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)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: *«Безпекова модель в ERP – системі Dynamics AX»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Карпешко А.І
підпис (прізвище та ініціали)

Керівник *Александр М.Б..*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б*
підпис (прізвище та ініціали)

Рецензент Крамар О.І
підпис (прізвище та ініціали)

м. Тернопіль – 20*20*

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМ. І. ПУЛЮЯ

Кафедра *кібербезпеки*
Спеціальність *125 Кібербезпека*

"З А Т В Е Р Д Ж У Ю"
Завідувач кафедри кібербезпеки
_____ *Н. В. Загородна*
"____" _____ *2020 р.*

ЗАВДАННЯ

на магістерську кваліфікаційну роботу студенту групи СБм - 61
Карпешку Андрію Ігоровичу

1. Тема роботи: *"Безпекова модель в ERP- системі Dynamics AX"* затверджена наказом по університету від "16" листопада 2020 р. № 4/7-842.

2. Термін здачі студентом закінченої роботи: " 14 " грудня 2020 р.

3. Вихідні дані для роботи*: вимоги до політики безпеки модулів ERP – системи, сформовані на основі потреб та специфіки діяльності сучасного підприємства*

4. Зміст розрахунково-пояснювальної записки: *Вступ – актуальність теми магістерської роботи. Основна частина – аналіз компонентів безпекової моделі в ERP – системі Dynamics AX. Дослідження поведінки захищених об'єктів в Microsoft Dynamics AX. Реалізація політики безпеки для окремого модулю ERP – системи Dynamics AX. Висновки.*

5. Перелік графічного матеріалу *інтерфейс ERP – системи Dynamics AX 2012, схеми об'єктів безпекової моделі ERP – системи Dynamics AX 2012.*

6. Перелік програмних продуктів, які належить використати в процесі розроблення роботи (проекту): *Пакет MS Office: процесор тексту Microsoft Word, процесор презентацій Microsoft Power Point, ERP – система Dynamics AX 2012.*

7. Консультування роботи, із зазначенням розділів роботи

Розділ	Консультант	Завдання видав		Завдання прийняв	
		підпис	дата	підпис	дата

8. Дата, коли видано завдання : *“ ” 2020 р.*

Керівник _____ *М.Б. Александер*

Завдання прийняв до виконання _____ *А.І Карпешко*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Пошук науково-технічної літератури. Складання плану роботи.*	*.2020*	*виконано*
2.	*Написання першого, другого розділу роботи.*	*.2020*	*виконано*
3.	*Реалізація політики безпеки для окремого модулю системи*	*.2020*	*виконано*
4	*Написання третього розділу роботи.*		
5.	*Написання розділу охорони праці та безпеки в надзвичайних ситуаціях*	*.2020*	*виконано*
6.	*Оформлення пояснювальної записки.*	*.2020*	*виконано*
7.	*Подання завершеної дипломної роботи на кафедру.*	*14.12.2020*	*виконано*

Студент _____ *А.І Карпешко*

Керівник _____ *М.Б. Александер*

АНОТАЦІЯ

Реалізація політики безпеки окремого модулю ERP – системи Dynamics AX 2012 з метою захисту інформації на підприємстві.// Дипломна робота ОР «Магістр» // Карпешко Андрій Ігорович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2020 // С. 72 , рис. 43 , табл. – , кресл. – , додат – 2.

Ключові слова: безпекова модель, політика безпеки, розмежування доступу, ERP – система Dynamics AX 2012.

Магістерська робота охоплює тему захисту даних в ERP – системі Dynamics AX 2012. В першому розділі здійснено аналіз компонентів безпекової моделі Dynamics AX. В другому розділі було проведено дослідження поведінки захищених об'єктів в системі та визначені основні об'єкти, які підлягають захисту. В третьому розділі реалізується політика безпеки для окремого модулю системи за допомогою створення ролей, привілегій та інших артефактів безпеки. В четвертому розділі зроблено огляд охорони праці в галузі ERP - розробки програмного забезпечення та безпеку в надзвичайних ситуаціях.

ANNOTATION

Implementation of the security policy of a separate ERP module - Dynamics AX 2012 system for protecting information at the enterprise// Thesis of the Master degree // Karpeshko Andriy Igorovich // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2020 // P. 72, Fig. 43, Tables – , Diagrams. -, Annexes. -, References 2.

Keywords: security model, security policy, access delimitation, ERP system Dynamics AX 2012.

The master's thesis covers the topic of data protection in the ERP - Dynamics AX 2012. In the first section, an analysis of the components of the security model Dynamics AX. The second section examines the behavior of protected objects in the system and identifies the main objects to be protected. The third section implements a security policy for a single system module by creating roles, privileges, and other security artifacts. The fourth section provides an overview of occupational safety and health in the field of ERP - software development and safety in emergencies.

ЗМІСТ

ВСТУП

Актуальність. На сьогоднішній день питання спрощення та автоматизація діяльності підприємств й різноманітних видів бізнесу є доволі важливим аспектом в житті таких організацій. Чим менше часу підприємство витрачає на бухгалтерський облік, створення ордерів на продаж чи купівлю, тим швидше й ефективніше дана структура працюватиме.

Окрім, цього ERP – система надає важливу інформацію про такі важливі деталі життя підприємства як його штат, підрозділи, які виконують ту чи іншу задачу, звіти за різноманітними параметрами діяльності підприємства, а також автоматичне створення аналітик й полегшення процесу працевлаштування та звільнення працівників підприємства.

Й це лише невелика частина стандартних можливостей ERP – системи Dynamics AX, за потреби можна створити нові функціональні модулі для вирішення тих чи інших завдань.

Проте, дуже важливим є питання захисту інформації що циркулює всередині ERP – системи. Розмежування доступу до даних є дуже важливим аспектом її функціонування, так як втрата чи спотворення даних може призвести до матеріальних чи репутаційних збитків підприємства. Чимало великих корпорацій втрачали велику кількість ресурсів із-за неправильного налаштування політики безпеки систем, котрі зберігають дані що циркулюють на підприємстві.

Метою дослідження є розробка політики безпеки даних для окремого модуля системи, для захисту даних від несанкціонованого доступу, втрати чи спотворення.

Об’єктом дослідження є безпекова модель ERP – системи Dynamics AX 2012 та ієрархія безпекових артефактів в системі.

Предметом дослідження є програмна реалізація політики безпеки модуля «Академія».

Пошуки шляхів досягнення цієї мети обумовили необхідність вирішення наступних завдань:

- Дослідження основних функціональних модулів системи;
- Дослідження безпекової архітектури;
- Дослідження безпекових артефактів;
- Дослідження структури підприємств, які використовують ERP - системи;
- Дослідження багатошарової архітектури системи;
- Дослідження основних об’єктів системи, котрі підлягають захисту;
- Розробка політики безпеки для окремого модуля системи.

У рамках даного дослідження будуть використані наступні **методи**: аналіз та порівняння для вивчення наукової літератури.

Наукова новизна дослідження: розмежування доступу для функціонального модулю «Академії» дає можливість вносити дані про оцінки за іспити для викладачів в системі та переглядати інформацію про успішність для студентів, розмежування доступу до модулю дасть змогу зберегти цілісність даних в системі.

Практичне значення дослідження: програмна реалізація політики безпеки для модуля «Академія», який призначений для обліку успішності студентів – академії.

Результати роботи апробовані на VIII науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя.

Пояснювальна записка обсягом 72 сторінок містить: 43 рисунків, та 2 додатки. Список використаних джерел розміщується на 2 сторінках і містить 11 джерел.

РОЗДІЛ 1. АНАЛІЗ КОМПОНЕНТІВ БЕЗПЕКОВОЇ МОДЕЛІ MICROSOFT DYNAMICS AX

1.1 Специфіка використання та основні функціональні модулі ERP – системи Dynamics AX

В інформаційній економіці XXI століття інформаційні ресурси набули такої ж важливості, як і сировина, виробниче обладнання, трудові ресурси. Тільки ті виробничі підприємства, які впровадили нові інформаційні технології у свої технологічні процеси, можуть бути конкурентоздатними у сучасних економічних умовах[1].

Microsoft Dynamics AX - унікальне рішення з єдиним візуальним об'єктно – орієнтованим середовищем розробки MorphX, що надає можливість швидкої адаптації системи до індивідуальних вимог клієнта. Microsoft Dynamics AX - це доведена тестуваннями можливість одночасної роботи до 3600 користувачів. Це комплексне ERP- рішення, створене спеціально для середніх і великих компаній, яке дозволяє їм розширити свої можливості і придбати нові конкурентні переваги. Microsoft Axapta ідеально підходить для компаній, що шукають повністю інтегроване рішення.

Dynamics AX - це рішення для планування корпоративних ресурсів (ERP), яке інтегрує процеси управління фінансовими ресурсами, управління операційними ресурсами та процеси управління людськими ресурсами, якими можуть володіти та контролювати транснаціональні та багатогалузеві організації, в тому числі в державному секторі. Рішення Dynamics AX охоплює як програму Dynamics AX, так і платформу програм Dynamics AX, на якій побудована програма. Платформа додатків розроблена для того, щоб бути платформою вибору для розробки масштабованих та розширюваних ERP-додатків у найкоротші терміни та з найменшими витратами.

Рівень платформи додатків забезпечує системні фреймворки та інструменти, що підтримують розробку масштабованих та розширюваних компонентів домену програми. Цей рівень складається із середовища розробки,

заснованої на моделі MorphX, мови програмування X ++, клієнтської платформи Windows, платформи Enterprise Portal, AOS та системної платформи додатків.

Ця система краще всього підходить для підприємств, на яких працює до 10 тис. співробітників і потреба в автоматизації, - від 20 до 500 одночасно працюючих користувачів (на практиці існують інсталяції з числом користувачів більше 1000, а також тестові інсталяції для 3000 одночасно працюючих з системою і більше 32 тис. звичайних користувачів).

Система буде корисна організаціям, що мають специфічні і складні бізнес-процеси (підприємства з розподіленою структурою, холдинги, дистриб'юторські і виробничі компанії, працюючі у сфері послуг, і т. д.)

Система Microsoft Dynamics AX є новим поколінням програм управління підприємством (ERP). Завдяки наявності більш ніж 1000 нових функцій і вбудованій галузевій функціональності для виробництва, дистрибуції, сервісного обслуговування і публічного сектора, Microsoft Dynamics надає розробникам надійну платформу для ефективнішої реалізації специфічної функціональності тих галузей, в яких вони працюють.

