності повідомлення, використовуючи PKI таким чином, що автор повідомлення підписується перед тим, як надсилати його з приватним ключем, і одержувач цього підписаного повідомлення може використовувати відкритий ключ відправника для підтвердження дійсності цього повідомлення. У більшості сценаріїв є можливим отримання пари ключів від довіреного третього учасника. PKI використовується для управління відкритими ключами шляхом встановлення обов'язкової угоди між відповідними особами суб'єктів.

Таке прив'язування здійснюється шляхом реєстрації та видачі сертифікатів у сертифікаційному органі (CA). Процес перевірки підпису автоматично переводиться на перевірку ідентичності підписувача на основі гарантованості рівня прив'язки. Таким чином, відкритий ключ розглядається як ідентичність у цих сценаріях. У той час як блокчейн Bitcoin приймає децентралізоване управління ідентифікацією, не маючи центрального органу для реєстрації користувача в системі, самі користувачі генерують цю пару ключів. Користувачі можуть генерувати необмежену кількість пар ключів. Ці ідентичності (хеші відкритих ключів) називаються адресами в Bitcoin. Оскільки немає центрального управління відкритими ключами, ці ідентичності і є фактично псевдонімами, складеними користувачами.

Отже, технологія блокчейн - є сучасним способом реалізації захисту даних. Даний метод тільки починає набирати обертів у сфері захисту баз даних MS SQL, та використовується тільки на хмарних базах даних

AZURE. На мою думку в даній методиці є потенціал, який потрібно розвивати, так використовувати в розподілених базах даних, для уникнення можливого втручання в достовірність інформації.

3.3 Методика захисту інформації в базах даних

Використовуйте ефективні технічні засоби захисту

- Системи централізованого управління оновленнями і патчами для використовуваного ПО. Для правильної приоритизации планів по оновлень необхідно враховувати відомості про актуальні загрози безпеці.
- Системи антивірусного захисту з вбудованою ізольованою середовищем («пісочницею») для динамічної перевірки файлів, здатні виявляти і блокувати шкідливі файли в корпоративній електронній пошті до моменту їх відкриття співробітниками та інші вірусні загрози. Найбільш ефективним буде використання антивірусного ПО, побудованого на рішеннях одночасно декількох виробників, здатного виявляти приховане присутність шкідливих програм і дозволяє виявляти і блокувати шкідливу активність в різних потоках даних - в поштовому, мережевому і веб-трафіку, в файлових сховищах, на веб-порталах. Важливо, щоб обране рішення дозволяло перевіряти файли не тільки в реальному часі, а й автоматично аналізувало вже перевірені раніше, це дозволить виявити виявлені раніше загрози при оновлені баз сигнатур.
- SIEM-рішення для своєчасного виявлення та ефективного реагування на інциденти інформаційної безпеки. Це дозволить своєчасно виявляти зловмисну активність, спроби злому інфраструктури, присутність зловмисника і вживати оперативних заходів по нейтралізації загроз.
- Автоматизовані засоби аналізу захищеності і виявлення вразливостей в ПО.

- Міжмережеві екрани рівня додатків (web application firewalls) - як превентивний захід захисту веб-ресурсів.
- Системи глибокого аналізу мережевого трафіку - для виявлення складних цільових атак як в реальному часі, так і в збережених копіях трафіку. Застосування такого рішення дозволить не тільки побачити не виявлені раніше факти злому, але і в режимі реального часу відслідковувати мережеві атаки, в тому числі запуск шкідливого ПО і хакерських інструментів, експлуатацію вразливостей ПЗ та атаки на контролер домену. Такий підхід дозволить істотно знизити час таємного присутності порушника в інфраструктурі, і тим самим мінімізувати ризики витоку важливих даних і порушення роботи бізнес-систем, знизити можливі фінансові втрати від присутності зловмисників.
- Спеціалізовані сервіси анти-DDoS.

Захищайте дані

- не зберігайте чутливу інформацію у відкритому вигляді або у відкритому доступі;
- регулярно створювати резервні копії систем і зберігайте їх на окремих серверах окремо від мережевих сегментів робочих систем;
- мінімізуйте, наскільки це можливо, привілеї користувачів і служб;
- використовуйте різні облікові записи і паролі доступу до різних ресурсів;
- застосовуйте двухфакторную автентифікацію там, де це можливо, наприклад для захисту привілейованих облікових записів.

Не допускайте використання простих паролів

- застосовуйте парольний політику, що передбачає суворі вимоги до мінімальної довжині і складності паролів;
- збільшіть термін використання паролів (не більше 90 днів);
- змініть стандартні паролі на нові, що задовольняють суворої пральний політиці.

Контролюйте безпеку систем

- своєчасно оновлюйте використовуване ПЗ в міру виходу патчів;
- перевіряйте і збільшуйте обізнаність співробітників в питаннях інформаційної безпеки;
- контролюйте поява небезпечних ресурсів на периметрі мережі; регулярно проводити інвентаризацію ресурсів, доступних для підключення з інтернету; аналізуйте захищеність таких ресурсів і зменшуйте ризики вразливостей в використовуваному ПО; гарним вибором постійний моніторинг публікацій про нові вразливості: це дозволяє оперативно виявляти такі уразливості в ресурсах компанії і своєчасно їх усувати;
- ефективно фільтруйте трафік для мінімізації доступних зовнішньому зловмисникові інтерфейсів мережевих служб; особливу увагу варто приділяти інтерфейсів віддаленого управління серверами і мережевим обладнанням;
- регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак на внутрішню інфраструктуру і оцінки ефективності вжитих заходів щодо захисту;
- регулярно проводити аналіз захищеності веб-додатків, включаючи аналіз вихідного коду, з метою виявлення та усунення вразливостей, що дозволяють проводити атаки, в тому числі на клієнтів додатки;
- відстежуйте кількість запитів до ресурсів в секунду, налаштуйте конфігурацію серверів і мережевих пристроїв таким чином, щоб нейтралізувати типові сценарії атаки (наприклад, TCP- і UDP-флуд або множинні запити до БД).

Подбайте про безпеку клієнтів

- підвищуйте обізнаність клієнтів в питаннях ІБ;
- регулярно нагадуйте клієнтам про правила безпечної роботи в інтернеті, пояснюйте методи атак і способи захисту;

- застерігайте клієнтів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої інформації кому б то не було по електронній пошті або під час телефонної розмови;
- пояснюйте клієнтам порядок дій в разі підозр про шахрайство;
- повідомляйте клієнтів про події, пов'язані з інформаційною безпекою.

Як вендору захистити свої продукти

- застосовуйте все ті ж заходи захисту, що рекомендовані для забезпечення безпеки організації;
- упровадите процеси забезпечення безпеки протягом усього циклу розробки ПЗ;
- проводите регулярний аналіз захищеності ПО і веб-додатків, включаючи аналіз вихідного коду;
- використовуйте актуальні версії веб-серверів і СУБД;
- відмовтеся від використання бібліотек і фреймворків, що мають відомі уразливості.

Як захиститися звичайному користувачеві

Не економте на безпеці

- використовуйте тільки ліцензійне ПЗ;
- використовуйте ефективні засоби антивірусного захисту на всіх пристроях;
- своєчасно оновлюйте використовуване ПЗ в міру виходу патчів.

Захищайте ваші дані

- найбільш важливі файли зберігайте не тільки на жорсткому диску комп'ютера, але і на знімних носіях, зовнішніх жорстких дисках або в хмарному сховищі;
- для повсякденної роботи в ОС використовуйте обліковий запис без привілеїв адміністратора;
- використовуйте двухфакторную автентифікацію там, де це можливо, наприклад для захисту електронної пошти.

Не використовуйте прості паролі

- використовуйте складні паролі, що складаються з незначних комбінацій букв, цифр і знаків, довжиною не менше 8 символів. Для створення і зберігання паролів можна скористатися менеджером паролів (захищеним сховищем з функціями генерації нових паролів);
- не використовуйте один і той же пароль для різних систем (для сайтів, електронної пошти та ін.);
- міняйте всі паролі хоча б раз на півроку, а краще - кожні два-три місяці.

