zris-rinok-noutbukiv-i-pk-339803.html. – Назва з екрану.

12. Windows 10 Professional [Електронний ресурс] // MT : продажа лицензионного программного обеспечения : сайт компании. – Режим доступу : http://mtsoft.kiev.ua/product/windows-10-professional. – Назва з екрану.

13. Нефёдова М. Армия США покупает поддержку Win XP за миллионы долларов. 48 сек на чтение [Електронний ресурс] / Мария Нефёдова // Хакер : компьютерный ж-л. – 2015. – 24 июня. – Режим доступу : https://xakep.ru/2015/06/24/xp-for-navy/. – Назва з екрану.

14. З'явилися перші подробиці про українську операційну систему [Електронний ресурс] // ТСН.ua. Новини технологій, науки та IT на 1+1. – Режим доступу : http://tsn.ua/nauka_it/z-yavilisya-pershi-podrobici-pro-ukrayinsku-operaciynu-sistemu-351625.html. – Назва з екрану.

УПРАВЛІННЯ БЕЗПЕКОЮ БАЗ ДАНИХ І СИСТЕМ ДАНИХ У СОЦІАЛЬНИХ СИСТЕМАХ

MANAGEMENT SAFETY OF DATABASES AND DATA SYSTEMS SOCIAL

УДК 004.5(477)

Тарасюк С.В.
асистент кафедри комп'ютерних
та інформаційних технологій
і моделювання економіки
Комунальний вищий навчальний заклад
«Інститут підприємництва «Стратегія»
Дніпропетровської обласної ради»
Глеб А.С.
асистент кафедри комп'ютерних
та інформаційних технологій
і моделювання економіки
Комунальний вищий навчальний заклад
«Інститут підприємництва «Стратегія»
Дніпропетровської обласної ради»

У статті розглянуто проблематику загроз безпеці баз даних та систем даних. Проаналізовано та розглянуто основні методики організації заходів безпеки даних. Наведено певний перелік програмних засобів та конструкцій, покликаних убезпечити програмне забезпечення від зовнішніх та внутрішніх загроз.
Ключові слова: *кіберпростір, кібератаки, бази даних, безпека, програмування, сервери, Інтернет, порт, скрипт, запит.*

В статье рассмотрено проблематику угроз безопасности баз данных и систем данных. Проанализировано и рассмотрено основные методики организации мероприятий безопасности данных. Приведен определенный перечень программных средств и конструкций, призванных оградить программное обеспечение от внешних и внутренних угроз.
Ключевые слова: *киберпространство, кибератаки, базы данных, безопасность, программирование, серверы, Интернет, порт, скрипт, запрос.*

The range of problems of threats to safety of databases and systems given is considered in the article. Basic methodologies of organization of safety of data measures are analysed and considered. A certain list over of programmatic facilities and constructions called to barrier software from external and internal threats is brought.
Key words: *cyberspace, databases, safety, programming, servers, Internet, port, script, query.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення системи кібербезпеки як складової системи забезпечення національної безпеки України.

Останні кібератаки на основні ресурси державних установ таких, як: «Державна казначейська служба», система «ЄДЕБО», «Укрзалізниця», «Мінсоцполітики» призвели до порушення безперебійної роботи даних ресурсів, а також надали зловмисникам доступ до баз та банків даних з великими об'ємами конфіденційної фінансової інформації, що у свою чергу змушує всі установи та організації переглянути політику безпеки власних інформаційних ресурсів. Так, як вищі навчальні заклади також впадають в коло зору зловмисників, то актуальною є задача дослідження та управління безпекою баз даних та систем даних у соціальних системах, до яких належать ВНЗ.

Аналіз останніх досліджень. Проблемами безпеки баз даних та систем даних займалися такі зарубіжні та вітчизняні вчені, як: Б. Брила, О. Вербицький, В. Галатенко, К. Луни, О. Мелешко,

О. Нечипоренко, П. Петин, Ю. Шестаков, В. Шульженко.