Microsoft Dynamics AX пропонує глобальне рішення, здатне масштабуватися у міру зростання будь-якого підприємства. Система досить проста, щоб бути розгорнутою в одному підрозділі, в одному регіоні, і в той же час досить надійна для підтримки унікальних вимог бізнесу більш ніж в 36-ти країнах - все робиться з однієї розгорнутої копії системи.

Завдяки гнучкому і безпечному середовищу розробки рішення на платформі Microsoft Axapta може бути легко адаптоване під особливості індивідуальних бізнес - процесів компанії. Система має власну п’яти рівневу архітектуру клієнт - сервер, яка дає можливість роботи через власні WEB, WAP і Windows - інтерфейси.

AOS виконує служби додатків MorphX, що викликаються за допомогою технології RPC та технології Windows Communication Foundation (WCF) в .NET Framework. AOS може розміщуватися на одному комп'ютері, але він також

може масштабуватися до багатьох комп'ютерів, коли потрібні додаткові паралельні сеанси користувача або виділені пакетні сервери.

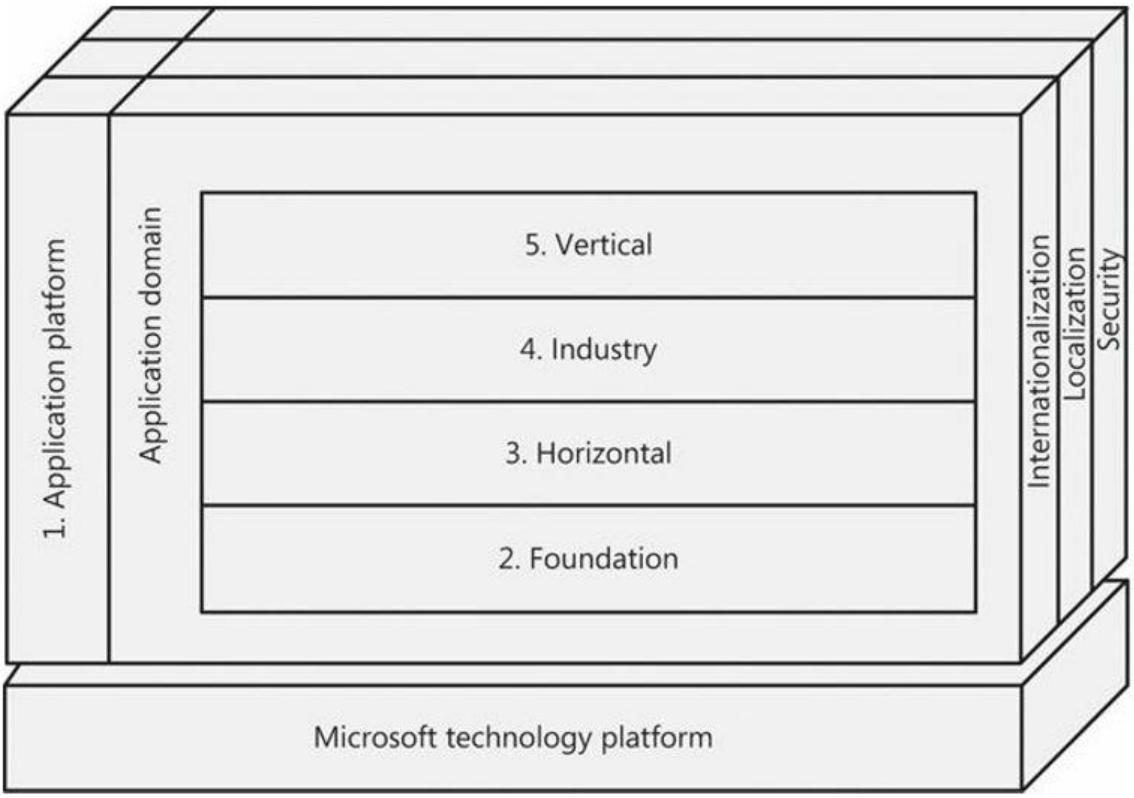


Рисунок 1.1 – Рівні архітектури Dynamics AX

У Microsoft Dynamics AX унікальна серед подібних систем за рахунок багатошарової структури бізнес - логіки, що забезпечує високу надійність при внесенні змін і різко знижує витрати на оновлення версій. Архітектура платформи програм AX підтримує розробку клієнтських програм Windows, веб-клієнтських програм SharePoint, інтеграційних клієнтських програм Office та сторонніх інтеграційних програм.

База даних SQL Server є єдиним компонентом рівня даних. На сервері баз даних розміщуються бази даних контенту та конфігурації SharePoint Server, модель AX та база даних програм, база даних SSRS та база даних SSAS.

Розширення звітності надають SSRS функції, характерні для платформи програм AX. Ці розширення отримують доступ до AOS через сервіси WCF, а

SSAS - через HTTP та HTTPS. Ці служби обробляють запити на дані аналітики, розміщені компонентом SQL Server на рівні даних.

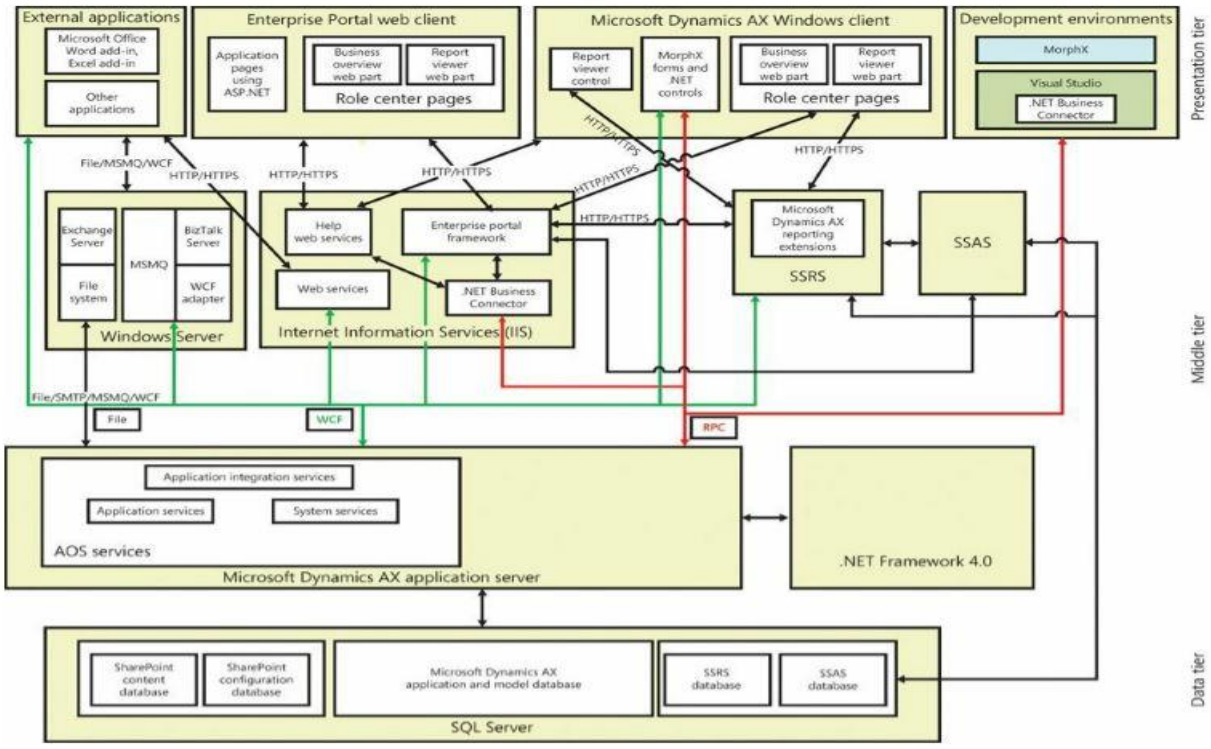


Рисунок 1.2 – Складові архітектури системи

Завдяки специфічній архітектурі Microsoft Dynamics AX є легко масштабованою і підходить для компаній, що швидко розвиваються. У Microsoft Dynamics AX спочатку закладена можливість працювати через Інтернет, що дозволяє вдало вибудовувати стосунки з партнерами по бізнесу.

Серцевина системи Microsoft Dynamics AX є набором єдиних модулів, органічно пов'язаних один з одним, що дозволяє замовникові розуміти, вимірювати і змінювати свій бізнес. При розробці цієї версії була перевірена ще раз кожна прикладна концепція, пов'язана з представленням підприємства в програмному забезпеченні.

Процеси розробки, придбання й впровадження складних систем, до яких відносять, зокрема, програмні комплекси, мають знаходитися під жорстким управлінським контролем[2].

Уніфіковані, природні моделі Microsoft Dynamics AX дозволяють моделювати прості підприємства швидко і легко і в той же час забезпечують

різноманітність і гнучкість виразних засобів для представлення навіть найскладніших організацій. Новий реліз системи Microsoft Dynamics AX істотно відрізняється від попередніх версій, що може зажадати від розробників і фахівців з розгортання, які працювали з попередніми версіями, серйозних зусиль для навчання.

З релізом AX 2012 розробка в системі Microsoft Dynamics AX стала простішою, ніж будь-коли. Розробники можуть працювати з мовою X++ безпосередньо з Microsoft Visual Studio і використати, наприклад, більше просунуті можливості редактора X++. Також реліз підтримує велику міру взаємодії з продуктами Microsoft SharePoint Server і SQL Server Reporting Services, так що розробники витрачають часу менше на рутинне налаштування компонентів. При першій інсталяції Microsoft Axapta відбувається установка усіх функцій системи. Невживані функціональні можливості залишаються прихованими від користувачів і активуються при введенні в систему відповідних ліцензійних кодів.

Підприємства, котрі впроваджують дану ERP - систему, мають ряд ключових переваг :

- Усебічний аналіз і зручність контролю бізнесу;
- Наочність представлення інформації і інтуїтивно зрозумілий інтерфейс;
- Можливість управління групою компаній;
- Низька сукупна вартість володіння (TCO) і кращий у своєму класі показник ROI;
- Повна картина фінансових операцій для швидкого ухвалення правильних рішень;
- Зменшення витрат на достовірний бухгалтерський облік, складання фінансової звітності і аналіз;
- Зменшення витратна достовірний бухгалтерський облік, складання фінансової звітності і аналіз;
- Ефективне управління грошовими потоками;

- Простий інструментарій фінансових операцій і стратегічного планування;
- Можливість управління фінансами для міжнародного бізнесу і розподілених холдингових структур;
- Ефективна організація процесу продажів, що дозволяє поліпшити обслуговування клієнтів;
- Оптимізація закупівель і складських операцій;
- Ефективне управління департаментами.