Будьте пильні

- перевіряйте всі вкладення, отримані по електронній пошті, за допомогою антивірусного ПО;
- з обережністю ставитись до сайтів з некоректними сертифікатами і враховуйте, що введені на них дані можуть бути перехоплені зловмисниками;
- будьте гранично уважні при введенні облікових даних на сайтах і під час роботи з онлайн-платежами;
- не переходьте за посиланнями на незнайомі підозрілі ресурси, особливо коли браузер попереджає про небезпеку;
- не переходьте за посиланнями з спливаючих вікон, навіть якщо рекламовані компанія або продукт вам знайомі;
- не завантажуйте файли з підозрілих веб-ресурсів або з інших невідомих джерел.

Об'єкт атаки - об'єкт деструктивного впливу з боку кіберзлочинців. Якщо методи соціальної інженерії спрямовані на отримання інформації безпосередньо від приватної особи, клієнта або співробітника компанії, то об'єктом атаки є категорія «Люди». Якщо ж методи соціальної інженерії застосовуються з метою доставки ВПО в інфраструктуру компанії або на комп'ютер приватної особи, то в якості об'єкта атаки вибирається категорія «Комп'ютери, сервери та мережеве обладнання».

Мотив атаки - першорядна мета кіберзлочинців. Наприклад, якщо в результаті атаки викрадені дані платіжних карт, мотивом в цьому випадку є отримання даних.

Методи атаки - сукупність прийомів, які використовувалися для досягнення мети. Наприклад, зловмисник може провести розвідку, виявити доступні для підключення вразливі мережеві служби, використовувати уразливості і отримати доступ до ресурсів або інформацію; такий процес ми називаємо хакингом. При цьому підбір облікових даних і використання вразливостей веб-додатків ми виділили в окремі категорії для більшої деталізації.

Категорія жертв - сфера діяльності атакований організації (або приватні особи, якщо в результаті атаки постраждали люди незалежно від місця їх роботи). Так, до сфери послуг ми відносимо організації, які надають послуги на комерційній основі (наприклад, консалтингові організації або готелі, ресторани та ін.). Категорія «Онлайн-сервіси» включає інтернет-майданчики, що дозволяють користувачам вирішувати їх завдання онлайн (наприклад, сайти-агрегатори для покупки квитків, бронювання номерів у готелях, блоги, соцмережі, месенджери і інші соціальні медіа-ресурси, відеохостінги, онлайн-ігри). Масштабні кібератаки, переважно шкідливі епідемії, які не обмежуються впливом на якусь одну галузь, ми віднесли до категорії «Без прив'язки до галузі».

За моєю оцінкою, більшість кібератак не віддається розголосу через репутаційних ризиків, тому оцінити точне число загроз не можуть навіть організації, що займаються розслідуванням інцидентів і аналізом дій хакерських груп. Дане дослідження проводиться з метою звернути увагу організацій і звичайних громадян, які цікавляться сучасним станом інформаційної безпеки, на найбільш актуальні методи і мотиви кібератак, а також з метою виявити основні тенденції в зміні ландшафту кіберзагроз.

Висновки до третього розділу

Отже в третьому розділі ми розглянули такі методи захисту даних як: авторизація методом TOTP, реалізація безпеки даних за допомогою технології блокчейн та загальні правила безпеки баз даних.

Метод TOTP є одним з найкращих способів для захищеної авторизації користувачів у будь-які ресурси, в тому числі доступи до баз даних. Даний метод базується на часі та хешуванні даних для авторизації. Дані рекомендується передавати у захищеному форматі, із використанням конкретного типу шифрування, наприклад RSA.

Реалізація технології блокчейн підходить для використання в розподілених базах даних. Завдяки цьому методу можливо реалізувати захист від змін чи фальсифікації даних в базах даних, що унеможливлює їх зміну, навіть при наявному доступі до бази даних. На сьогодні цей метод широко застосовується для криптовалют, але також і цю технологію блокчейн розвивають для її використання у хмарних базах даних, наприклад Microsoft Azure.

У третьому підрозділі розглянуто методи та рекомендації щодо захисту баз даних, а також базова інформація щодо захисту від можливих атак на інформації і способи її збереження. Якщо використовувати запропоновану мною методику - ви ліквідовуєте можливість будь-яких sql-атак.

Розділ 5. СПЕЦІАЛЬНИЙ РОЗДІЛ

Оскільки в даній роботі розглядалось питання захисту баз даних MS SQL та MySQL то і написання даного захисту буде проводитись безпосередньо в студії розробки MS SQL та частково в брандмауері системи Windows

SQL Server Management studio – середовище розробки та налаштуваннь баз даних MS SQL.

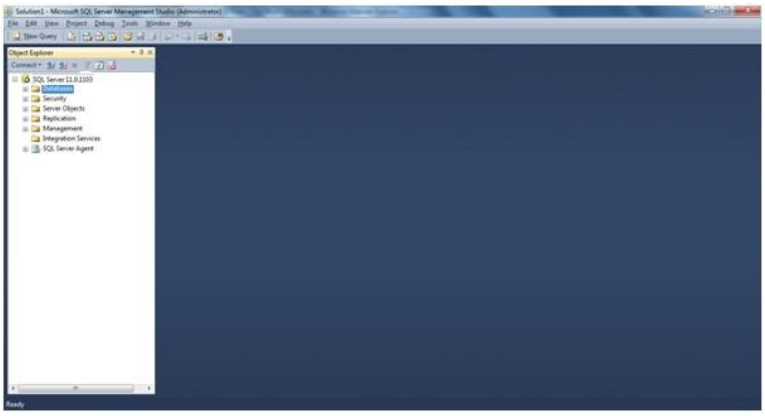


Рис 4.1 SQL Server Management studio

Всього існує декілька ліцензій даної платформи:

1. Express
2. Standart
3. Enterprice
4. Developer
5. Evaluetion

Вони відрязняються як по доступному функціоналі дій так і по ресурсоємкості. Зокрема безкоштовна версія Express дозволяє використовувати серверу тільки 2гб оперативної пам’яті, що дозволяє працювати тільки малим об’єктам, без високої нагрузки на систему.

Також варто відзначити що важливу роль відіграє саме характеристики сервера. Основною характеристикою на яку варто звернути увагу – це швидкість зчитування та запису на жорсткий диск.Багато хто дивиться тільки завантаження процесора, але не треба

забувати що СУБД - це сховище даних. Обсяги даних ростуть, продуктивність процесорів зростає, а швидкість HDD практично не змінюється. З SSD ситуація трохи краща, але терабайти на них зберігати затратно.

Для дисків нам важливі такі показники:

- середня довжина черги (операцій введення-виведення очікують виконання, штук);
- швидкість читання-запису (в Мб / с).

Серверна версія диспетчера задач, як правило (залежить від версії системи), показує і те й інше. Якщо немає - запускаємо оснащення панелі управління "Performance Monitor" (Системний монітор). Нас цікавлять лічильники:

- Фізичний (логічний) диск / Середній час читання (записи)
- Фізичний (логічний) диск / Середня довжина черги диска
- Фізичний (логічний) диск / Швидкість обміну з диском

Для роботи SQL сервера в мережі необхідно також відкрити порти для SQL – TCP 1433. За для зменшення можливості ін’єкції краще використовувати проксі, що б дані передавались не напряму на порт 1433, а будь-який інший.

Для використання технології Blockchain нам необхідна розподіленна база даних.

Розподілена система керування базами даних (РСКБД) — це програмне забезпечення, яке керує РБД і надає такі механізми доступу до них, що їх застосування дає користувачу можливість працювати з РБД як з однією цілісною базою даних.