Їх наукові роботи широко охоплюють проблематику безпеки даних і слугують основою для дослідження засобів та методів забезпечення безпеки даних у межах вищих навчальних закладів.

Постановка завдання. Виходячи з вищезазначеного, метою роботи є дослідження та управління безпекою баз даних і сховищ даних у системі ВНЗ та розробка заходів покликаних визначити чинники через дію яких, актуалізуються загрози кібербезпеці.

Виклад основного матеріалу дослідження. Для того, щоб глибше зрозуміти проблематику безпеки – необхідно дослідити специфіку виникнення загроз інформаційних систем, баз та банків даних і на основі отриманих результатів надати рекомендації та розробити заходи щодо недопущення загроз баз даних у корпоративній мережі ВНЗ та за її межами. Для цього використаємо аналітичні дані всесвітньої компанії Application Security, що спеціалізується на аналіз мережевих загроз [1].

Згідно з даними дослідження цієї компанії організаційні нюанси можуть представляти значніші ризики для безпеки баз даних, ніж зовнішні фактори. Як стверджують аналітики, у більшості випадків бази даних знаходяться під юрисдикцією відразу двох відділів, що займаються контролем програмно-апаратного комплексу та інформаційною безпекою організації. У зв'язку з цим може бути відсутнім консенсус у пріоритетах, а також утиск посадових обов'язків на користь одного з відділів. Крім того, багато хто з респондентів заявляли про відсутність необхідного фінансування.

Поштовхом до дослідження стало опитування, за підсумками якого з'ясувалося, що переважна більшість респондентів (81%) помітили значне зростання ризиків в області інформаційної безпеки за останні три роки. Четверо з п'яти опитаних визнали, що збільшення технічних знань, а також зухвалість кіберзлочинців і інших розробників шкідливого ПЗ, стали ключовим фактором для реалізації більш високих рівнів захисту. 51% респондентів сказали, що після оприлюднення інформації про атаки кіберзлочинних угруповань Anonymous і LulzSec їх компанії підвищили ступінь інформаційного захисту. 36% підвищили частоту проведення аудитів.

Активісти посприяли реалізації додаткових заходів безпеки в 34% компаній-респондентів, проте лише 14% відзначили, що це посприяло збільшенню фінансування відділів інформаційної безпеки. У 11% організацій провели додаткові кадрові та консультаційні заходи. Аналітики також приділили особливу увагу хмарним технологіям. За даними дослідження 19% опитаних перемістили бази даних у приватні хмари або віртуальні середовища. 2% скористалися послугами громадських хмарних сервісів. 63% респондентів вважають, що питання інформаційної безпеки є основною проблемою при роботі загальнодоступними віртуальними сервісами.

Серед тих респондентів, чиї компанії постраждали від злому, приблизно 32% заявили, що витрати організації у зв'язку з інцидентом перевищили $ 100 тисяч, а 11% стверджують, що організація втратила більше $ 1 мільйона. Крім того, 83% опитаних висловили невпевненість у тому, що їх бази даних надійно захищені.

У межах даного дослідження розглянемо основні методи та засоби забезпечення безпеки баз і систем даних. Для цього необхідно розуміти, що система безпеки є невід'ємною частиною правильно спроектованої системи з базою даних. У загальному вигляді систему безпеки можна представити у вигляді моделі, яку складають шість відносно незалежних рівнів:

- фізична безпека;
- безпека мережевого доступу;
- доменна безпека;
- безпека локального комп'ютера;
- безпека сервера баз даних;
- безпека програмних додатків.

Розглянемо детально кожен з цих рівнів.

Перший рівень моделі безпеки інформаційної системи з базою даних представлений фізичною безпекою. Фізична безпека забезпечує захист доступу до інфраструктури, яку утворюють внутрішні мережеві компоненти та апаратне обладнання, що підтримує роботу серверних компонент системи.

На другому рівні – безпека мережевого доступу. Вона включає такі компоненти, як шифрування пакетів та ізоляція транспортного протоколу. Шифрування пакетів реалізоване на проміжному рівні між клієнтом і сервером баз даних за допомогою протоколу SSL (Secure Socket Layer) або шифрування при виклику віддалених процедур (RPC). Інша дієва методика забезпечення безпеки мережевого доступу полягає у застосуванні брандмауера або спеціалізованого обладнання для розмежування комп'ютерних мереж.