Dynamics ERP підходить для середніх та великих підприємств. Середні підприємства отримують вигоду від заздалегідь визначеної локалізації для країни, в якій вони працюють. Ці локалізації можна здійснити, купуючи ліцензійні коди у Microsoft. В результаті вартість значно зменшується, оскільки підприємства платять лише за те, що йому потрібно. Великі підприємства, які мають диверсифікований бізнес, можуть отримати вигоду, використовуючи різні модулі в рамках одного рішення ERP.

Рисунок 1.3 – Функціональні модулі системи

На переважній більшості сучасних українських підприємств підготовка документів ведеться із допомогою програмного забезпечення інформаційних систем та оргтехніки, а їх опрацювання та зберігання відбувається тільки на твердих носіях. Така суперечність призводить до ускладнення пошуку потрібного документа та зниження ефективності роботи усього колективу[3]. Використання Dynamics AX вирішує дану проблему на підприємствах різних типів.

Основними функціональними модулями ERP – системи Dynamics AX є:

- Кредиторська заборгованість;
- Дебіторська заборгованість;
- Персонал підприємства;
- Бюджетування;
- Управління готівкою та банками;
- Основні активи;
- Управління запасами та складами;
- Закупівля;
- Управління проектами та бухгалтерський облік.

Модуль «Кредиторська заборгованість» допомагає керувати рахунками постачальників, створювати та відстежувати вихідні рахунки-фактури, вводити номер рахунку в електронному або ручному режимі, або попросити постачальника вводити рахунки-фактури через портал постачальника.

Модуль «Дебіторська заборгованість» дає можливість керувати рахунками - фактурами та вхідними платежами.

Модуль «Бюджетування» дозволяє вам встановлювати, створювати та переглядати бюджети, створювати записи бюджетного реєстру для початкового бюджету, відстежувати кошти, доступні для запланованих програм, переглядати або передавати бюджет, переглядати стан та історію бюджету, створювати звіти про бюджет, серед інших видів діяльності.

Модуль «Управління готівкою та банками» дозволяє вести банківські рахунки та фінансові інструменти вашої організації, такі як векселі, чеки та депозитні квитанції. Модуль інтегрований з різними модулями, включаючи головну книгу, дебіторську заборгованість та кредиторську заборгованість.

Модуль «Основні активи» допомагає керувати основними фондами вашої організації, такими як обладнання, земля, транспортні засоби та будівлі, а також налаштувати інформацію про придбання активів та їх амортизацію на основі встановленої капіталізації або розрахувати коригування основних засобів, щоб знати оптимальний час їх вибуття.

Модуль «Персонал підприємства» дає чіткий огляд роботи робітників, дозволяючи керівництву підприємства визначити сфери, які вони можуть одночасно підвищити ефективність та зменшити витрати на утримання персоналу. Список завдань, які може виконати цей модуль включає підтримку вичерпної інформації про працівників, адміністрування організаційних структур, контроль прогулів, перевірку результативності працівників тощо. Також даний модуль включає в себе функціонал, який дозволяє автоматизувати облік відвідуваності.

Модуль «Управління запасами й складами» допомагає контролювати вхідні та вихідні дії, котрі пов’язані з інвентаризацією на підприємстві. Модуль можна інтегрувати з різними продуктами Microsoft, включаючи управління інформацією про товари, Microsoft Excel, аналіз SQL Server та SQL. Окрім цього даний модуль дає змогу створювати ієрархію складів всередині одного підприємства.

Модуль «Закупівля» допомагає автоматизувати процес створення політики закупівель, а також спрощує управління процесом закупівель, що в свою чергу прискорює відповідні процеси та сприяє підвищенню ефективності підприємства.

Модуль «Управління проектами та бухгалтерський облік» дозволяє керувати різними проектами та виконувати їх, а також налаштовувати проекти.

1.2 Аналіз структури безпекового фреймворку ERP – системи Dynamics AX

Виникнення нових видів загроз змушує розробників систем захисту адаптувати свої продукти до актуальних обставин. Якщо вчасно не реагувати на виникаючі загрози та запобігати їм, користі не буде навіть від сотні систем виявлення атак[4]. В Україні та світі все більше інформації доступно у базах даних: особиста інформація, лікарські документи, дипломи, реєстри документів тощо[5].

Dynamics AX представляє нову структуру безпеки, яка базується на моделі рольової безпеки. Ця структура розроблена, щоб полегшити підтримку безпеки в міру розвитку потреб організації в безпеці. Це також спрощує процес впровадження захисту базового рівня.

Системні адміністратори та розробники керують частинами нової системи безпеки. Розробники створюють і визначають артефакти безпеки, що забезпечують доступ до захищених об'єктів. Системні адміністратори постійно керують захистом користувачів.

Ви можете використовувати систему безпеки для створення артефактів безпеки, які контролюють доступ до форм, звітів, меню та пунктів меню. Dynamics AX також представляє нову розширювану систему захисту даних, яка дозволяє обмежувати доступ до конфіденційних даних на детальному рівні, щоб користувачі бачили лише ті дані, які необхідні для виконання своїх робіт.

Структури ліцензування та конфігурації дають можливість ліцензувати модулі програм, забезпечуючи таким чином доступ до різних областей програм. Ви також можете вмикати та вимикати функціональність незалежно від ліцензування, використовуючи конфігураційні ключі.

Система безпеки Dynamics AX складається з трьох рівнів: аутентифікація, авторизація та безпека даних.

Аутентифікація - це процес встановлення ідентифікації користувача. Користувачів Dynamics AX можна аутентифікувати двома способами. Перший спосіб - це використання інтегрованої автентифікації

Windows для аутентифікації користувачів Active Directory.

Другий спосіб автентифікації користувача називається гнучкою аутентифікацією. Завдяки гнучкій аутентифікації користувач може бути аутентифікований для використання веб-клієнта AX Enterprise Portal, не вимагаючи облікових даних Active Directory. Гнучка автентифікація використовує автентифікацію на основі претензій для перевірки користувачів на Enterprise Portal.

Авторизація, яка також називається контролем доступу, визначає, чи дозволено користувачеві виконувати певну дію.

Dynamics AX представляє нову структуру безпеки, яка називається розширюваною системою захисту даних (XDS), яку можна використовувати для управління доступом до даних транзакцій, призначаючи політику безпеки даних ролям безпеки. Політики захисту даних можуть обмежувати доступ до даних на основі дати набрання чинності або даних користувачів, таких як територія продажу або організація, до якої призначений користувач.

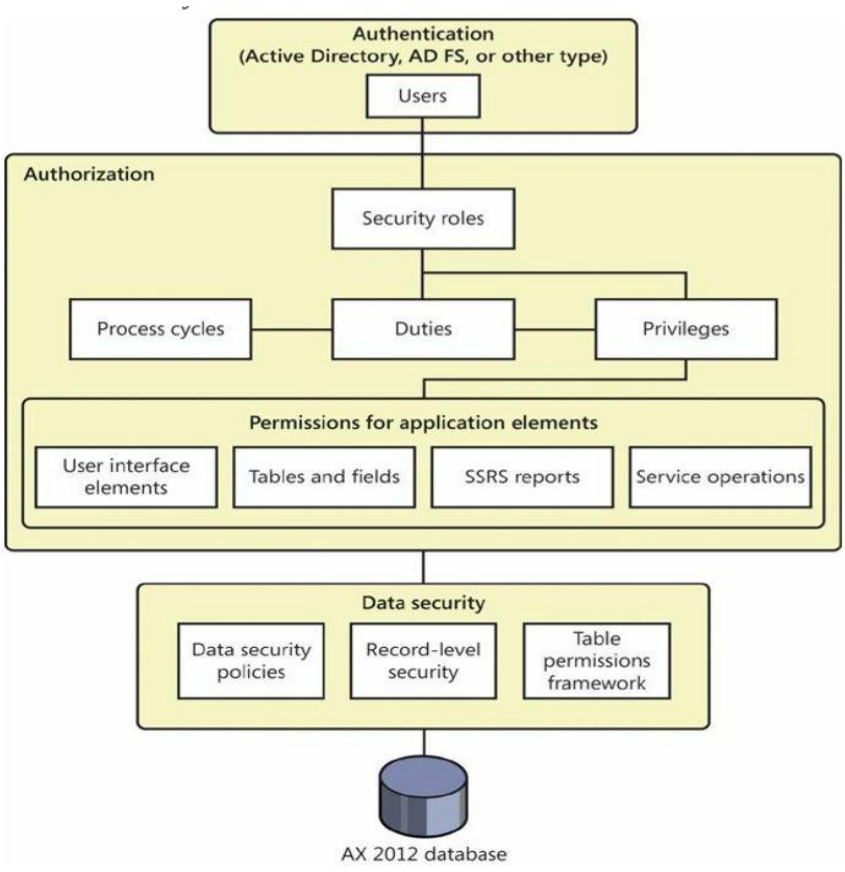


Рисунок 1.4 – Структура безпекового фреймворку системи

На додаток до XDS, ви можете використовувати рівень захисту для обмеження доступу до даних, що базується на запиті. Однак, оскільки в майбутньому випуску Microsoft Dynamics AX функція захисту рівня запису буде застарілою, рекомендується замість неї використовувати XDS.

Бізнес-процес - це скоординований набір видів діяльності, в ході яких один або кілька учасників споживають, виробляють та використовують економічні ресурси для досягнення організаційних цілей. У контексті моделі безпеки бізнес-процеси називаються циклами процесів.

Щоб допомогти системному адміністратору знайти обов'язки, які повинні бути призначені для ролей, обов'язки організовані за бізнес-процесами, до яких вони належать. Наприклад, у циклі процесу бухгалтерського обліку ви можете знайти ведення бухгалтерських книг та ведення обов’язків банківських операцій. Цикли процесів використовуються лише для організації. Крім того, Dynamics AX має систему дозволів для захисту даних. Структура дозволів для таблиць дозволяє забезпечити захист даних для певних таблиць Сервером об’єктів додатків (AOS). Явні перевірки авторизації виконуються, коли користувач намагається отримати доступ до даних, що стосуються таблиць, які захищені рамками дозволів для таблиці. Доступ до захищеного об'єкта в Dynamics AX контролюється за допомогою різних артефактів безпеки, таких як дозволи, привілеї, обов'язки, ролі та політики.