Розподілена система баз даних (РСБД) — це РБД разом із РСКБД. Не слід плутати РСБД з централізованою базою даних, що використовується в мережі У цьому випадку база даних розташована на одному з комп'ютерів, а всі інші мають доступ до неї через комунікаційну мережу. Не є розподіленою також база даних, що працює в середовищі багатопроцесорних комп'ютерів.

Для використання плейсхолдерів необхідно створювати збережувальні процедури.

Процедура MySQL являє собою підпрограму, що зберігається в базі даних. Вона містить ім'я, список параметрів і оператори SQL. Всі популярні системи управління базами даних підтримують збережені процедури. Вони були введені в MySQL 5.

Існує два види підпрограм: процедури, що і функції, які повертають значення, які використовуються в інших операторах SQL.

Основна відмінність полягає в тому, що функції можуть використовуватися, як будь-яке інше вираження в операторах SQL, а збережені процедури повинні викликатися за допомогою оператора CALL.

Збережені процедури працюють швидко. Перевага сервера MySQL полягає в тому, що він використовує кешування, а також заздалегідь задані оператори. Основний приріст швидкості дає скорочення мережевого трафіку. Якщо є повторювані завдання, які вимагають перевірки, обробки циклів, декількох операторів, і при цьому не вимагають взаємодії з користувачем, це можна реалізувати за допомогою одного виклику процедури, яка зберігається на сервері;

MySQL збережені процедури є універсальними. При написанні збереженої процедури на SQL вона буде працювати на будь-якій платформі, яка використовує MySQL. У цьому перевага SQL над іншими мовами, такими як Java, C або PHP.

Вихідний код збережених процедур завжди доступний в базі даних. Це ефективна практика зв'язати дані з процесами, які їх обробляють.

Розділ 4. Обгрунтування економічної ефективності

Дана дипломна робота розглядає питання захисту конфіденційності інформації в базах даних таких гігантів як MySQL та MsSQL від SQL-атак. Щоб захистити інформацію, та не дати зловмисникам ознайомитися з нею була розроблена методика планування web-додатку, яка допомагає звести захист від можливих атак направлених на проникнення в базу даних та захват серверу.

Суспільство все більш залежить від автоматизованого світу. Щоб існувати віртуально повинні бути дані людини. Користуючись системою та різноманітними додатками ці дані формуються та додаються на основі діяльності в інтернет. Ці дані бувають настільки повними, що можуть повністю скласти соціальний, інтимний, емоційний, фізичний портрети людини. Коли ці дані використовують проти власника, можна знайти слабкі місця та спонукати власника до певних дій. Щоб цього не сталося треба захищати цю таємницю. Це зробити досить легко, якщо виконувати, певні правила.

4.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції:

- вартість розробки проекту інформаційної безпеки (розробка схем пристроїв, політики функціонування системи тощо);
- вартість створення основного й додаткового програмного забезпечення (ПЗ);
- витрати на первісні закупівлі апаратного забезпечення;
- витрати на навчання технічних фахівців і обслуговуючого персоналу. Спершу розрахуємо час, який буде витрачено на створення ПЗ:

$t_д$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_б$ – тривалість розробки блок-схеми алгоритму;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_д$ – тривалість підготовки технічної документації на ПЗ.

Умовна кількість оперантів у програмі:

$Q = q \cdot c\ (1 + p)$, штук, (5.2)

де q – очікувана кількість оперантів - 30;

c – коефіцієнт складності програми -1.5;

p – коефіцієнт корекції програми в процесі її опрацювання – 0.05.

$Q = 30 \cdot 0.8(1+0.05) = 25.2$, штук.

Оцінка тривалості складання технічного завдання на розробку ПЗ $\boldsymbol{t_{тз}}$ – 2 год.

Тривалість вивчення технічного завдання:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k} = \frac{25.2 \cdot 1.2}{0.4725} = \frac{}{80 \cdot 0.8} = \quad \text{, годин,} \qquad (5.3)$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом

- до 2 років – 0,8;

Тривалість розробки блок-схеми алгоритму:

$$t_{о} = \frac{Q}{(20...25) \cdot k} = \frac{25.2}{20 \cdot 0.8} = 1.575 \text{, годин.} \quad (5.4)$$

Тривалість складання програми за готовою блок-схемою:

$$t_{пр} = \frac{Q}{(20...25) \cdot k} = \frac{25.2}{20 \cdot 0.8} = 1.575 \text{, годин.} \quad (5.5)$$

Тривалість опрацювання програми на ПК:

$$t_{опв} = \frac{1,5Q}{(4...5) \cdot k} = \frac{1.5 \cdot 25.2}{4 \cdot 0.8} = 11.8125 \text{, годин.} \quad (5.6)$$

Тривалість підготовки технічної документації на ПЗ:

$$t_{о} = \frac{Q}{(15...20) \cdot} + \frac{Q}{(15...2)} \cdot 0.75 = \frac{25.2}{} + \frac{25.2}{3.36} \cdot 0.75 = \text{ годин.} \quad (5.7)$$

Розрахунок витрат на створення програмного продукту

$K_{пз} = З_{зп} + З_{мч}$. грн (5.8)

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$З_{зп} = t \cdot З_{пр} = 20.795 \cdot 19.04 = 395.93$, грн, (5.9)

де t – загальна тривалість створення ПЗ, годин;

$З_{пр}$ – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$З_{мч} = t_{опр} C_{мч} + t_д \cdot C_{мч} = 0.98 \cdot (3.36 \cdot 11.8125) = 14.86$, грн. (5.11)

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P_p \cdot C_e + \frac{Ф_{зал} \cdot H_a + K_{лпз} \cdot H_{апз}}{F_p} = 0.5 \cdot 1.68 + \frac{2700 \cdot 0.1}{1920} = 0.98, \text{ грн/год,} \quad (5.12)$$

де P – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 1.68 грн/кВт·година; $Ф_{перв}$– первісна вартість ПК на початок року, 2700 грн.; H_a – річна норма амортизації на ПК, 0.1 частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920

год).

Отже, $K_{пз} = 395.93 + 14.86 = 410.79$ грн (5.13)

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ тис. грн} \quad (5.14)$$

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Таблиця 5.1 Вартість закупівлі апаратного забезпечення та допоміжних матеріалів

Назва комплектуючих	Вартість, грн.
Процесор: Intel(R) Celeron(R) CPU 1000M @	1000
Системна плата: MSI H110M PRO-VHL	700
ОЗУ для Intel: GOODRAM 1GB DDR4 2133MHZ	300
Жесткий диск: TOSHIBA HDWD110UZSVA	500
Корпус з блоком живлення: CHIEFTEC LT-01B-500GPA 500W	200
Разом	2700

$К_{аз}$ = 2.7 тис. грн.

Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень що складають 1 тис. грн; $К_{навч}$ =1 тис. грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають, 0.5 тис. грн. $К_{н}$ = 0.5 тис. грн.

К = 0.41979 + 2.7 + 1 + 0.5 = 4.619 тис. грн. (5.15)

3.1 Експлуатаційні витрати:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_{тос} \qquad (5.16)$$

де витрати на навчання адміністративного персоналу й кінцевих користувачів($С_н$). визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації – 1 тис. грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) – 20% або 922 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} = 3200\ 12 + 3200\ \ 0.22\ \ 12 = 46\ \ 848 \text{ грн.} \qquad (5.17)$$

де $З_{осн}$, $З_{дод}$ – основна мінімальна заробітна плата на 01.12.2017, грн на рік.

