УДК 004

РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ МОДУЛЯ «КАФЕДРА» ІНФОРМАЦІЙНОЇ СИСТЕМИ УНІВЕРСИТЕТУ НА ОСНОВІ РОЛЬОВОЇ ПОЛІТИКИ ДОСТУПУ

Б. В. Соловей[1, a], Л. Ю. Гальчинський[2]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Дана робота присвячена питанню ефективної та безпечної роботи з даними в підрозділі вищого навчального закладу. Розглянуто наявний процес обміну інформацією між викладачем і кафедрою щодо їх науково-педагогічної діяльності, а також проблеми що супроводжують цей процес. Проведений аналіз показав суттєві недоліки в організації та обробці даних на рівнях викладач-кафедра та кафедра-факультет, що проявляють себе невиправданим дублюванням, несвоєчасністю подання, чисельними помилками та викликають непотрібну напругу в людей. Цей стан речей породжений несистемним напівручним підходом при обробці даних на рівні викладач-кафедра, бо існуючі інформаційні системи для ВНЗ приділяли надто мало уваги цьому рівню. Ще менше у цих системах уваги присвячено безпековим питанням, зокрема з точки зору захисту персональних даних. В роботі пропонуються принципи кібербезпеки для рівня Викладач-Кафедра інформаційної системи, в якій буде автоматизовано обробку даних.

Ключові слова: кібербезпека, RBAC, AIC

Вступ

Інформаційна система є одним із фундаментальних засобів підтримки діяльності сучасних навчальних закладів. В сучасній вітчизняній літературі інформаційні системи для навчальних закладів мають неусталену, довгу і незручну назву: Інформаційні системи управління освітнім процесом(ІСУОП) [1], або інтегрована інформаційна системи управління університетом (ІІСУ) [1], причому вони не охоплюють всю предметну область. Разом з тим у світовій літературі давно використовується термін Академічна інформаційна система(AIC) [2], він здається нам більш вдалим, тому ми і будемо його використовувати.

Інформація про наукову діяльність викладачів, котра оброблюється в AIC, включена до критеріїв оцінки університетів у всьому світі [3]. Таким чином, існування AIC для університетів є життєво важливим. Більше того, з плином часу роль AIC буде зростати. Відтак питання забезпечення якості AIC буде залишатися актуальним. Є багато аспектів якості програмного забезпечення(ПЗ), які можна оцінити. McCall [4] стверджує, що ПЗ, як правило, має 11 факторів, які потім об'єднуються у три категорії. Одним з найважливіших аспектів якості AIC є безпековий. Для ПЗ аспект безпеки пов'язаний із захистом даних та інформації. Таким чином якість системи в цілому залежить від того, наскільки правильно будуть пов'язані інформаційний та безпековий аспекти. Розробники AIC для ВНЗ України по-різному розуміють цю проблему. І хоча безпековий аспект завжди враховувався, але повноцінно реалізувати політику безпеки в AIC не вдалось. Причин тут декілька, проте ми розглянемо тільки одну з них. Ця проблема знаходиться на рівні Науково-педагогічний працівник(НПП)-Кафедра та Кафедра-Факультет. Справа в тому, що розробники AIC мало приділяли увагу цим рівням, а першому з них практично ніякої. На даний момент в Україні функціонує багато AIC, які автоматизовують процеси обміну даними в підрозділах університету, переважно рівня ректорату та відповідних функціональних служб, але вони часто нехтують рівнями кафедра-факультет і кафедра, а також через нечіткість вимог до таких систем питання безпеки не обговорюється. В деяких рішеннях не враховувалась можливість несанкціонованого доступу з боку мережі [5]. AIC в деяких вищих начальних закладах України серед яких і Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» – це закриті системи, інформація про функціональну повноту цих систем недоступна [5], проте відомо, що інформаційні потреби часто реалізуються засобами офісних пакетів, хоча б мали бути інтегровані в AIC університетів.

Так, наприклад в одному з небагатьох документів [1], що розглядає проблему AIC в Україні з системних позицій, вказується на необхідність розробки модуля «Кафедра», в якому його функціонування пов'язане з забезпеченням документів:

[a] solovey.bohdan@gmail.com

- Навчальний план. Є основним нормативним документом, що визначає організацію навчального процесу.
- Форма № 1. Для планування та обліку навчальної роботи науково-педагогічних працівників університету за чвертями та семестрами.
- Форма № 2. Містить інформацію про види та обсяги навчального навантаження кафедри по семестрах і за навчальний рік залежно від форми навчання студентів.
- Форма № 3. Містить інформацію про навчальне навантаження викладачів кафедри.
- Форма № 4. Інформація про навантаження викладачів. ЇЇ джерело – Форма № 3 за місяцями, семестрами і за рік.