Третій рівень забезпечує доменну безпеку. Вона реалізується за допомогою служб каталогу облікових записів області мережевих імен. Наприклад, у гетерогенних мережах під управлінням серверної операційної системи з ядром Linux [2], цю роль виконують служби Samba, LDAP, Cerberos та Iptabless. Якщо сервер баз даних є членом мережевого домена, можна наділити обліковий запис користувача або групи користувачів привілеями для доступу до сервера баз даних і виконання на ньому певних дій з читання, запису або редагування бази даних.

Служби обліку доменних записів користувачів комп'ютерної мережі забезпечують надійну перевірку прав користувачів на рівні доступу до мере-

жевих компонентів. Доменні паролі зашифровуються з метою уникнення їх перехоплення під час передачі по мережі. Крім того, широко застосовуються заходи з визначення мінімальної довжини пароля та терміну його дії.

На четвертому рівні забезпечується безпека локального комп'ютера. Вона зумовлює проведення аудиту безпеки засобами самої операційної системи, розмежування прав доступу до файлів та реєстру, а також функціонування служб шифрування. Сервери сучасних баз даних зазвичай працюють під управлінням операційних систем сімейств Windows або Unix, які у свою чергу підтримують аудит системи безпеки, дозволяючи відстежувати такі події, як вхід користувачів у систему, спроби читання та редагування баз даних.

П'ятий рівень забезпечує систему безпеки сервера баз даних, яка включає чотири категорії безпеки:

- аутентифікацію;
- авторизацію;
- шифрування;
- служби аудиту.

Процес надання доступу до бази даних складається з двох фаз: спочатку виконується підключення до сервера баз даних, а потім відкривається доступ до бази даних з усіма її об'єктами. Дозвіл на роботу з об'єктами дає можливість користувачу виконувати дії над об'єктами бази даних, наприклад, таблицями та представленнями. Дозвіл на виконання SQL-операторів дає можливість користувачам створювати об'єкти бази даних, переглядати та маніпулювати даними [3].

Для зменшення кількості адміністративних операцій, які необхідно виконати для надання дозволів користувачам БД, сучасні СУБД підтримують групування користувачів за групами. Права доступу можна надати групі, так само, як і окремому користувачу. Якщо права доступу призначаються групі, то кожен користувач, включений у цю групу, набуває її права доступу. Спадкоємство – це здатність об'єкта (у даному випадку користувача) приймати всі властивості іншого об'єкта. Групи мають властивість вкладеності одна в одну, що дозволяє будувати ієрархію груп.

Усі дії, що виконуються в базі даних, відстежуються за допомогою аудиту СУБД. Деякі об'єкти бази даних, наприклад, збережені процедури, дозволяється зашифровувати, щоб захистити їхній вміст від несанкціонованого читання.

Шостий рівень організовує безпеку програмних додатків. Додаток може розширювати можливості системи безпеки баз даних, доповнюючи її власними функціями безпеки.

Програмний засіб, що звертається до бази даних, викликає спеціальну системну процедуру (у SQL Server це sp_setapprole) з метою активізації ролі програмних додатків. Крім того, у додатку реалізована власна система безпеки, непідконтрольна СУБД. Для ізоляції додатків від деталей механізму доступу до даних застосовуються функції API доступу до даних, що підтримуються технологіями, такими як: ADO, OLE DB та ODBC [4].

Згідно з моделлю безпеки бази даних відповідальність за кожен її рівень розподіляється між визначеними посадовими особами. За реалізацію перших чотирьох рівнів системи безпеки бази даних відповідають мережеві та системні адміністратори, адміністратори та розробники бази даних відповідають за п'ятий рівень, а розробники додатків – за шостий. Фахівці з інформаційної безпеки, як правило, спостерігають за проектуванням системи безпеки в загальному обсязі.