Єдиний соціальний внесок – 0.22, частки одиниці;

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0.4 \cdot 365 \cdot 24 \cdot 1.68 = 3\ 433.92 \text{ грн,} \qquad (5.18)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення вторгнень визначаються у відсотках від вартості капітальних витрат 2%. А саме:

$C_{тос}$ = К · 0.2 = 92.39 грн

Ск = 1 + 0.922 + 46.848 +3.43392 + 0,09239 = 52,29631 , тис. грн. (5.19)

4.2 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина *відвернених втрат*, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Вихідні дані:

$t_п$ =60 годин – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$=30 годин – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$=15 годин – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної

мережі, годин;

$З_о$=3200 грн – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$ 4000 грн – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$=1 – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ = 3 – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О = 200 000 грн – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$П_{зч}$ = 1000 грн – вартість заміни встаткування або запасних частин, грн; I=1 – число атакованих вузлів або сегментів корпоративної мережі;

N = 14 – середнє число можливих атак на рік. (В минулому році було 20)

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \text{ грн.} \qquad (5.20)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності 3 співробітників з ЗП атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за 60 годин простою внаслідок атаки:

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (5.21)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати 4000 грн 3 співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$=30:

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum\sum U * N * I = 11272.26 \cdot 24 \cdot 1 = 270534.24 \text{ грн.} \quad (5.24)$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$E = B \cdot R - C = 270534.24 \quad 0.7 - 52296.31 = 137077.14$ грн, (5.25)

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис.

г
р
н
.

4.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{E}{K} = \frac{58172,14}{4619.79} = 29.67$$, частки одиниці, (5.26)

Е – загальний ефект від впровадження системи інформаційної безпеки, грн; К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн. Термін окупності:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{12.59} = 0.03$$ років. (5.27)

Розділ 6. Охорона праці та безпека в надзвичайних ситуаціях

6.1 Охорона праці

Робота щодо розробки методики захисту баз даних проводяться в кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп'ютери (ПК) та периферійні пристрої. Під час роботи з персональним комп'ютером можуть виникнути такі небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом яких може бути принтер, сканер), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу.

Особливу увагу під час написання роботи потрібно звертати увагу на приміщення, в яких виконувалась, як сама робота, так і її оформлення.

Розробка методики захисту інформації супроводжуються значним напруженням трудового процесу, певним емоційним напруженням та потребують належного психофізіологічного мікроклімату у колективі. Таким чином, здійснюючи характеристику процесу праці, необхідно звернути увагу на такі аспекти:

- фізичне навантаження (переважна робоча поза, ергономічна характеристика робочого місця, категорія робіт за ступенем важкості трудового процесу);
- нервово-психічна напруженість праці (напруженість зору, кількість і складність оброблювальної інформації, тривалість зосередженого спостереження, кількість об'єктів спостереження, наявність та тривалість технологічних перерв протягом робочого дня, шумове забруднення).

Під час виконання даної роботи використовують персональні комп'ютери та периферійні пристрої (лазерні та струменеві друкарки, копіювальну техніку, сканери). Негативний вплив цих пристроїв на організм людини виникає через неадекватне (надто велике або надто мале) навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і прояву стресових реакцій. Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м'язово-скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок. Роботу персональних комп'ютерів та периферійних пристроїв супроводжує виділення багатьох хімічних речовин, зокрема озону, оксидів нітрогену та аерозолів (високодисперсних частинок тонера).

Обов'язковою умовою є те, що на робочому місці повинні знаходитись лише ті технічні засоби, які необхідні для

виконання робочого завдання, і розміщуватися вони повинні в межах досяжності з метою виключення частих нахилів і поворотів корпусу людини, що працює.

З урахуванням характеру трудової діяльності, напруженості та важкості праці з використанням ПК під час основної роботи за восьми годинної робочої зміни встановлюють додаткові регламентовані перерви:

- для розробників програм тривалістю 15 хв через кожну годину роботи;
- для операторів персональних комп'ютерів тривалістю 15 хв через дві години роботи;
- для операторів комп'ютерного набору тривалістю 10 хв через кожну годину роботи.

За жодних умов безперервна робота з ПК не повинна перевищувати чотири години. Також одним з важливих чинників, від якого залежать працездатність і здоров'я людини, – це освітлення. Світло регулює всі функції людського організму і впливає на психологічний стан і настрій, обмін речовин, гормональний фон і розумову активність. Найздоровіше освітлення забезпечує природне світло. Його ефективне використання можливе, якщо глибина приміщень не перевищує 6 м. Окрім того, хорошим вирішенням можуть будуть скляні перегородки, що забезпечують зорову і звукову ізоляцію, але в той же час не перешкоджають проникненню природного світла.

Особливо важливим є дотримання заходів особистої гігієни на робочому місці, а саме щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому

місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього розпорядку.

Під час виконання робіт операторського типу, пов’язаних з нервово-емоційним напруженням, у приміщеннях під час роботи з екранними пристроями, на пультах і постах керування технологічними процесами та в інших приміщеннях мають дотримуватися оптимальні умови мікроклімату відповідно до

Як відомо, тривала робота за комп’ютером та з документами при недостатньому рівні освітленості може призвести до значного перенапруження зору, тому вимоги до освітлення є досить важливими.

Додатково, окрім вже перелічених документів, вимоги до освітлення встановлено ДБН В.2.5-28:2018 «Природне і штучне освітлення», затвердженими наказом Мінрегіону від 28.02.2019.

Мікроклімат виробничих приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати вимогам Санітарних норм мікроклімату виробничих приміщень ДСН 3.3.6.042-99, затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 42 (далі - ДСН 3.3.6.042-99).

Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і

навколишнім середовищем (з урахуванням виду роботи) та відповідати вимогам ДСанПІН 3.3.2.007-98.

Під час виконання робіт операторського типу, пов'язаних з нервово-емоційним напруженням, у приміщеннях під час роботи з екранними пристроями, на пультах і постах керування технологічними процесами та в інших приміщеннях мають дотримуватися оптимальні умови мікроклімату відповідно до вимог ДСН 3.3.6.042-99.

6.2 Ергономічні вимоги до робочого міся користувача персональним комп'ютером(ПК)

Робоче місце – це зона трудових дій працівника, обладнана для виконання певних операцій виробничого процесу, де взаємодіють три головні елементи праці – предмет, засоби і суб'єкт праці. На одному робочому місці можуть працювати два або кілька працівників, які виконують спільне завдання. Наукова організація робочого місця передбачає створення працівникові всіх необхідних умов для високопродуктивної і високоякісної праці за менших фізичних зусиль і мінімальному нервовому напруженні та передбачає:

- оснащеність робочого місця відповідним основним і допоміжним устаткуванням, технологічною і організаційною оснасткою;

- раціональне планування, тобто найзручніше і найефективніше розміщення усіх елементів робочого місця для трудового процесу;
- створення безпечних і здорових умов праці.

Просторова організація робочого місця повинна забезпечувати:

- відповідність планування робочого місця санітарним і протипожежним нормам і вимогам;
- безпеку працівникам;
- відповідність просторових відношень між елементами робочого місця, антропометричними, біомеханічними, фізіологічними, психофізіологічними і психічними можливостями людини, що працює;
- можливість виконання основних і допоміжних операцій в робочому положенні, що відповідає специфіці трудового процесу, в раціональній робочій позі і з використанням найбільш ефективних прийомів праці;
- вільне переміщення працівника за оптимальними траєкторіями;
- достатню площу для розміщення обладнання, інструменту, засобів контролю, деталей.

Просторові та розмірні співвідношення між елементами робочого місця повинні дозволяти:

- розміщення працівника з урахуванням робочих рухів і переміщень згідно з технологічним процесом;
- оптимальний огляд джерела візуальної інформації;
- зміну робочої пози і положення;

- раціональне розміщення основних і допоміжних засобів праці.

Обов’язковою умовою є те, що на робочому місці повинні знаходитись лише ті технічні засоби, які необхідні для виконання робочого завдання, і розміщуватися вони повинні в межах досяжності з метою виключення частих нахилів і поворотів корпусу людини, що працює.

Під час роботи з персональним комп’ютером повинні бути дотримані певні вимоги.