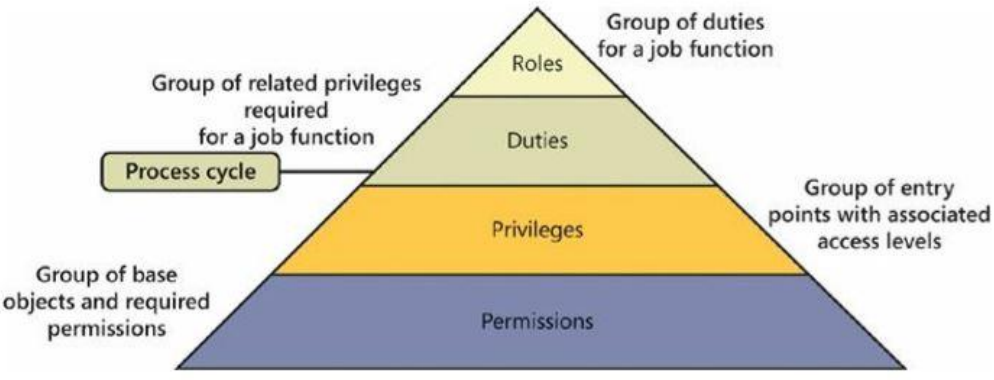


Рисунок 1.5 – Артефакти безпекової моделі в Dynamics AX

1.3 Основні компоненти безпекової моделі та їх призначення

Щоб гарантувати захист даних у системі, Microsoft Dynamics пропонує модель безпеки, засновану на суворому розподілі ролей. Це означає, що це не окремі користувачі, які мають певний рівень доступу до даних, а швидше ролі безпеки. Це економить час адміністраторам, яким згодом не потрібно керувати доступом для кожного окремого користувача.

Користувачі отримують доступ лише до рівня інформації, необхідної для своєї робочої діяльності. Це досягається за допомогою категоризації ролей користувача, розробленої відповідно до структури вашого бізнесу.

Усі користувачі повинні бути призначені щонайменше для однієї ролі захисту (у разі необхідності їх може бути більше однієї), і, якщо є потреба, команди можуть бути призначені власниками певних записів чи організацій, тим самим забезпечуючи всім членам команди однаковий рівень доступу. Рольова модель безпеки є ієрархічною. З одного боку, існує ієрархія ролей, що означає, що деякі з них (звані "дочірніми ролями") можуть бути безпосередньо пов'язані з іншими (називаються "батьківські ролі"). Наприклад, роль менеджера з продажу може бути батьком ролі продавця. Авторизація, яка також називається контролем доступу, визначає, чи дозволено користувачеві виконувати певну дію.

У Dynamics AX дозволи безпеки використовуються для управління доступом до окремих елементів програми: меню, пунктів меню, кнопок дій та команд, звітів, сервісних операцій, елементів меню веб-URL, веб-елементів керування та полів як в Dynamics AX клієнт Windows та на Enterprise Portal. І навпаки, існує інший вид ієрархії, який пропонує різні рівні специфікації для елементів, що контролюють доступ до компонентів системи. Це означає, що всі ролі Dynamics 365 мають набір пов'язаних з цим обов'язків, що відповідають бізнес- діяльності конкретної компанії. Обов'язки містять привілеї, що визначають рівень доступу до даних компанії для кожного користувача. Привілеї, у свою чергу,

містять дозволи для окремих складових заявок.

Рисунок 1.6 – Ієрархія артефактів безпекової моделі

Ролі безпеки визначають, які частини користувальницького інтерфейсу працівник може переглядати та працювати. У межах кожної ролі різні рівні доступу до даних можуть бути призначені індивідуально.

Вони визначають, що користувач може, а що не може робити в межах кожної сутності. Існує 5 рівнів доступу до ролей захисту Dynamics 365: жоден, базовий, локальний (бізнес-одиниця), глибокий (батьківський) та глобальний (організація). Dynamics 365 Finance пропонує спрощений підхід до розробки ролей користувачів порівняно з попередніми версіями MD ERP.

Завдяки Dynamics 365 Finance and Operations, ролі безпеки, необхідні для виконання будь-якого завдання, можна було визначити лише за допомогою набору інструментів розвитку безпеки, який вимагав встановлення системними адміністраторами. Тепер вони можуть використовувати вбудований інструмент діагностики безпеки, який визначає всі ролі, обов'язки та привілеї, необхідні для виконання певного завдання.

У AX 2012 нова модель безпеки відповідає принципам рольового контролю доступу. Ця модель безпеки є ієрархічною, кожен елемент в ієрархії представляє різний рівень деталізації. Дозволи представляють доступ до окремих захищених об’єктів, таких як пункти меню та таблиці.

Привілеї складаються з дозволів і представляють доступ до таких завдань, як скасування платежів або обробка депозитів. Обов'язки складаються з привілеїв і представляють частини бізнес-процесу, наприклад, ведення банківських операцій. Ролі складаються з обов'язків (а іноді і

привілеїв), які визначають доступ користувача до AX 2012. Ці ролі відповідають ролям в організації, наприклад, бухгалтеру чи менеджеру з управління персоналом.

Кожна роль має набір покладених на неї обов'язків. Обов'язки відображають бізнес-процеси, характерні для кожної компанії, які призначаються адміністратором. Один обов'язок може відповідати більш ніж одній ролі. Коли пов’язані обов'язки покладаються на окремі ролі, вони "відокремлюються". Розподіл обов'язків допомагає компанії слідувати нормативним вимогам, таким як Міжнародні стандарти фінансової звітності, серед інших, специфічні для кожної компанії, галузі та місця розташування.

При призначенні певної ролі користувач отримує доступ до пов'язаного з ним набору привілеїв. Вони можуть бути віднесені безпосередньо до ролі або до певного обов'язку. Привілеї через визначений рівень доступу дозволяють користувачам виконувати конкретні завдання (наприклад, створювати, читати, писати, видаляти тощо). Для кожного привілею існує набір пов'язаних дозволів.

Всього існує 7 типів ролей в Dynamics AX:

- Primary owner;
- Owner;
- Admin;
- Editor;
- Contributor;
- Viewer;
- Billing.

Primary owner - особа, яка створює обліковий запис, автоматично стає первинним власником. Вони мають повний контроль над обліковим записом, і лише вони можуть передавати право власності іншому користувачеві. На відміну від інших ролей, на акаунті може бути лише один первинний власник.

Owner - старші менеджери команди, відповідальні за додавання нових користувачів, підтримку існуючих користувачів та виставлення рахунків,

можуть бути додані як власники. Власники мають майже повний контроль над обліковим записом. В обліковому записі може бути кілька власників.

Admin - технічні адміністратори мають повний контроль над файлами в обліковому записі. Вони можуть призначити нових користувачів та змінити існуючі ролі користувачів, крім ролей власника. Вони не можуть переглядати та не керувати будь-якою платіжною інформацією.

Editor - ця роль надає доступ до щоденних операцій з управління файлами (завантаження, видалення, перейменування, переміщення та копіювання). Редактори не можуть спорожнити кошик, тож якщо файли видалено помилково, власник або користувач адміністратора може отримати їх протягом 30 днів. Якщо папка заблокована, редактори та дописувачі не можуть видалити, перейменувати чи перезаписати будь-який із своїх файлів чи папок. Contibutor - користувач з обмеженою роллю може додавати вміст у ваш обліковий запис - завантажувати та створювати нові папки та файли.

Viewer - дуже обмежена роль, програма перегляду може лише переглядати файли та завантажувати їх.

Billing - ідеально підходить для фінансів та бухгалтерії, ця роль надає повну можливість оплати та виставлення рахунків з мінімальною можливістю файлів.

Table of roles and permissions

	Primary Owner	Owner	Admin	Editor	Contributor	Viewer	Billing
File management							
View files/folders	✓	✓	✓	✓	✓	✓	✓
Download files/folders	✓	✓	✓	✓	✓	✓	✓
Download CSV lists	✓	✓	✓	✓	✓	✓	✓
Create folders	✓	✓	✓	✓	✓	✗	✗
Upload files/folders	✓	✓	✓	✓	✓	✗	✗
Move files/folders	✓	✓	✓	✓	✗	✗	✗
Copy files/folders	✓	✓	✓	✓	✗	✗	✗
Rename files/folders	✓	✓	✓	✓	✗	✗	✗
Delete files/folders	✓	✓	✓	✓	✗	✗	✗
Share folders	✓	✓	✓	✓	✗	✗	✗
Empty trash	✓	✓	✓	✗	✗	✗	✗
Lock/unlock folders	✓	✓	✓	✗	✗	✗	✗
Change folder settings	✓	✓	✓	✗	✗	✗	✗

Рисунок 1.7 – Повноваження ролей

Висновки до першого розділу

Dynamics AX – ERP - система, яка дозволяє автоматизувати роботу підприємства будь – яких масштабів, в незалежності від специфіки його роботи. Дана система є багаторівневим застосунком, котрий містить в собі спектр готових рішень та функціональних модулів, котрі емулюють ті чи інші процеси на виробництві. Безпекова модель Dynamics AX реалізується безпековим фреймворком Extensible data security, який дає можливість виконати налаштування політики безпеки будь – якої складності.

Політика безпеки реалізується за допомогою надання привілегій доступу до тих чи інших об’єктів системи для певних користувачів, для яких задається певна роль. На примітивному рівні провести розмежування доступу можна за допомогою створення відповідних об’єктів – артефактів та коректного їх налаштування в залежності від специфіки політики безпеки.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ПОВЕДІНКИ ЗАХИЩЕНИХ ОБ'ЄКТІВ В MICROSOFT DYNAMICS AX

2.1 Основні об'єкти ERP – системи, що підлягають захисту

В ERP – системі Dynamics AX безпекова модель здатна забезпечити розмежування доступу до різноманітних об'єктів. Проте за для реалізації базової політики безпеки окремого модуля достатньо захистити такі об'єкти як:

- Таблиці;
- Форми;
- Елементи меню.

Таблиці є основними об'єктами в Microsoft Dynamics AX і зберігають дані, що використовуються системою. Таблиця складається із записів (або рядків), які містять інформацію про один запис у таблиці. Наприклад, конкретний клієнт чи товар. Запис складається з одного або декількох полів (або стовпців), які містять дискретний шматок даних певного типу даних.

У Microsoft Dynamics AX таблиці розташовані в дереві об'єктів (AOT). Назва таблиці може містити літери та цифри, але повинна починатися з букви. Пробіли та спеціальні символи заборонені. Кожна таблиця містить такі основні елементи:

- Поля;
- Групи полів;
- Індекси;
- Зв'язки;
- Методи;
- Методи видалення;

Вузол «Поля» містить усі поля в таблиці. Вказуючи тип даних поля, ви визначаєте тип даних, які можна зберігати в ньому. Microsoft Dynamics AX виконує перевірку даних, щоб гарантувати, що в кожне поле таблиці вводяться лише дійсні дані. Обмеження також додаються до бази даних для встановлення значень полів за замовчуванням, якщо поле залишається порожнім.