Згідно цих рівнів авторами було досліджено, випробувано та впроваджено певні технології комплексного захисту баз даних та інформаційних систем у межах корпоративної мережі ВНЗ з метою своєчасного виявлення кіберзагроз та їх ліквідації.

Загроза кібербезпеці актуалізується через:

- невідповідність інфраструктури електронних комунікацій, рівня її розвитку та захищеності сучасним вимогам;
- недостатній рівень захищеності критичної інфраструктури, електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
- безсистемність заходів кіберзахисту критичної інфраструктури;
- недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та електронних інформаційних ресурсів;
- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Першою частиною реалізації було впровадження доменної структури корпоративної мережі під управлінням серверної операційної системи на базі ядра «Linux». Налаштування базових систем безпеки операційної системи було розділено на декілька етапів, які розглянуто нижче.

По-перше, було заблоковано всі порти, крім необхідних. Залишаємо лише необхідні 80-й та 443-й та один порт для віддаленого шифрованого доступу. Для цього встановлюємо та налаштовуємо програмний засіб – брандмауер наступним чином:

- sudo apt-get install ufw;
- sudo ufw allow ssh;
- sudo ufw allow http;
- sudo ufw enable

А також додаємо правила, щоб дозволити або заборонити доступ наступним чином:

- ufw allow to 192.168.23.1 port 8080 from 192.168.23.0/24 proto tcp

• ufw allow to 192.168.23.10 port 80 from 192.168.23.0/24 proto tcp
• ufw allow to 192.168.23.10 port 3128 from 192.168.23.0/24 proto tcp

Наступним етапом є коригування налаштувань shared memory – fstab, тому що є можливість використати розділ /dev/shm для атаки на сервіс httpd, що у свою чергу може надати кіберзлочинцю доступ до інших сервісів, тому щоб зробити fstab більш безпечнішим відкоригуємо певні директиви наступним чином:

• sudo vi /etc/fstab
• tmpfs /dev/shm tmpfs defaults,noexec,nosuid 0 0
• reboot

Сервіс баз даних встановлюємо локально та дозволяємо доступ до нього за внутрішньою адресою сервера, а саме 127.0.0.1, так званий localhost, що унеможливить доступ до баз даних ззовні. Для унеможливлення безпосереднього доступу до БД, використаємо шифрування даних – як вдалий спосіб запобігти такій ситуації, але лише незначна кількість БД надають таку можливість. Найбільш просте рішення цієї проблеми – встановлення програмного пакету для шифрування даних, а потім використання його у розробці програмних засобів. Більша частина мов програмування, які використовують при розробці програмних систем з базами даних, мають у своєму складі розширення Mcrypt і Mhash, що реалізовують різні алгоритми криптування. При такому підході програмний засіб спочатку шифрує дані, а потім дешифрує їх при запиті. Нижче наведено приклад того, як працює шифрування даних, що реалізовано за допомогою однієї з найбільш розповсюджених мов програмування – PHP, більш відомий, як хешування, тобто зберігання MD5-хешу від пароля в БД, замість зберігання оригінального значення:

```
$ Query = sprintf ("INSERT INTO users (name, pwd) VALUES ('% s', '% s');",
    addslashes ($ username), md5 ($ password));
$ Result = pg_exec ($ connection, $ query);
$ Query = sprintf ("SELECT 1 FROM users WHERE name = '% s' AND pwd = '% s';",
    addslashes ($ username), md5 ($ password));
$ Result = pg_exec ($ connection, $ query);
if (pg_numrows ($ result)> 0) {
    echo "Welcome, $ username!";
}
else {
echo "Authentication failed for $ username.";
```

Наступним етапом є проведення оптимізації систем керування базами даних з відкритим вихідним кодом. Очевидно, що зловмисник повинен володіти відмінними знаннями щодо архітектури побудови запитів до серверу бази даних, проте отримати дану інформацію досить легко. Наприклад, якщо база даних є пакетом з відкритим вихідним кодом або іншим чином загальнодоступних пакетів з встановленням по замовчуванню, то ця інформація повністю відкрита та доступна. Інші методи загроз відбуваються через перевірку загальноприйнятих імен таблиць чи атрибутів полів [4].