Вимоги до приміщення. Площу приміщень, в яких розташовують персональні комп’ютери, визначають згідно з чинними нормативними документами з розрахунку на одне робоче місце, обладнане ПК:

- площа − менше 6,0 м^2;
- об’єм − не менше 20,0 м^3, з урахуванням максимальної кількості осіб, які одночасно працюють у зміні;
- робочі місця повинні бути розташовані на відстані не менше ніж 1 м від стіни з вікном;
- відстань між тильною поверхнею одного комп’ютера та екраном іншого не повинна бути меншою 2,5 м;
- прохід між рядами робочих місць має бути не меншим 1 м.

Вимоги до організації робочого місця з ПК. Конструкція робочого місця користувача ПК має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками:

- ступні ніг − на підлозі або на підставці для ніг;

- стегна − в горизонтальній площині;
- передпліччя − вертикально;
- лікті − під кутом 70–90° до вертикальної площини;
- зап’ястя зігнуті під кутом не більше 20° відносно горизонтальної площини;
- нахил голови – 15-20° відносно вертикальної площини.

Якщо користування ПК є основним видом діяльності, то ПК і його периферійні пристрої (принтер, сканер тощо) розміщується на основному робочому столі, як правило, з лівого боку. Якщо використання ПК є періодичним, то він, як правило, розміщується на приставному столі, переважно з лівого боку від основного робочого столу.

Робоче сидіння (сидіння, стілець, крісло) користувача ПК повинно мати такі основні елементи: сидіння, спинку, стаціонарні або знімні підлокітники. У конструкцію сидіння можуть бути введені додаткові елементи, що не є обов’язковими: підголовник та підставка для ніг. Робоче сидіння користувача ПК повинно бути підйомно поворотним, таким, що регулюється за висотою, кутом нахилу сидіння та спинки, за відстанню спинки до переднього краю сидіння, висотою підлокітників. Регулювання кожного параметрама є бути незалежним, плавним або ступінчатим, мати надійну фіксацію.

Монітор та клавіатура мають розташовуватися на оптимальній відстані від очей користувача, але не ближче 600 мм, з урахуванням розміру алфавітно-цифрових знаків та символів. Розташування монітору має забезпечувати зручність

зорового спостереження у вертикальній площині під кутом ±30 град. від лінії зору працівника. Клавіатуру слід розміщувати на поверхні столу або на спеціальній регульованій за висотою, робочій поверхні окремо від столу на відстані 100–300 мм від краю, ближчого до працівника. Кут нахилу клавіатури має бути в межах 5–15 градусів.

Режим праці та відпочинку користувачів ПК встановлюють з урахуванням психофізіологічної напруженості їхньої праці, динаміки функціонального стану систем організму та працездатності. Раціональний режим праці та відпочинку передбачає запровадження регламентованих перерв, рівномірний розподіл навантажень протягом робочого дня, регулярні комплекси вправ для очей, рук, хребта, поліпшення мозкового кругообігу та психофізіологічне розвантаження.

З урахуванням характеру трудової діяльності, напруженості та важкості праці з використанням ПК під час основної роботи за восьми годинної робочої зміни встановлюють додаткові регламентовані перерви:

- для розробників програм тривалістю 15 хв через кожну годину роботи;
- для операторів персональних комп’ютерів тривалістю 15 хв через дві години роботи;
- для операторів комп’ютерного набору тривалістю 10 хв через кожну годину роботи.

За жодних умов безперервна робота з ПК не повинна перевищувати чотири години. Також одним з важливих чинників, від якого залежать працездатність і здоров’я людини, –

це освітлення. Світло регулює всі функції людського організму і впливає на психологічний стан і настрій, обмін речовин, гормональний фон і розумову активність. Найздоровіше освітлення забезпечує природне світло. Його ефективне використання можливе, якщо глибина приміщень не перевищує 6 м. Окрім того, хорошим вирішенням можуть будуть скляні перегородки, що забезпечують зорову і звукову ізоляцію, але в той же час не перешкоджають проникненню природного світла.

Ще варто звернути увагу на такий чинник, як шум , що часто є причиною зниження рівня працездатності, підвищення рівня загальної та професійної захворюваності, частоти виробничих травм. Шум як стрес-чинник є загальнобіологічним подразником, який негативно впливає на всі органи і системи організму.

Рівень шуму, що супроводжує роботу користувачів персональних комп’ютерів (зумовлений як роботою системних блоків, клавіатури, так і друкуванням на принтерах, а також зовнішніми чинниками), коливається в межах 50–65 дБА. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. Тому на практиці рекомендують знижувати фактичний рівень шуму у приміщеннях, де створюють комп’ютерні програми, виконують теоретичні та творчі роботи.

Особливо важливим є дотримання заходів особистої гігієни на робочому місці, а саме щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці

необхідно дотримуватись вимог правил внутрішнього розпорядку.

6.3 Безпека в надзвичайних ситуаціях

Надзвичайна ситуація – порушення нормальних умов життя і діяльності людей на об’єкті або території, спричинене аварією, катастрофою, стихійним лихом чи іншою небезпечною подією, яка призвела (може призвести) до загибелі людей або значних матеріальних втрат.

Серед надзвичайних ситуацій техногенного характеру домінують пожежі та вибухи, а серед небезпек природного характеру – аномальні гідрометеорологічні явища та медико-біологічні загрози. Пожежа – це неконтрольоване горіння, яке супроводжується виділенням тепла, світла, диму та інших продуктів. Горіння виникає за таких трьох умов: наявності окисника, наявності горючої речовини, наявності температури, за якої горюча речовина може самостійно горіти. Якщо немає хоча б однієї із цих умов, горіння стає неможливим. На цьому постулаті ґрунтується переважна більшість профілактичних заходів, спрямованих на відвернення пожеж.

Описуючи пожежовибухонебезпечність середовища варто відзначити: пожежовибухонебезпечні властивості речовин і матеріалів, які використовують під час виконання дипломних (кваліфікаційних) робіт (горючість, верхня та нижня концентраційні межі загоряння, температура запалення).

Головними причинами виникнення пожеж та вибухів

є:

- порушення пожежних норм і правил;
- порушення правил встановлення та експлуатації систем енергопостачання, опалення, вентиляції;
- порушення правил експлуатації електричного та газового обладнання;
- порушення правил зберігання пожежовибухонебезпечних матеріалів;
- використання відкритого вогню в заборонених місцях;
- погане знання персоналом протипожежних правил;
- не обережна поведінка з вогнем.

Серед загальних вимог до евакуаційних шляхів та виходів необхідно відмітити, що ними можуть бути дверні отвори, якщо вони ведуть з приміщень:

- безпосередньо назовні;
- на сходовий майданчик з виходом назовні безпосередньо або через вестибюль;
- у прохід або коридор з безпосереднім виходом назовні або на сходовий майданчик;
- у сусідні приміщення того ж поверху, що не містять виробництв, які належать за вибухопожежною та пожежною небезпекою до категорій А, Б і В та мають безпосередній вихід назовні або на сходовий майданчик.

Для безпечної евакуації шляхи та виходи мають відповідати таким вимогам:

- евакуаційні шляхи і виходи повинні утримуватися вільними, не захаращуватися та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщеннях;
- кількість та розміри евакуаційних виходів, їхні конструктивні рішення, умови освітленості, забезпечення не задимленості, протяжність шляхів евакуації, їхнє оздоблення повинні відповідати протипожежним вимогам будівельних норм;
- у приміщенні, яке має один евакуаційний вихід, дозволяється одночасно розміщувати не більше 50 осіб, а у разі перебування в ньому понад 50 осіб повинно бути щонайменше два виходи, які відповідають вимогам будівельних норм;
- двері на шляхах евакуації повинні відчинятися в напрямку виходу з будівель (приміщень) і замикатися лише на внутрішні запори, які легко відмикаються.