Кожне поле таблиці має ряд властивостей, що описують поведінку поля. Властивість Type містить власний тип даних поля. Коли створюється нова таблиця, системні поля автоматично додаються до кожної таблиці. Ці поля є в таблиці бази даних, але їх не видно у вузлі полів. Системні поля, які додаються до таблиці, залежать від значення певних властивостей таблиці, як показано в наступній таблиці.

Індекс - це специфічна для таблиці структура бази даних, яка прискорює пошук рядків із таблиці. Індекси використовуються для підвищення ефективності пошуку даних, а іноді і для забезпечення існування унікальних записів. Використання доступних індексів для полегшення ефективного пошуку даних залежить від специфічного оптимізатора запитів до бази даних.

Властивість AllowDuplicates в індексі має найбільший вплив на те, як використовується індекс. Якщо встановлено значення «ні», система створює унікальний індекс за вказаними полями бази даних.

Microsoft Dynamics AX вимагає унікального індексу для кожної таблиці. Якщо в таблиці немає індексів або всі індекси відключені, автоматично створюється системний індекс. Системний індекс створюється в полях RecId і DataAreaId, якщо існує поле DataAreaId. В іншому випадку в полі RecId створюється системний індекс. Ви можете бачити системні індекси в базі даних, але вони не видно в AOT. Якщо в таблиці є індекси, але жоден з них не є унікальним, час виконання оцінює середню довжину ключа існуючих індексів, вибирає індекс із найменшою довжиною ключа, а потім додає стовпець RecId для створення унікального індексу.

Зв’язки визначають відношення між двома таблицями, які містять пов'язані дані. Табличні відносини використовуються для забезпечення

посилальної цілісності серед інших функцій. Табличні зв’язки найчастіше використовуються у полях форми, щоб забезпечити пошук інформації в іншій таблиці.

Методи видалення використовуються для підтримки узгодженості бази даних при видаленні запису. Визначте дії видалення, щоб вказати, що має відбуватися, коли дані, що видаляються в поточній таблиці, пов’язані з даними іншої таблиці.

Значення методів видалення можуть бути наступними:

- None;
- Cascade;
- Restricted;
- Cascade + Restricted.’

Вузол «Методи» відображає всі методи, доступні з таблиці. Даний вузол дозволяє додати новий метод або замінити методи в класі ядра таблиці та додати свій власний код. Методи забезпечують можливість додавання коду X ++ до таблиць. Наприклад, ви можете додати код, щоб відтворити функціональність тригерів SQL Server для методів оновлення та вставки або надати більш складні процедури під час видалення даних. Можливості, які методи надають для функціональності стандартної таблиці - безмежні. Ви можете впровадити складні бізнес-правила, перевірки, пошуку тощо.

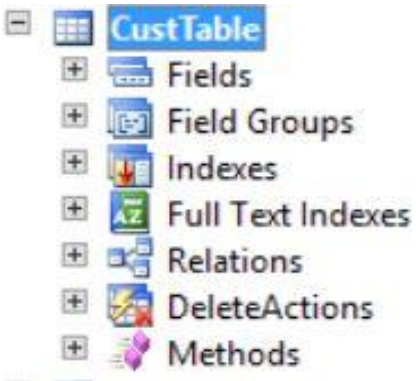


Рисунок 2.1 – Вигляд таблиці та її складових елементів в системі

Таблиця AX трактується як об'єкт і можуть бути створені нові статичні методи для реалізації функцій пошуку. Поширеним прикладом є метод пошуку, який реалізований у більшості стандартних таблиць AX у системі. Ви також можете розширити функціональність стандартного методу таблиці, використовуючи успадкування, яке є концепцією, що використовується об'єктно-орієнтованим програмуванням. Таблиці AX подібні до таблиць SQL Server тим, що дані зберігаються у стовпцях і рядках. Фактично, зберігаючи зміни до таблиці AX, AX синхронізує ці зміни з базою даних SQL Server і зрештою, створює таблицю SQL Server. Окрім всіх цих складових, кожна таблиця в системі містить набір параметрів, котрі дозволяють провести детальне налаштування даних що циркулюють в ній.

Меню параметрів таблиці зображено на рисунку 2.2:

Рисунок 2.2 – Меню параметрів таблиці в системі

Окрім зміни параметрів з користувацького інтерфейсу, є можливість звертатись до параметрів таблиці з коду. У Microsoft Dynamics AX 2012 таблиці можуть успадковувати або розширювати таблиці, розташовані над ними в ієрархії. Базова таблиця містить поля, загальні для всіх таблиць, які з неї походять. Похідна таблиця успадковує ці поля, але також містить поля,

унікальні для її призначення. Кожна таблиця містить властивості Support Inheritance and Extends, які можна використовувати для управління успадкуванням таблиці. Щоб полегшити ідентифікацію записів у таблицях AX та уникнути дублікатів, AX додає стовпець до кожної таблиці з назвою RecId. Стовпець RecId - це 64-розрядний цілий стовпець, якому автоматично присвоюється унікальний номер у таблиці щоразу, коли створюється новий запис. Після призначення стовпець RecId не можна редагувати за допомогою інтерфейсу AX. Стовпець RecId не є полем автоматичного збільшення SQL Server, і номер, присвоєний запису, генерується системою AX. Якщо ви вставите запис за допомогою інструментів запитів SQL Server, стовпець RecId залишиться порожнім.

Окрім стандартних таблиць, Dynamics AX дозволяє створювати тимчасові таблиці типу InMemory та TempDB. AX 2012 також підтримує функціональність тимчасових таблиць. У попередніх випусках Microsoft Dynamics AX надавала можливість створювати тимчасові таблиці InMemory, які зіставляються з файловою таблицею індексованого методу послідовного доступу (ISAM), яка доступна лише під час виконання сервера об'єктів додатків (AOS) або клієнт. AX 2012 пропонує новий тип тимчасової таблиці, яка зберігається в базі даних TempDB у Microsoft SQL Server.

Файл ISAM, що представляє тимчасову таблицю InMemory, містить дані та всі індекси, визначені для таблиці в AOT. Оскільки робота з меншими наборами даних, як правило, швидша, ніж робота з більшими наборами даних, середовище виконання AX 2012 контролює розмір кожної тимчасової таблиці InMemory. Якщо розмір менше 128 кілобайт (КБ), тимчасова таблиця залишається в пам'яті. Якщо розмір перевищує 128 КБ, тимчасова таблиця записується у фізичний файл ISAM. Перехід з пам'яті на фізичний файл суттєво впливає на продуктивність.

Хоча тимчасові таблиці InMemory не співпадають з реляційною базою даних, усі оператори мови обробки даних (DML) у X ++ дійсні для таблиць, які працюють як тимчасові таблиці InMemory. Однак середовище виконання AX

2012 виконує деякі оператори зі зниженням, оскільки функціональність файлу ISAM не пропонує таку ж функціональність, як реляційна база даних. Наприклад, оператори, що базуються на наборах, завжди виконуються як операції "запис за записом". Коли оголошується буфер запису для тимчасової таблиці InMemory, таблиця не містить жодних записів. Для роботи з таблицею потрібно вставити записи. Тимчасова таблиця InMemory та всі записи втрачаються, коли жоден з оголошених буферів записів не вказує на тимчасовий набір даних. Пам'ять і простір файлів не виділяються до тимчасової таблиці InMemory, доки не буде вставлено перший запис. Тимчасова таблиця розташована на рівні, куди було вставлено перший запис. Наприклад, якщо перша вставка відбувається на рівні сервера, пам'ять виділяється на цей рівень, і врешті-решт тимчасовий файл буде створений на рівні сервера[6]. Методи запуску бази даних у тимчасових таблицях поводяться майже так само, як і у звичайних таблицях, але за невеликими винятками. Коли вставка, оновлення та видалення викликаються в тимчасовому буфері записів, вони не викликають жодного з методів реєстрації бази даних або створення подій для класу програми, якщо для таблиці було налаштовано журналювання бази даних або попередження. Коли винятки викидаються і перехоплюються поза межами транзакції, якщо середовище виконання AX 2012 вже викликало оператор ttsabort, тимчасові дані не відкочуються. Код програми в AX 2012 часто використовує тимчасові таблиці для проміжного зберігання. Для цього потрібні об’єднання зі звичайними таблицями та, в деяких випадках, операції на основі наборів. Але тимчасові таблиці InMemory надають обмежену підтримку приєднання. Ці об'єднання виконуються рівнем даних в AOS, що не дає ідеальної продуктивності. Крім того, як уже згадувалося раніше, операції на основі наборів завжди знижуються до операцій рядка за рядками для таблиць InMemory. Тимчасові таблиці TempDB були додані до AX 2012, щоб забезпечити високопродуктивне рішення для цих сценаріїв. Оскільки ці тимчасові таблиці зберігаються в базі даних SQL Server, можна

використовувати такі операції з базами даних, як об'єднання.

Тимчасові таблиці TempDB використовують ті самі конструкції програмування X ++, що і тимчасові таблиці InMemory. Ключова відмінність полягає в тому, що вони зберігаються в базі даних SQL Server TempDB. Форма є основною одиницею відображення у клієнта. Типова форма відображає поля, які відображають поточний запис та кнопки, що представляють дії, які користувач може виконати з цим записом, і механізм зміни того, який запис відображається. Повноцінне створення форми в Dynamics AX потребує:

1. Створення об’єкту форми в системі;
2. Створення джерел даних (таблиць та інших структур за для відображення інформації);
3. Створення функціональних контролів для управління формою;
4. Створення методів контролів, форми або джерел даних, в залежності від функціоналу, котрий дана форма реалізує;
5. Додавання логіки в класи, котрі пов’язані з формами;
6. Створення вкладених форм.