Наприклад, форма входу, що використовує такі імена, як: 'users' таблиця зазвичай має назви колонок 'id', 'username', та 'password'.

Ці загрози для БД можливі за умови, що розробник не переймався питанням безпеки БД. Тому не варто довіряти даним, що надходять із клієнтської сторони, навіть якщо це дані вибору форми select box, приховані вхідні дані полів чи дані cookie.

Перший приклад демонструє, що такий ніби бездоганний запит може створити загрозу у безпеці даних.

Тому замість з'єднання з БД, як адміністратор чи власник БД, було використано зареєстрованого користувача із обмеженими правами та підготовлені вирази із зв'язаними змінними. Для їх використання застосовуються PDO , MySQLi чи інші відповідні бібліотеки.

Також було застосовано перевірку, чи введені дані відповідають очікуваному типу даних [5]. Наприклад, мова PHP має широкий спектр відповідних функцій валідації, від найпростіших Variable Functions та Character Type Functions (також, is_numeric(), ctype_digit() відповідно).

Якщо скрипт очікує числових вхідних даних, то використовується верифікація даних за допомогою ctype_digit(), або тип даних settype(), або числові відображення sprintf() [6]. В якості прикладу показано формування запиту безпечної посторінкової навігації:

```
<?php
settype($offset, 'integer');
$query = "SELECT id, name
    FROM products
    ORDER BY name
    LIMIT 20
    OFFSET $offset;";
$query = sprintf( "SELECT id, name
    FROM products
    ORDER BY name
    LIMIT 20
    OFFSET %d;",$offset);
?>
```

Також було застосовано збережені процедури, які унеможливлюють користувачем передачу даних напряму до БД.

Крім того, налаштовано журнал логів запитів до серверу БД [7]. Звісно журнал ніяким чином не унеможливлює вразливість серверу БД, проте він надає інформацію про сторонні запити та корисну інформацію щодо аналізу для покращення безпеки запиту.

Висновки з проведеного дослідження. Отже, всі вищенаведені засоби не надають стовідсотко-

вого захисту від зовнішніх та внутрішніх загроз, але рішення безпеки не можна налаштувати одноразово, воно вимагає постійного моніторингу протягом усього періоду використання, відстеження подій безпеки та оптимізації пов'язаних з цим політик.

У роботі було досліджено систему загроз та детально налаштовано клієнтську частину програмного забезпечення, що відповідає за політику безпеки з надання клієнтам корпоративної комп'ютерної мережі доступу до баз даних і систем даних, захищений брандмауером, для налаштування якого відповідним чином наведені створені конфігураційні файли та описана сама процедура створення.

Дослідження показало, що впровадження продуманої архітектури безпеки і правильний вибір засобів захисту баз даних та інформаційних систем дозволить значно зменшити ризики та мінімізувати можливі втрати від зловмисного впливу.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Advanced Analytics [Електронний ресурс] : Інтернет–ресурс. – Режим доступу : http://info.appsecinc.com.

2. Рада національної безпеки і оборони України [Електронний ресурс] : офіц. веб-портал. – Режим доступу : http://www.rnbo.gov.ua/documents/417.html.

3. Колісніченко Д. Линукс сервер / Д. Колісніченко. – СПб. : Санкт-Петербург, 2011. – 736 с.

4. Bill Phillips, Brian Hardy. PHP Programming: The Big Nerd Ranch Big. Nerd Ranch Guides, 2013.

5. Дейт К. Дж. Введение в системы баз данных / К. Дж. Дейт. – М. : Вильямс, 2011. – 172 с.

6. Кириллов В. В. Основы проектирования реляционных баз данных [Електронний ресурс] / В.В. Кириллов. – Режим доступу : http://www.citforum.ru/database/dbguide/index.shtml.

7. Котляров В. П. Основы тестирования программного обеспечения / В. П. Котляров. – СПБ. : Бином, 2009.