Також вказується, що модуль «Кафедра», а також модуль «Деканат» за своїм складом і призначенням можуть бути реалізовані за допомогою реляційної розподіленої бази даних, що дозволить збільшити швидкість обробки даних, зменшити час на їхню реплікацію та підвищити сталість системи в цілому. Щодо безпеки, то тільки для модуля «Ректорат» доцільно вживати засоби підвищеного захисту та шифрування конфіденційних даних. Однак, в сучасній практиці АІС наразі на рівні кафедри не робиться ні автоматизації, ні забезпечення інформаційної безпеки.

В межах підрозділу вищого навчального закладу, а саме кафедри функціонує процес передачі наборів даних викладачів, таких як їх особисті дані та дані про їх науково-педагогічну діяльність. Напівручна технологія обробки цих даних, що супроводжується такими наслідками як висока трудомісткість, помилки при вводі та дублювання даних приводить не тільки до перевитрат часу, але й також не дає можливості реалізувати аспект безпеки даних. Все це потребує системного вирішення, тобто захист даних має бути органічно включений в інформаційний процес.

1. Аналіз проблем

1.1. Нинішній процес обробки даних на кафедрі

Збір і обробка такої інформації в ручному режимі є дуже трудомістким процесом, який вимагає багато уважності і значних затрат часу, тож забезпечення надійного захисту інформації може здаватись зайвим або другорядним, адже воно певною мірою ускладнює і сповільнює процес. Серед даних які передаються від наукових працівників на кафедру можна виділити частину до якої входять такі, за допомогою яких можна ідентифікувати особу:

- паспортні дані
- адреса проживання
- дата народження
- номер диплому про вищу освіту
- ідентифікаційний код

Такі дані можна віднести до персональних, які захищаються законом України «Про захист персональних даних» [6]. Також обробляється інформація про наукову діяльність за останні 5 років і оновлюється коли викладачі публікують статті, наукові роботи, або беруть участь в конференціях і т.д. Це все потрібно оновлювати і передавати в систему ЄДЕБО[1].

З інформаційної точки зору це питання вирішується з використання методології моделей баз даних(БД), зокрема реляційної моделі, яка фактично стала традиційною і підлягає реалізації сучасними системами керування базами даних(СКБД). Проте безпековий аспект потребує спеціального аналізу. І тільки з його врахуванням можна реалізовувати проект для модуля «Кафедра».

1.2. Аналіз загроз

Частина даних які готує ВНЗ не підлягає розголошенню, а інші матеріали потребують спеціальних режимів використання. Це підтверджує, що тут циркулює інформація різного рівня доступу і функціонального наповнення. Її можна поділити на два основні типи з точки зору поширення і використання: загальнодоступна інформація та інформація з обмеженим доступом(ІОД). Більшість даних, які циркулюють на рівнях викладач-кафедра та кафедра-факультет потрапляють до ІОД. Для ІОД, на відміну від загальнодоступної, потрібно чітко визначити де, ким, в якому обсязі і на яких умовах може здійснюватися доступ.

ВНЗ це публічний заклад з аудиторією, яка часто змінюється, а також це місце підвищеної уваги з боку «кіберзлочинців» початкового рівня, у цьому і полягає специфіка захисту інформації в освітній системі. Основна група потенційних порушників у ВНЗ це студенти, які мають високий рівень підготовки. Молодий вік поєднаний з юнацьким максималізмом інколи спонукають їх блиснути вміннями перед однокурсниками: розповсюдити віруси, «покарати» викладача і тд. Достатньо згадати, що перші комп'ютерні правопорушення народилися саме в вузі (черв'як Морріса) [7].

До основних загроз безпеки АІС можна віднести:

- спроби адміністрування БД/несанкціонованого віддаленого адміністрування ОС;;
- несанкціоноване дослідження/сканування мережі/портів;
- видалення інформації;
- спроби злому/установка вірусних програм і троянських коней;
- пошук «дірок» в безпеці ОС, firewall, Proxy-серверів;

Основними джерелами можливих загроз інформації є:

- Інтернет;
- навчальні аудиторії з комп'ютерами;
- службові аудиторії кафедри з комп'ютерами на робочих місцях викладачів та допоміжного персоналу.

[1] Єдина державна електронна база з питань освіти. https://info.edbo.gov.ua/about/

Основні об'єкти, що потребують захисту від несанкціонованого доступу:

- БД / www / ftp-сервери;
- панель/консоль керування обліковими записами;
- локальні обчислювальні мережі та сервери дослідницьких проектів.

2. Вирішення проблеми

Головне завдання роботи: полегшити роботу членам кафедри при обробці даних щоб процес став простішим, надійнішим та більш захищеним при обробці та передачі даних. Це має бути зроблено за допомогою спеціально розробленої і захищеної системи. Система має бути побудована таким чином, щоб процеси передачі інформації були захищеними, а архітектура системи була гнучкою і в разі потреби розширювалась.