Розділ 7. Екологія

7.1 Гости і стандарти на монітори і ПЕОМ

Відеотермінали ЕОМ, ПЕОМ, спеціальні периферійні пристрої ЕОМ і устаткування для обслуговування, ремонту та налагодження ЕОМ мають відповідати вимогам чинних в Україні стандартів та нормативних актів з охорони праці. Аналогічне обладнання закордонного виробництва додатково має відповідати вимогам стандартів держав-виробників і мати про це відповідну позначку на корпусі, у паспорті або іншій експлуатаційній документації та сертифікат України, що засвідчує його відповідність вимогам щодо забезпечення безпеки праці, життя і здоров'я людини. Без наявності сертифіката, інструкції, іншої експлуатаційної документації заборонено використовувати для виробничих потреб нове обладнання закордонного виробництва.

У разі відхилення від вимог нормативних документів можливість використання обладнання узгоджують, з Держгірпромнаглядом, Держстандартом і організацією-замовнинком до укладання контракту на постачання.

Табл. 6.1 **Вимоги до відеотерміналів**

Примечание [CO1]:

Найменування параметра	Значення параметра
Яскравість знака (яскравість фону), кд/ м^2	від 35 до 120
Зовнішня освітленість екрана, лк	від 100 до 250
Контраст (для монохромних зображень)	від 3:1 до 1,5:1
Нерівномірність яскравості в робочій зоні екрана	не більше 1.7:1
Відхилення форми робочої зони екрана від прямокутності: - по горизонталі та вертикалі	не більше 2 %
- по діагоналі	не більше 4 % від відношення суми коротких сторін до суми довгих
Різниця довжин рядків або стовпчиків	не більше 2 % віл середнього значення
Розмір мінімального елемента зображення (пікселя) для монохромних зображень, мм	0,3

6.2 Робота з банками екологічної інформації

Інформація про навколишнє середовище відіграє важливу роль не лише у формуванні політики управління екологічним середовищем, а й у процесі прийняття рішень, спрямованих на захист та поліпшення навколишнього середовища для підтримання доброї якості живих істот.

Зрозумівши це значення екологічної інформації уряд Індії створив екологічну систему ENVIS, як планову програму. У центрі уваги ENVIS з моменту створення було надано інформацію про навколишнє середовище особам, які приймають рішення, планувальникам політики, науковцям та інженерам, науково-дослідним працівникам по всій країні.

Для реалізації цієї програми були створенні команди зацікавлених установ та організацій в країні, які активно долучаються до роботи, що стосується різних предметних областей навколишнього середовища. Таким чином ENVIS розробляється як децентралізована система з розподіленою мережею таких установ та організацій. Координаційний центр знаходиться в Міністерстві охорони навколишнього середовища.

ENVIS був визнаний Національним координаційним центром NFP для INFOTERRA, глобальної екологічної інформаційної мережі Програми ООН з навколишнього середовища UNEP.

Законодавство України потребує змін не лише в стандартах збереження екологічної інформації, а й системі організації збору

та збереження даних у єдину систему (банк даних). Стандарти збору інформації дадуть можливість швидко і ефективно опрацьовувати банк даних, в результаті яких швидко і якісно приймати рішення про внесення можливих змін для покращення екологічної ситуації в Країні.

На сьогодні національне законодавство відносить до екологічної інформації відомості про:

- стан навколишнього природного середовища чи його об'єктів – землі, води, надр, атмосферного повітря, рослинного та тваринного світу та рівні їх забруднення;
- біологічне різноманіття і його компоненти, включаючи генетично видозмінені організми та їх взаємодію з об'єктами навколишнього природного середовища;
- джерела, фактори, матеріали, речовини, продукцію, енергію, фізичні фактори (шум, вібрацію, електромагнітне випромінювання, радіацію), які впливають або можуть вплинути на стан навколишнього природного середовища та здоров'я людей;
- загрозу виникнення і причини надзвичайних екологічних ситуацій, результати ліквідації цих явищ, рекомендації щодо заходів, спрямованих на зменшення їх негативного впливу на природні об'єкти та здоров'я людей;
- екологічні прогнози, плани і програми, заходи, у тому числі адміністративні, державну екологічну політику, законодавство про охорону навколишнього природного середовища;

- витрати, пов'язані із здійсненням природоохоронних заходів за рахунок фондів охорони навколишнього природного середовища інших джерел фінансування, економічний аналіз, проведений у процесі прийняття рішень з питань, що стосуються довкілля (ст. 25 Закону «Про охорону навколишнього природного середовища»).

Основними джерелами інформації є: дані моніторингу довкілля, кадастрів природних ресурсів, реєстри, автоматизовані банки даних, архіви, а також довідки, що видаються уповноваженими органами державної влади, органами місцевого самоврядування, громадськими організаціями, окремими посадовими особами.

Основним джерелом первинної інформації з екології середовища є статистична звітність, яка складається з багатьох показників і контролюються державою. Банки екологічної статистичної інформації - це вторинна накопичена інформація, певним чином упорядкована чи опрацьована. Оперативна, якісна і точна обробка великих масивів статистичної інформації може бути виконана лише з використанням сучасних засобів обчислювальної техніки. Наявність потужних, надійних і разом з тим простих в експлуатації програмних продуктів статистичного аналізу звільняє дослідника від рутинних операцій, розширює сферу застосування статистичних методів в різних галузях людської діяльності, сприяє появі якісно нових можливостей статистичного аналізу і моделювання даних. Використання пакетів прикладних програм - це єдиний реальний практичний

інструмент розв'язування задач багатофакторного кореляційно-регресійного та аналізу в багатовимірному просторі.

Висновки

У першому розділі було проведена така робота, як огляд літератури та збір даних. Аналітика про кібератаки за кінець 2019 року розповідає про необхідність створення методики захисту інформації в базах даних та дотримання стандартів безпечного програмування систем web-додатків інтернет-суспільством.

Отже, основними принципами захисту інформації є її конфіденційність, цілісність і достовірність. Захист інформації потребує централізованості, плановості, конкретики і цілеспрямованості, активності, надійності і універсальності, а також мати економічний ефект. Захист інформації існує на рівні робочого місця користувача, на рівні підрозділу і всього підприємства. Є чотири групи захисту інформації: технічні, програмні, змішані і організаційні. Найбільш вразливою є інформація в інтернеті, а тому рекомендується використовувати надійні паролі, шифрування даних, антивірусні програми, а також налаштовувати паролі на BIOS для її ефективного захисту.

Кіберзагрози –- це сукупність факторів і умов, що створюють небезпеку порушення інформаційної безпеки. Цілеспрямовані атаки переважають над масовими і становлять 59% усіх атак. Більшість з них спрямована на викрадення інформації у фізичних чи юридичних осіб для отримання фінансової вигоди. Серед найпоширеніших загроз інформаційній

безпеці варто відзначити використання шкідливого ПЗ, соціальну інженерію, хакінг, експлуатації веб-вразливостей, підбір облікових даних.

Наведені приклади показують гостру актуальність обраної проблеми та які наслідки за собою вона має. Проблема захисту інформації розгалужена та багатогранна. Має безліч суміжних питань.

В другому розділі розглянуто типи атак та їх приклади на SQL сервера. Розглянуто базовий приклад вразливостей SQL-сервера завдяки якому можливо отримати повний адміністративний доступ до сервера.

Також розглянуто методику боротьби з sql-ін’єкціями засобами плейсхолдерів. Плейсхолдери - це змінні які чітко вказують що і як повино бути передано клієнтом на сервер, без можливості вставити в них ін’єкцію. В даному розділі описані правила користування плейхолдерами, випадки їх використання та переваги.

В третьому розділі ми розглянули такі методи захисту даних як: авторизація методом TOTP, реалізація безпеки в розподілених базах даних за допомогою технології блокчейн та загальні правила безпеки баз даних.

Метод TOTP є одним з найкращих способів для захищеної авторизації користувачів у будь-які ресурси, в тому числі доступи до баз даних. Даний метод базується на часі та хешуванні даних для авторизації. Дані рекомендується передавати у захищеному

форматі, із використанням конкретного типу шифрування, наприклад RSA.