Вигляд стандартної форми в користувацькому інтерфейсі, зображений на рисунку 2.3

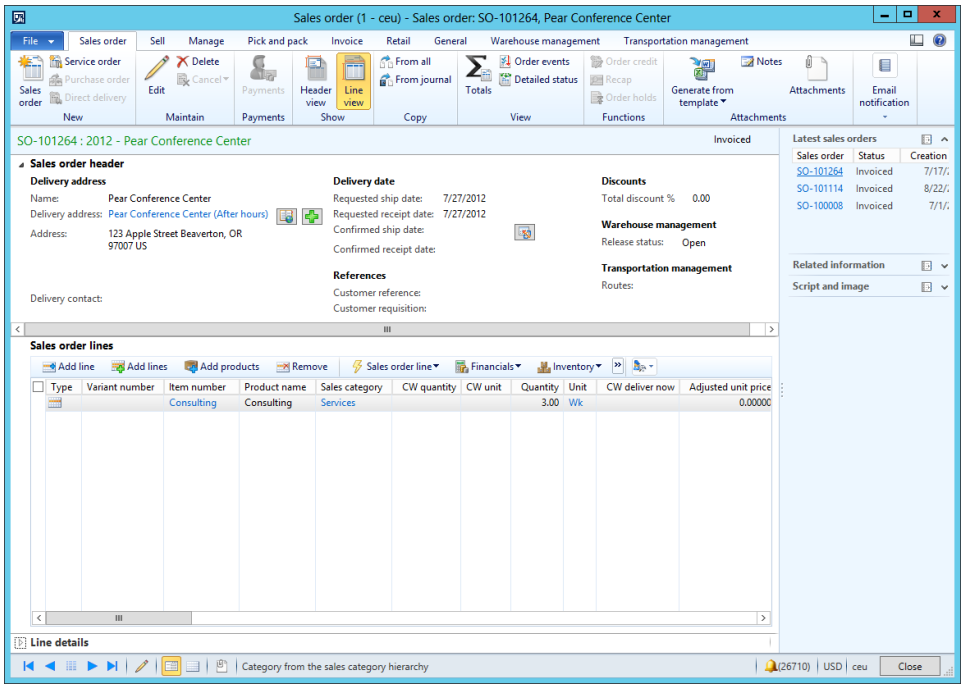


Рисунок 2.3 – Форма «Ордер на продаж»

У попередніх версіях Microsoft Dynamics AX існували неформальні шаблони для розробки форм. У AX 2012 було формалізовано кілька шаблонів форм, які надаються як шаблони.

До основних типів форм в Dynamics AX відносяться:

- List page;
- Drop dialog;
- Dialog;
- Details form;
- Simple list;
- Simple list and details;
- Table of contents;

Метадані форми у AX 2012 є достатньо великими, але вони добре структуровані та прості в роботі, що дає можливість створювати різноманітні рішення. Налаштування метаданих є кращим перед налаштуванням коду, оскільки зміни метаданих (їх також називають дельтами) легше об'єднати, ніж зміни коду. Щоб забезпечити найбільший рівень повторного використання, будь-які зміни, внесені в метадані, повинні вноситися на найнижчий можливий рівень - наприклад, у таблиці.

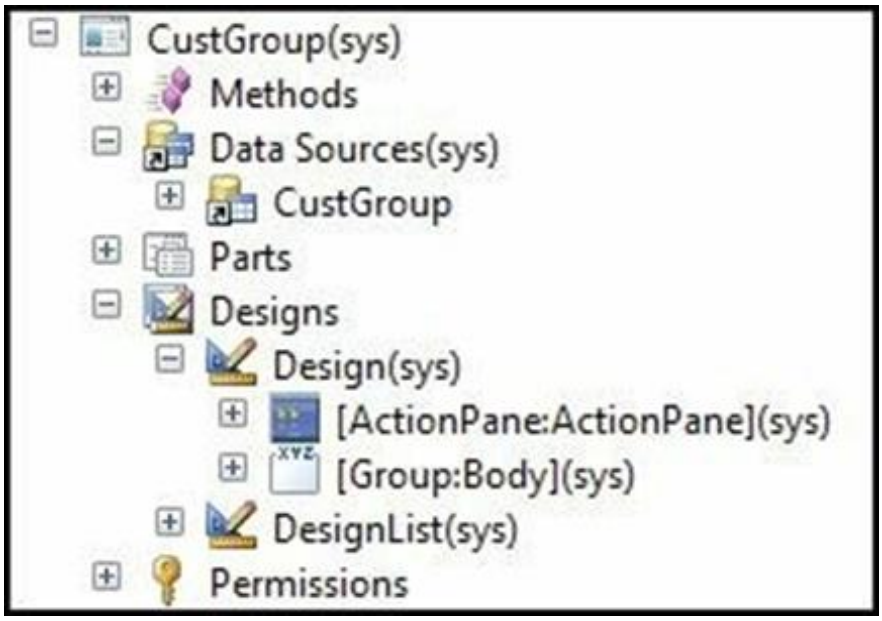


Рисунок 2.4 – Метадані форми в системі

Джерело даних форми вказує на певну таблицю чи іншу структуру, котра містить в собі структуровані дані. Список полів у джерелі даних форми автоматично заповнюється полями, визначеними у ресурсі, на який він посилається. З цього списку можна прив'язати елементи керування до тих полів або будь-якого з методів даних, що існують у таблиці або джерелі даних форми. AX 2012 має детальну структуру доступу до даних, яка спрощує додавання даних, форматування та прив'язування елементів керування до цих даних. Основою цього є джерело даних форми, яке дозволяє прив'язувати таблиці та поля до форми. Джерело даних форми вказує на певну таблицю, карту чи подання. Список полів у джерелі даних форми автоматично заповнюється полями, визначеними у ресурсі, на який він посилається. З цього списку можна прив'язати елементи керування до тих полів або будь-якого з методів даних, що існують у таблиці або джерелі даних форми.

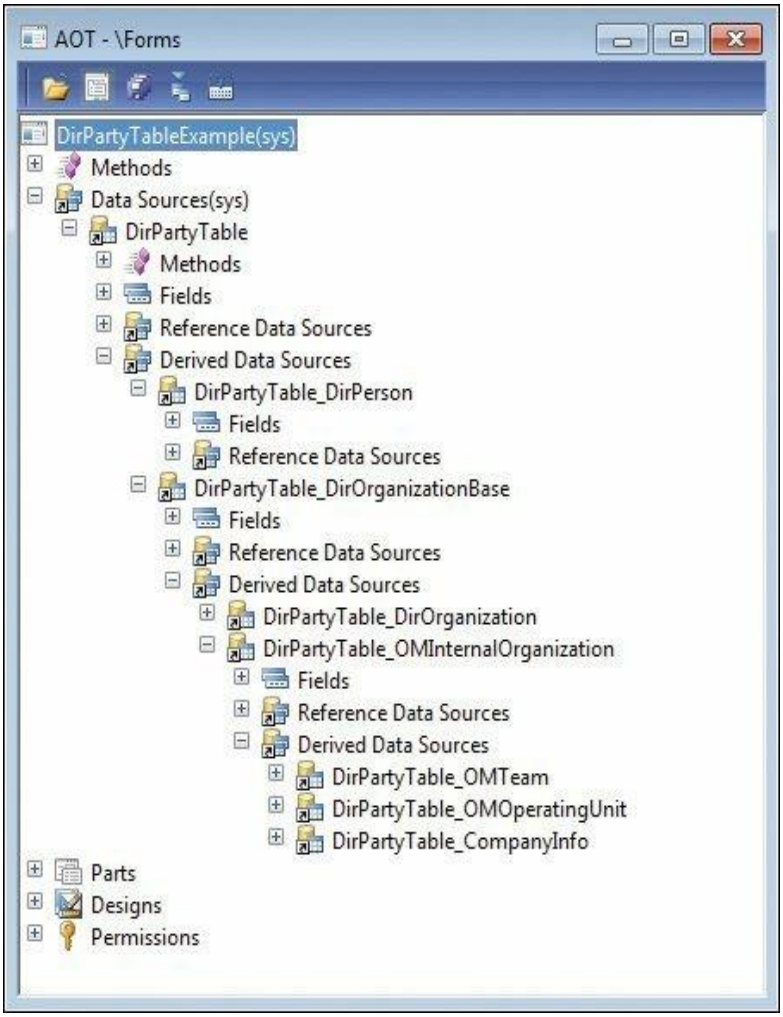


Рисунок 2.5 – Форма з вкладеними джерелами даних

Джерела даних форми можна поділити на наступні групи:

- Кореневі джерела даних;
- Мастер – дата;
- Поєднані джерела даних;
- Посилання.

Завдяки тому що в форму можна вкладати безліч джерел даних, спрощується завдання створення потужних модулів, котрі обробляють велику кількість різноманітних даних.

AX 2012 включає великий вибір елементів керування, за допомогою яких можна швидко створювати керовані даними форми. Додаючи елементи керування у форму, необхідно встановлювати якомога менше властивостей, щоб елементи керування могли повною мірою використовувати переваги за замовчуванням та автоматичні значення. Значення властивостей за замовчуванням на елементах керування дозволяють AX 2012 використовувати заздалегідь визначену функціональність під час визначення характеристик та поведінки дисплея.

Використовуючи елемент керування Group, можна організувати пов’язані поля та інші елементи керування у логічні групи у формі. Окрім цього, можна створити та позначити елемент керування групою вручну (за допомогою властивості Caption) та створити елемент керування Group, використовуючи властивість DataGroup, щоб вказати на групу полів, яку було попередньо визначено в таблиці (джерело даних).

Рекомендовано використовувати групи полів таблиці, коли це можливо. Групи полів таблиці дозволяють полегшити обслуговування програми, оскільки зміна групи полів таблиці впливає на кожну форму або звіт, що використовує цю групу полів.

При ручному створенні елементів керування обов’язково необхідно надавати описовий та зрозумілий підпис, який точно описує групу, а також її призначення на формі.

Елементи меню незамінна частина в ERP - системи AX 2012. В системі використовуються як елементи відображення та елементи дії. Елементи відображення використовуються для переходу до форми в клієнті AX 2012, яка відображає деталі запису, що обробляється робочим процесом. Елементи веб-меню використовуються для переходу до того самого типу веб-сторінки на Enterprise Portal. Пункти меню дій використовуються для кожної можливої дії, яку користувач може виконати щодо робочого процесу. Вони також надають ще одну точку інтеграції для інтеграції власного коду.

Функціонально елементи меню в системі можна розділити на такі 3 види:

- Елементи – відображення;
- Елементи – дії;
- Елементи – демонстрації;

Елементи відображення Dynamics AX 2012 використовуються для посилання на такі об’єкти, як форми та діалоги. Основна мета пунктів меню цього типу полягає в тому, що вони використовуються для подання даних. Елементи –демонстрації використовуються для виводу результатів запиту в базу даних чи виводу інших даних що циркулюють в системі. Також ці елементи використовуються для посилань на класи.

Елементи – дії використовуються у випадках, коли вам потрібно виконати певну дію на основі натискання на елемента меню. Наприклад, якщо потрібно запустити функцію в класі одним натиском миші. Хорошим прикладом цього може бути дія оновлення сьогоднішніх замовлень.