2.1. Захист даних при передачі даних по мережі

Позаяк оброблені дані необхідно передавати як на рівні кафедри між співробітниками, так і передавати на вищі рівні, пропонується зробити невеликий вебресурс з обмеженим доступом до нього. Передача даних між клієнтом та сервером повинна здійснюватись з шифруванням наприклад через HTTPS[2]. За допомогою протоколу TLS [3]обмін даними проводиться на захищеному рівні, а це дуже важливо для веб-ресурсів, які зберігають конфіденційну інформацію клієнтів [8].

2.2. Захист даних при обробці даних на кафедрі

Захист даних при їх обробці на кафедрі в рамках АІС можна реалізувати за рахунок політики безпеки. В реляційній моделі є властивості захисту даних, але вони стосуються питань уникнення втрат даних при обробці. При захисті даних, зокрема персональних потребуються зовсім інші підходи, а саме політики безпеки. Вони добре відомі. Це в першу чергу обов'язковий контроль доступу (MAC) та дискреційний контроль доступу (DAC). MAC – для багаторівневих захищених військових програм, DAC – для задоволення потреб безпеки в обробці даних для промислових та цивільних установ. Проте застосування таких політик для цієї задачі є недоцільним [9]. У цій статті доведено, що DAC не завжди є основним для контролю доступу для комерційних та цивільних державних організацій. Натомість описано тип недискреційного контролю доступу – на основі рольового контролю доступу (RBAC), який є більш релевантною політикою безпеки обробки даних для цивільних систем, ніж DAC. Це стосується і сфери

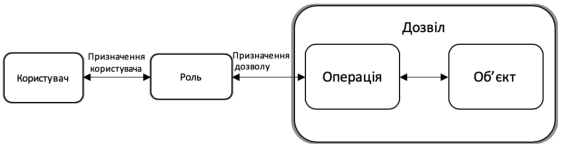

Рис. 1. Основні елементи RBAC: Користувач – людина, роль – набір функцій для виконання певних задач, дозвіл – авторизована операція над об'єктом. В RBAC користувачі закріплюються до ролей(призначення користувача), кожна з яких містить набір дозволів(призначення дозволу).

ВНЗ. Розглянемо цей підхід для захисту персональних даних для модуля «Кафедра» АІС.

Очевидно, проектуючи БД на основі реляційної моделі даних доведеться враховувати специфічні для неї сутності та зв'язки між ними. Це традиційний підхід, відомий з часів Едгара Кодда. Однак цей класичний підхід необхідно дещо модифікувати, якщо ставиться задача рольового контролю доступу. В цьому контексті доведеться внести певні обмеження на запити можливих учасників-користувачів модуля «Кафедра» АІС. Першим кроком у цьому напрямку є виявлення учасників і встановлення ролей, які й забезпечать не тільки цілісність даних як у традиційній РБД, але і захист персональних даних.

Контроль доступу – найважливіша особливість будь-якої захищеної системи. Взагалі кажучи, вона передбачає сегрегацію суб'єкта до об'єкта відповідно до реалізації політики безпеки в даній системі. Основні елементи керування доступом на основі ролей зображено на Рис.1. Для модуля «Кафедра» дещо спростимо задачу і запропонуємо такі ролі:

- «адмін» – має право на створення, читання, оновлення, видалення інформації в розділі даних користувачів; Користувач з роллю «адмін» може змінювати ролі інших користувачів.
- «модератор» – має право на створення, читання, оновлення, видалення будь-якої інформації в розділі персональних даних користувачів;
- «методист» – має право на створення, читання, оновлення, видалення будь-якої інформації в розділі «Науково-педагогічна діяльність»;
- «науково-педагогічний працівник» – має право на створення, читання, оновлення, видалення інформації у всіх розділах лише з записами котрі пов'язані з ним.
- «гість» – має право на реєстрацію, після якої йому автоматично створиться запис в розділі персональних даних, «адмін» повинен призначити йому роль в системі.

Працівник кафедри відповідальний за роботу з персональними даними повинен мати роль «модератор», за роботу з даними про науково-педагогічну діяльність – «методист», наукові працівники про яких збирається інформація – «науково-педагогічний працівник», або «гість». Роль «адмін» призначена для людини яка регулює роботу АІС. На Рис. 2. можна побачити використання RBAC в АІС що проектується (роль «гість» спеціально упущено).

[2]Hyper Text Transfer Protocol Secure – схема URI, що синтаксично ідентична http

[3]Transport Layer Security – протокол, що надає можливості безпечної передачі даних в Інтернет. Використовує асиметричне шифрування і сертифікати X.509.