Реалізація технології блокчейн підходить для використання в розподілених базах даних. Завдяки цьому методу можливо реалізувати захист від змін чи фальсифікації даних в базах даних, що унеможливлює їх зміну, навіть при наявному доступі до бази даних. На сьогодні цей метод широко застосовується для криптовалют, але також і цю технологію блокчейн розвивають для її використання у хмарних базах даних, наприклад Microsoft Azure.

У третьому підрозділі розглянуто методи та рекомендації щодо захисту баз даних, а також базова інформація щодо захисту від можливих атак на інформації і способи її збереження. Якщо використовувати запропоновану мною методику - ви ліквідовуєте можливість будь-яких sql-атак.

Узагальнюючи всю роботу ми отримуємо методику взаємодій декількох сучасних способів захисту баз даних. Використовуючи кожен з методів ми отримуємо універсальну формулу захисту від будь-як актуальних типів атак на бази-даних.

Бібліографія

1. Баранчиков А.И., Баранчиков П.А., Пилькин А.Н. Алгоритмы и модели доступа к записям БД. М.: Горячая линия-Телеком, 2011. 182 с. . – Дата перегляду: 5.12.2019
2. Безопасность web-приложений: а нужно ли тестирование?. – [Електронний ресурс] – Режим доступу: http://www.jetinfo.ru/stati/bezopasnost-web-prilozhenij-a-nuzhno-li-testirovanie. – Дата перегляду: 5.12.2019
3. Блокчейн // tadviser – [Електронний ресурс] – Режим доступу: http://www.tadviser.ru/index.php/Статья:Блокчейн_(Blockchain) . – Дата перегляду: 5.12.2019
4. Блокчейн против базы данных: понимание различий между ними // 101blockchain. – [Електронний ресурс] – Режим доступу: https://101blockchains.com/ru/блокчейн-против-базы-данных/. – Дата перегляду: 5.12.2019
5. Бортовчук Ю.В., Крылова К.А., Ермолаева Л.В. Информационная безопасность в современных системах управления базами данных

Современные проблемы экономического и социального развития. 2010. № 6. С.224-225. . – Дата перегляду: 5.12.2019

6. Горбачевская Е.Н., Катьянов А.Ю., Краснов С.С. Информационная безопасность средствами СУБД Oracle // Укр. ВУиТ. 2015 № 2 (24). С.72-85. . – Дата перегляду: 5.12.2019
7. Защита информации - актуальность и методы // kak-bog.ru. – [Електронний ресурс] – Режим доступу: http://kak-bog.ru/zashchita-informacii-aktualnost-i-metody. – Дата перегляду: 5.12.2019
8. Защита от SQL-инъекций в PHP и MySQL // Хабрахабр. – [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/148701/. – Дата перегляду: 5.12.2019
9. Зегжда П.Д. Обеспечение безопасности информации в условиях создания единого информационного пространства // Защита информации. Инсайд. 2007. № 4 (16). С.28-33. . – Дата перегляду: 5.12.2019
10. Информационная безопасность бизнеса. Исследование текущих тенденций в области информационной безопасности бизнеса. 2014.. – [Електронний ресурс] – Режим доступу: http://media.kaspersky.com/pdf/IT_risk_ report_Russia_2014.pdf. . – Дата перегляду: 5.12.2019
11. Как понять нужно ли интегрировать blockchain в ваш продукт? // Хабрахабр. – [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/web_payment_ru/blog/301972/. – Дата перегляду: 30.11.2019

12. Катренко Л. А., Пістун І. П. Охорона праці в галузі освіти: Навч. Посіб. – Суми: ВДТ «Університетська книга», 2004. – 304 с. . – Дата перегляду: 30.11.2019
13. Концепция одноразовых паролей в системе аутентификации // bytemag. – [Електронний ресурс] – Режим доступу: https://www.bytemag.ru/articles/detail.php?ID=9101. – Дата перегляду: 30.11.2019
14. Методы защиты баз данных: защита паролем, шифрование, разграничение прав доступа. – [Електронний ресурс] – Режим доступу: https://habrahabr.ru/post/149238/. – Дата перегляду: 30.11.2019
15. Методы защиты баз данных: защита паролем, шифрование, разграничение прав доступа. – [Електронний ресурс] – Режим доступу: https://studopedia.ru/9_88862_aktualnost-zashchiti-bazi-dannih-metodi-. – Дата перегляду: 30.11.2019
16. Минимальная заработная плата // Статистика. – [Електронний ресурс] – Режим доступу: https://index.minfin.com.ua/labour/salary/min/. – Дата перегляду: 30.11.2019
17. Охорона праці [З.М. Яремко, С.В. Тимошук, О.І. Третяк та ін.:]; за ред. З.М. Яремка. – Львів: ВЦ ЛНУ імені Івана Франка, 2010. – 310 с. . – Дата перегляду: 30.11.2019
18. Охорона праці та промислова безпека: Навч. посіб. / К. Н. Ткачук, В. В. Зацарний, Р. В. Сабарно, С. Ф. Каштанов, Л. О. Мітюк, Л. Д. Третьякова, К. К.Ткачук, А.В. Чадюк. За ред. К.Н. Ткачука і В.В. Зацарного. – К., 2009. – 454 с. . – Дата перегляду: 30.11.2019

19. Охорона праці та промислова безпека: Навч. посіб. / К. Н. Ткачук, В. В. Зацарний, Р. В. Сабарно, С. Ф. Каштанов, Л. О. Мітюк, Л. Д. Третьякова, К. К.Ткачук, А.В. Чадюк. За ред. К.Н. Ткачука і В.В. Зацарного. – К., 2009. – 454 с. . – Дата перегляду: 30.11.2019
20. Подборка материалов по SQL Injection. – [Електронний ресурс] – Режим доступу: http://injection.rulezz.ru/. – Дата перегляду: 30.11.2019
21. Полтавцева М.А. Задача хранения прав доступа к данным в СУБД на примере Microsoft SQL Server // Актуальные направления фундаментальных и прикладных исследований: матер. V Междунар. научно-практич. конф. 2015 С. 118-120. . – Дата перегляду: 30.11.2019
22. Поляков А.М. Безопасность Oracle глазами аудитора: нападение и защита.М.: ДМК Пресс, 2014. 336 с. . – Дата перегляду: 30.11.2019
23. Потапов А.Е., Манухина Д.В., Соломатина А.С., Бадмаев А.И., Яковлев А.В., Нилова А.С. Безопасность локальных баз данных на примере SQL Server Compact // Укр. Тамбов. ун-та. Серия: Естественные и технические науки. 2014. № 3. С. 915-917. . – Дата перегляду: 30.11.2019

24. Смирнов С.Н. Безопасность систем баз данных. М.: Гелиос АРВ, 2007. 352 с. . – Дата перегляду: 20.11.2019
25. Ткаченко Н.А. Реализация монитора безопасности СУБД MySQL в dbf / dam системах // ПДМ. Дополнение. 2014. № 7. С. 99-101. . – Дата перегляду: 20.11.2019