Основними параметрами елементів меню в системі є :

- Ім’я;
- Конфігураційні налаштування;
- Опис;
- Тип виконання;
- Параметр з яким виконується елемент меню;
- Параметр - безпеки;

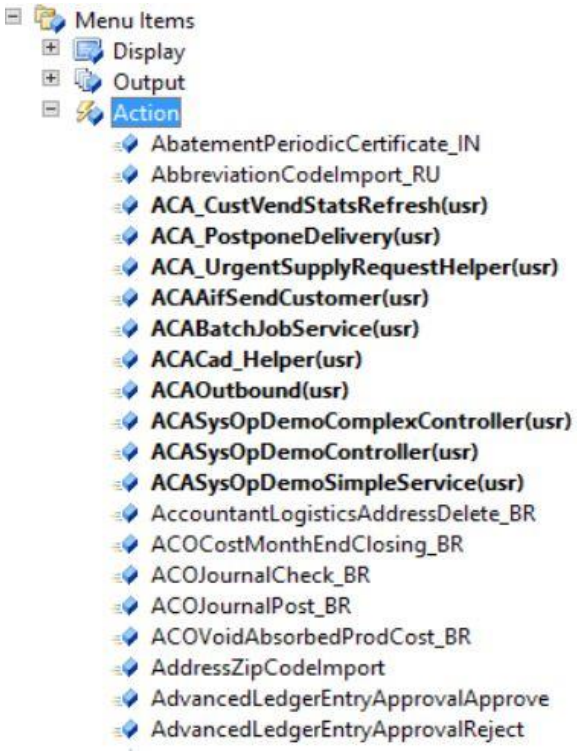


Рисунок 2.6 – Меню елементи в системі

Проте на універсальність усіх видів елементів меню, елементи – дії прийнято використовувати для запуску класів в системі, елементи – відображення для запуску форм, елементи – демонстрації для відображення звітів в системі.

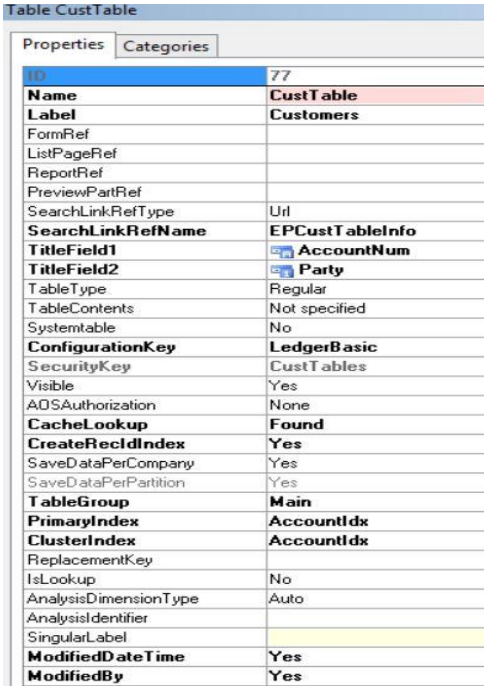


Рисунок 2.7 – Меню параметрів елементу

2.2. Налаштування захисту об’єктів ERP – системи

AX 2012 представляє нову структуру безпеки, яка називається розширюваною системою захисту даних (XDS), яку можна використовувати для управління доступом до транзакційних даних, призначаючи політики безпеки даних ролям безпеки. Політики захисту даних можуть обмежувати доступ до даних на основі дати набрання чинності або даних користувачів, таких як територія продажу або організація, до якої призначений користувач.

На додаток до XDS, можна використовувати захист на рівні запису, щоб обмежити доступ до даних, що базується на запиті. Однак, оскільки в майбутньому випуску Microsoft Dynamics AX функція захисту рівня запису буде застарілою, рекомендується використовувати XDS[7].

Крім того, AX 2012 має систему дозволів для захисту даних. Структура дозволів для таблиць дозволяє забезпечити захист даних для певних таблиць сервером об’єктів додатків (AOS). Явні перевірки авторизації виконуються, коли користувач намагається отримати доступ до даних, що стосуються таблиць, які захищені рамками дозволів для таблиці. Доступ до захищених об'єктів в AX 2012 контролюється за допомогою різних артефактів безпеки, таких як дозволи, привілеї, обов'язки, ролі та політики. Ви можете створювати та керувати цими артефактами, використовуючи дерево об’єктів додатків (AOT).

Рисунок 2.8 - Артефакти безпеки в дереві додатків

При побудові політики безпеки, впершу чергу необхідно вирішити питання захисту форм. Першим кроком є контроль доступу до даних у

формі. Коли ви зберігаєте форму в AOT, AX 2012 автоматично виявляє всі таблиці та інші елементи, до яких форма звертається. Ця функціональність називається автоматичним висновком. Автовисновок спрощує налаштування дозволів для таблиці. На основі таблиць, які використовуються у формі, дозволи на створення, читання, оновлення та видалення (CRUD) встановлюються автоматично для цієї форми.

Розмежування доступу до об’єкту, забезпечується заданням привілегій(режиму доступу) до нього. Й в залежності, від ролі користувача й привілегії котра задана для нього для доступу до цього об’єкта, він буде отримувати певний рівень доступу до нього.

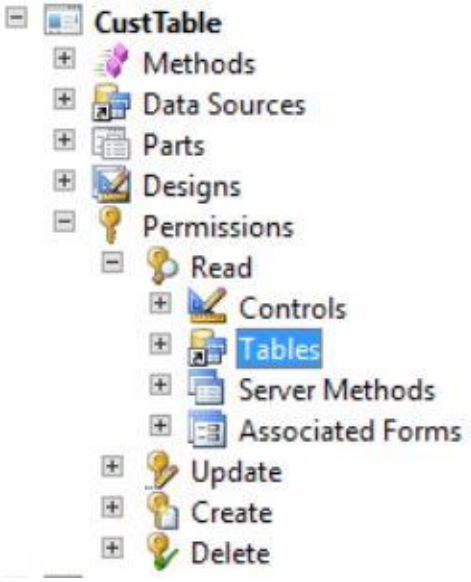


Рисунок 2.9 – Список привілегій для форми

Привілегії доступу до об’єкта в Dynamics AX бувають наступними:

- Create;
- Read;
- Write;
- Delete;
- Append;
- Append To;
- Assign;

- Share;

Create – дає можливість створити новий запис. Які записи можна створити, залежить від рівня доступу дозволу, визначеного у вашій ролі безпеки. Read –дає можливість відкрити запис для перегляду вмісту. Які записи можна прочитати, залежить від рівня доступу дозволу, визначеного у вашій ролі безпеки. Write – дає можливість внести зміни до запису. Які записи можна змінити, залежить від рівня доступу дозволу, визначеного у вашій ролі безпеки.

Delete – дає можливість назавжди видалити запис. Які записи можна видалити, залежить від рівня доступу дозволу, визначеного у вашій ролі безпеки. Append - дає можливість пов’язати поточний запис з іншим записом. Наприклад, примітка може бути додана до можливості, якщо користувач має права на додавання до нотатки. Записи, які можна додати, залежать від рівня доступу дозволу, визначеного у вашій ролі безпеки. У випадку відносин, що перебувають у багатьох до багатьох, ви повинні мати додаток привілею для того, щоб обидва суб'єкти були асоційовані або роз'єднані. Append to – дає можливість пов’язати запис з поточним записом. Наприклад, якщо у користувача є можливість додавати права на можливість, користувач може додати нотатку до цієї можливості. Записи, які можна додати, залежать від рівня доступу дозволу, визначеного у вашій ролі безпеки. Share – дає можливість надання доступу до запису іншому користувачеві, зберігаючи власний доступ. Які записи можна поділити, залежить від рівня доступу дозволу, визначеного у вашій ролі безпеки. Assign – надає право власності на запис іншому користувачеві. Які записи можна призначити, залежить від рівня доступу дозволу, визначеного у вашій ролі безпеки. Окрім цього, всі привілегії функціонально поділяються на 2 групи:

- Привілегії користувача;
- Привілегії команди;

Привілегії користувача надаються безпосередньо, коли користувачеві

призначена роль безпеки. Користувач може створювати та мати доступ до записів, створених користувачеві, коли був заданий базовий рівень доступу для створення та читання.

Привілеї команди надаються як пільги для члена команди. Для членів команди, які не мають власних привілеїв користувача, вони можуть створювати записи разом із командою як власником, і вони мають доступ до записів, що належать команді, коли був заданий базовий рівень доступу для створення та читання.

Користувачі отримують доступ лише до рівня інформації, необхідної для своєї робочої діяльності. Це досягається за допомогою категоризації ролей користувача, розробленої відповідно до структури вашого бізнесу.

Роль безпеки може бути встановлена для надання членам команди прямих прав користувальницького доступу на базовому рівні. Учасник команди може створювати власні записи, а також записи, які мають команду як власника, коли задано базовий рівень доступу для створення. Коли задано базовий рівень доступу для читання, член команди може отримати доступ до записів.

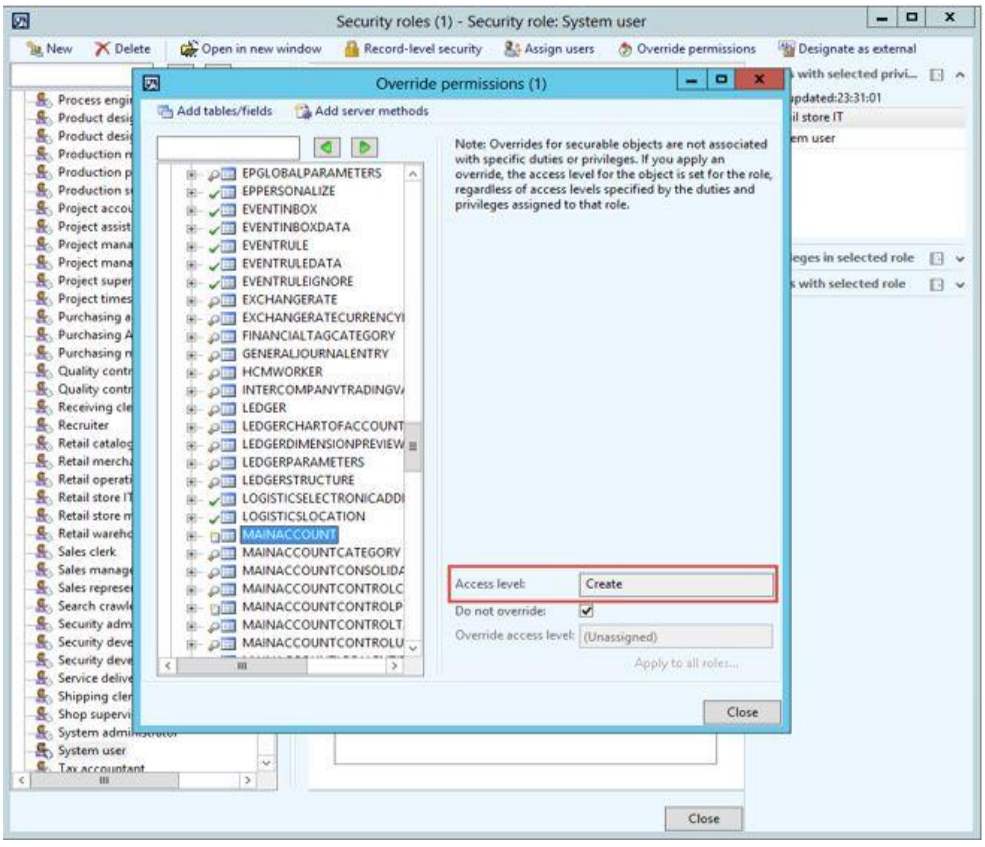


Рисунок 2.10 – Задання привілегії для певної ролі в системі

Після створення дозволів для різних захищених об'єктів необхідно надати доступ до цих захищених об'єктів через ролі безпеки. Першим кроком є створення привілеїв. Після цього необхідно включити ці привілеї в обов'язки або безпосередньо призначити їх ролям безпеки.