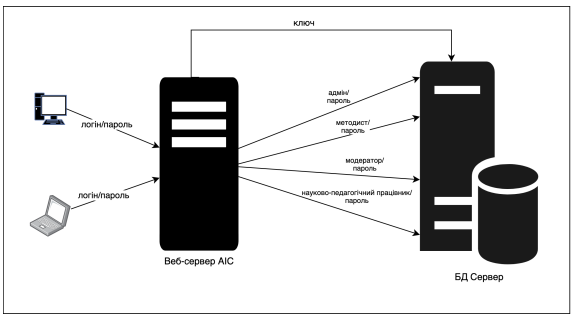

Рис. 2. Впровадження RBAC в AIC.

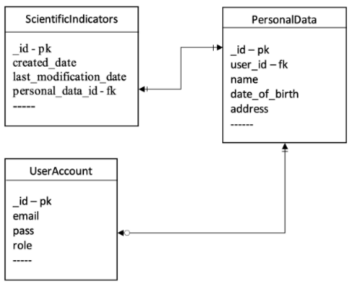

Рис. 3. База даних.

2.3. Модифікація моделі бази даних

На Рис. 3 наведене схематичне зображення основних таблиць потрібних для модуля «Кафедра» AIC, яка проектується з врахуванням вимог RBAC згідно розглянутих ролей в дещо спрощеному вигляді. «UserAccount» – таблиця для зберігання набору даних про обліковий запис користувача AIC(включно з роллю та дозволами).

«PersonalData» – таблиця для зберігання набору даних про працівника, містить чутливу інформацію. Може прив'язуватись до запису в «UserAccount».

«ScientificIndicators» – таблиця для зберігання набору даних показників науково-педагогічної діяльності працівників кафедри, котра прив'язана до запису в «PersonalData».

3. Можлива реалізація

Для AIC буде використовуватися реляційна СКБД така як MySQL, або PostgreSQL. Реалізувати розділення доступу потрібно програмно на рівні застосунку. Можна виділити наступні пункти:

- Доступ до системи повинен надаватись за індивідуальним логіном і паролем.
- Розділення доступу на основі RBAC.
- Для того щоб швидко та безпечно розвернути всю систему доцільно використовувати контейнери Docker[4], адже їх можна швидко і легко налаштувати під свої потреби.
- Для мінімальних затрат часу на розробку і підтримку системи доцільно використати мову програмування Python.

[4]Інструментарій для управління ізольованими контейнерами.

Висновки

В результаті проведеного аналізу було встановлено суттєві недоліки існуючих в Україні AIC для рівня Кафедра-Викладач та Факультет-Кафедра, які в основному пов'язані з тим, що робота проводиться в напівручному режимі, а політики безпеки визначені нечітко. Це у свою чергу породжує безпекову вразливість AIC в цілому, зокрема незахищеність персональних даних. Запропоновано методику проектування модуля «Кафедра» з врахуванням політики рольового доступу RBAC. Для спрощення, захисту та підвищення ефективності інформаційної діяльності кафедри було запропоновано розробити веб-сервіс який буде створений на принципах, які дозволяють забезпечувати кібербезпеку і автоматизувати передачу та обробку інформації.

Перелік використаних джерел

1. ЛЮБЧАК, Володимир Олександрович, et al— Методологічні основи створення, впровадження і розвитку інтегрованої інформаційної системи управління університетом. 2015.
2. Indrayani, E.— (2013). — Management of academic information system (AIS) at higher education in the city of Bandung. Procedia-Social and Behavioral Sciences, 103, 628-636.
3. THE World University Rankings 2020: methodology.— [Електронний ресурс] URL: `https://www.timeshighereducation.com/world-university-rankings/world-university-rankings-2020-methodology`. (дата звернення 11.04.2020).
4. Galin, D. — Software Quality Assurance: From theory to implementation//— Лондон: Вид-во «Pearson», 2004.
5. Ю. А. Коцюк, Ю. О. Данилець//— Наукові записки Національного університету «Острозька академія».— Серія «Економіка»: науковий журнал. – Острог : Вид-во НУ«ОА», травень 2016. – № 1(29).С.71–75.
6. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI.— Ст. 2. URL: `https://zakon.rada.gov.ua/laws/show/2297-17` (дата звернення: 11.04.2020).
7. Волков А. В.— Обеспечение ИБ в вузах//— Информационная безопасность. 2006. № 3, 4
8. «Що таке https? І навіщо він потрібен кожному сайту.»— [Електронний ресурс] URL: `https://www.ukraine.com.ua/uk/blog/seo-optimization/chto-takoe-https-i-zachem-on-nuzhen-kazhdomu-sajtu.html`. (дата звернення 11.04.2020).
9. 15th National Computer Security Conference— Балтимор, жовтень 1992. ст. 554-563