26. Ткаченко Н.А. Реализация монитора безопасности СУБД MySQL в dbf / dam системах // ПДМ. Дополнение. 2014. № 7. С. 99-101. . – Дата перегляду: 20.11.2019
27. Трахтенберг І. М., Коршун М. М., Чебанова О. В. Гігієна праці та виробнича санітарія. – К.: Основа, 1997. – 464 с. . – Дата перегляду: 20.11.2019
28. Уязвимость CVE-2017-8570 // codeby. – [Електронний ресурс] – Режим доступу: http://catcut.net/gXVE. – Дата перегляду: 20.11.2019
29. Эргономика / Адамчук В. В., Варна Т. П., Воротникова В. В.и др.; Под ред. проф. Адамчука В. В. –М.: ЮНИТИ-ДАНА, 1999. –254 с. . – Дата перегляду: 20.11.2019
30. Эргономика / Адамчук В. В., Варна Т. П., Воротникова В. В.и др.; Под ред. проф. Адамчука В. В. –М.: ЮНИТИ-ДАНА, 1999. –254 с. . – Дата перегляду: 20.11.2019
31. Яремко З. М. Безпека життєдіяльності. Навч. посібник.–Львів: Видавничий центр ЛНУ імені Івана Франка, 2005. –301 с. . – Дата перегляду: 20.11.2019
32. 11 Steps to Secure SQL // upguard. – [Електронний ресурс] – Режим доступу: https://www.upguard.com/blog/11-steps-to-secure-sql. – Дата перегляду: 14.11.2019
33. Are SQL placeholder safe? // Codecademy. – [Електронний ресурс] – Режим доступу: http://catcut.net/ITVE. – Дата перегляду: 14.11.2019
34. Authentication, authorization, privileges, and auditing // IBM. – [Електронний ресурс] – Режим доступу: http://catcut.net/O1WE. – Дата перегляду: 14.11.2019

35. Blockchain – распределенная база данных // nvdaily. – [Електронний ресурс] – Режим доступу: https://nvdaily.ru/info/116465.html. – Дата перегляду: 14.11.2019
36. Blockchain technology — a very special kind of Distributed Database // Medium. – [Електронний ресурс] – Режим доступу: https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118. – Дата перегляду: 14.11.2019
37. Burtescu E. Database security attacks and control me - thods. Journ. of Applied Quantitative Methods 2009, vol. 4, no. 4, pp. 449-454 . – Дата перегляду: 04.11.2019
38. Database Security Technical Implementation Guide (STIG). // US Department of Defense. Vers. 7. Release 1. 2004. – [Електронний ресурс] – Режим доступу: https://www.computer.org/cms/s2esc/s2esc_excom/Minutes/2005-03/ DISA% 20STIGs / DATABASE-STIG- V7R1.pdf. – Дата перегляду: 04.11.2019
39. Database SQL Language Reference // Oracle.com. – [Електронний ресурс] – Режим доступу: http://catcut.net/7VVE. – Дата перегляду: 04.11.2019
40. How To Prevent SQL Injection Attacks // Назва ресурсу. – [Електронний ресурс] – Режим доступу: http://catcut.net/JWVE. – Дата перегляду: 04.11.2019
41. How to protect your website agains SQL injection attacks // sitepoint. – [Електронний ресурс] – Режим доступу: http://catcut.net/XWVE. – Дата перегляду: 04.11.2019

42. INFOWATCH // Статистика атак на веб додатки – [Електронний ресурс] – Режим доступу: Посилання на ресурс https://www.infowatch.ru/analytics/leaks_monitoring/19302. – Дата перегляду: 04.11.2019
43. INFOWATCH // Статистика атак на веб додатки – [Електронний ресурс] – Режим доступу: Посилання на ресурс https://www.infowatch.ru/analytics/leaks_monitoring/19481. – Дата перегляду: 30.10.2019
44. Introducing SQL Server Security // ITproToday – [Електронний ресурс] – Режим доступу: http://catcut.net/N1WE. – Дата перегляду: 17.10.2019
45. Lesov P. Database security: a historical perspective.perspectiv. 2010. URL: http://arxiv.org/ftp/arxiv/papers/1004/1004.4022.pdf. – Дата перегляду: 17.10.2019
46. Murray M.C. Database security: what students need to know. JITE: IIP, vol. 9, 2010 pp. 61-77. . – Дата перегляду: 17.10.2019
47. OATH Submits TOTP: Time-Based One Time Password Specification to IETF // WebCite. – [Еле. – Дата перегляду: 30.10.2019ктронний ресурс] – Режим доступу: http://catcut.net/yXVE
48. OATH: yesterday, today, and tomorrow // LWN.net. – [Електронний ресурс] – Режим доступу: https://lwn.net/Articles/419968/. – Дата перегляду: 30.10.2019
49. Overview of SQL Server Security // Microsoft. – [Електронний ресурс] – Режим доступу: http://catcut.net/C1WE. – Дата перегляду: 30.10.2019

50. PHP mySQL Prepared Statements Tuturial to Prevent SQL Injection // Websitebeaver. – [Електронний ресурс] – Режим доступу: http://catcut.net/ZVVE. – Дата перегляду: 30.10.2019
51. PHP PDO prepared Statements Tuturial to Prevent SQL Injection // Websitebeaver – [Електронний ресурс] – Режим доступу: http://catcut.net/bWVE. – Дата перегляду: 21.10.2019
52. PL/SQL placeholder duplication // dba-oracle. – [Електронний ресурс] – Режим доступу: http://www.dba-oracle.com/t_plsql_placeholder_duplication.htm. – Дата перегляду: 21.10.2019
53. Placeholder SQL // osisoft. – [Електронний ресурс] – Режим доступу: http://catcut.net/ATVE. – Дата перегляду: 21.10.2019
54. Placeholders in SQL query // perlmonks. – [Електронний ресурс] – Режим доступу: https://www.perlmonks.org/?node_id=1103424. – Дата перегляду: 21.10.2019
55. PostgreSQL vs Oracle. – [Електронний ресурс] – Режим доступу: http://www.jetinfo.ru/stati/bezopasnost-web-prilozhenij-a-nuzhno-li-testirovanie. – Дата перегляду: 21.10.2019
56. Protecting against SQL injection // HACKSPLAINING. – [Електронний ресурс] – Режим доступу: https://cutt.ly/Se6EcKG. – Дата перегляду: 17.10.2019
57. Qiu M., Davis S. Database security mechanisms and implementation. IACIS, Issues in Inform. Syst. 2002 vol. 03 pp. 529-534.
58. Rohilla S., Mittal P.K. Database Security: Threads and Challenges. Intern. Journ. of Advanced Research in Computer Science and Software Engineering, 2013, vol. 3, iss. 5, pp. 810-813. . – Дата перегляду: 17.10.2019

59. Sandhu Ravi S., Jajodia Sushil. Data and database security and controls. Handbook of Information Security Management, Auerbach Publishers, 1993, pp. 181-199. – Дата перегляду: 17.10.2019
60. SQL injection // PORTSWIGGER. – [Електронний ресурс] – Режим доступу: https://portswigger.net/web-security/sql-injection. – Дата перегляду: 14.10.2019
61. SQL injection // Wikipedia – [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/SQL_injection. – Дата перегляду: 14.10.2019
62. SQL placeholder in WHERE IN issue, inserted string fail // Stackoverflow. – [Електронний ресурс] – Режим доступу: http://catcut.net/hVVE. – Дата перегляду: 14.10.2019
63. SQL protection // habrahabr. – [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/136809/. – Дата перегляду: 14.10.2019
64. SQL Server Security Basics // netwrixBlog. – [Електронний ресурс] – Режим доступу: http://catcut.net/F1WE. – Дата перегляду: 14.10.2019
65. SQL Server Security Best Practices for 2019 // dnsstuff. – [Електронний ресурс] – Режим доступу: https://www.dnsstuff.com/sql-server-security. – Дата перегляду: 14.10.2019
66. SQL Server Security Tips // mssqltips. – [Електронний ресурс] – Режим доступу: https://www.mssqltips.com/sql-server-tip-category/19/security/. – Дата перегляду: 14.10.2019

67. SQL Wildcards // w3schools – [Електронний ресурс] – Режим доступу: https://www.w3schools.com/sql/sql_wildcards.asp. – Дата перегляду: 12.10.2019
68. TOTP // wikipedia. – [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Time-based_One-time_Password_algorithtml. – Дата перегляду: 12.10.2019
69. Use placeholders for any SQL query // Drupal.com. – [Електронний ресурс] – Режим доступу: https://cutt.ly/Qe6EchC. – Дата перегляду: 12.10.2019
70. What is the SQL injection vulnerability // netsparker. – [Електронний ресурс] – Режим доступу: http://catcut.net/QWVE. – Дата перегляду: 12.10.2019