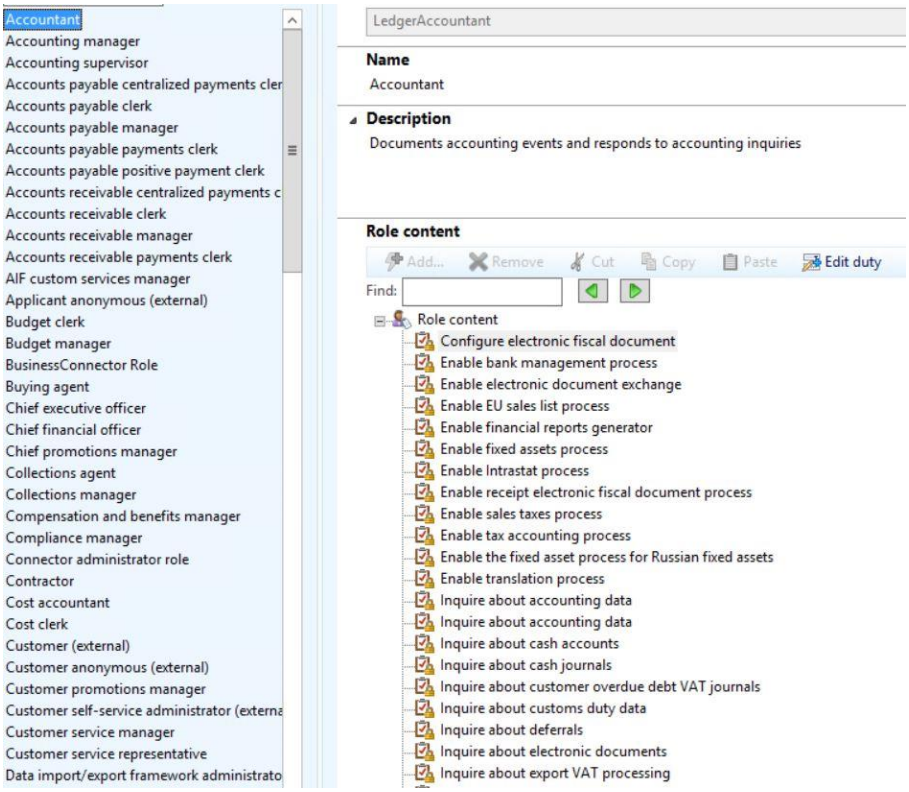


Рисунок 2.11 – Стандартні ролі для користувача «Accountant»

Усім користувачам повинна бути призначена принаймні одна роль безпеки, щоб мати доступ до Microsoft Dynamics AX. Ролі безпеки, призначені користувачеві, визначають обов'язки, які користувач може виконувати, та частини користувацького інтерфейсу, які користувач може переглядати. Адміністратори можуть застосовувати політики безпеки даних, щоб обмежити дані, до яких користувачі в ролі мають доступ. Наприклад, користувач у ролі може мати доступ до даних лише від однієї організації. Адміністратор також може вказати рівень доступу, який користувачі в ролі мають до поточних, минулих та майбутніх записів. Наприклад, користувачам у ролі можуть бути призначені привілеї, що дозволяють переглядати записи

за всі періоди, але дозволяють змінювати записи лише для поточного періоду.

2.3. Дослідження поведінки ERP - системи при несанкціонованому доступі до об’єктів

Безпекова модель AX 2012 при спробі доступу до об’єкту проводить ряд перевірок за для коректного відпрацювання розмежування доступу. Розмежування доступу проводиться при створенні політики безпеки системи, котру необхідно створити перед початком експлуатації системи в межах підприємства. Так як кількість користувачів в системі, а також ролей, в яких ці користувачі задіяні може бути достатньо великою надзвичайно важливо провести вірний розподіл прав до об’єктів в системі[8].

При спробі доступу до об’єкту або проведення певних маніпуляцій з даними на об’єкті безпекова модель перевіряє чи має право чинний користувач здійснювати ту чи іншу дію над об’єктом. Наприклад, якщо для ролі до якої відноситься користувач надана привілегія «Read», при спробі додати, видалити чи змінити будь – який запис на формі, система видасть повідомлення про помилку доступу, як це зображено на рисунку 2.12:

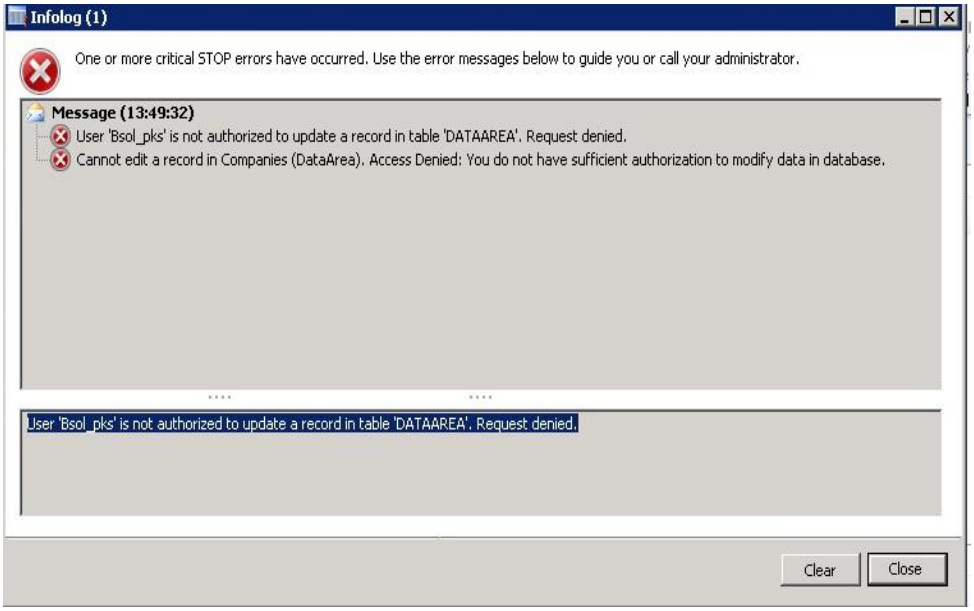


Рисунок 2.12 – відмова в доступі до об’єкту

Повідомлення про помилку містить інформацію про джерело даних (таблицю) в котру користувач намагався внести зміни, а також про низький рівень привілегій по відношенню до даної структури даних.

Висновки до другого розділу

Основними об’єктами, котрі потребують захисту в системі Dynamics AX 2012 є таблиці, форми та елементи меню. Адже, саме в таблицях циркулює більшість інформації підприємства, втрата чи модифікація якої може спричинити суттєві репутаційні та матеріальні збитки для підприємства. Форми та елементи меню в свою чергу призначені для більш зручної демонстрації даних що циркулюють в таблицях.

Захист об’єктів в Dynamics AX базується на роботі привілегій котрі надані певним ролям користувачів в системі. В залежності від типу привілегій, користувач отримує певні повноваження щодо модифікації та перегляду структур даних в системі. Суворе дотримання політики безпеки при розмежуванні доступу до об’єктів сприяє мінімізації можливості несанкціонованого доступу серед персоналу підприємства. AX 2012 надає можливість гнучкого налаштування безпекової моделі в залежності від потреб, роду діяльності та штату підприємства.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПОЛІТИКИ БЕЗПЕКИ ДЛЯ ОКРЕМОГО МОДУЛЮ ERP – СИСТЕМИ DYNAMICS AX

3.1 Огляд функціонального модуля «Академія»

Функціональний модуль ERP – системи «Академія» є розширенням стандартного функціоналу системи і не є стандарним модулем системи.

Перед його безпосередньою розробкою ставились наступні вимоги до модуля:

1) Реалізувати новий модуль "DAX Academy";
2) Реалізувати функціонал Certifications;
3) Реалізувати необхідні структури даних та UI (має бути доступним з меню модуля);
4) Реалізувати функцію (та додати її на форму сертифікацій) в вигляді Drop-dialog: "Change activity". Параметри: New state (Active/Inactive), Selected certifications (multi-select lookup, де за замовчанням вибрано активну сертифікацію, тобто, можна застосовувати до декількох сертифікацій). Відповідно, функція має змінювати стан поля Active сертифікації.
5) Реалізувати Number sequence модуль для модуля "DAX Academy". Має містити номерні серії для Exam Id та Student Id.
6) Реалізувати параметри модуля: Default student level (той рівень, з яким створюється запис нового академіста), Minimum number of exams for graduation (Мінімальна кількість екзаменів, що дозволить студенту випуститися, перейти в стан "Graduated"). Також форма параметрів має містити Tab для номерних серій модуля.
7) Реалізувати сутність та форму студента (форма - list page, доступна через 3 різні меню елементи: All students, Studying students (Level < Graduated), Graduated students (Level = Graduated).
8) Реалізувати сутність та форму "Exam score records", котра має бути доступна лише через меню елемент на students list page.

Функціонально модуль «Академія» складається з наступних об’єктів:

- Таблиця ACA_DAX_ExamScores;
- Таблиця ACA_DAX_Students;
- Таблиця ACA_DAX_Certifications;
- Таблиця ACA_DAX_Parameters;
- Форма ACA_DAX_StudentsEditForm;
- Форма ACA_DAX_Certification;
- Форма ACA_DAX_ExamScores;
- Форма ACA_DAX_ExamScoresLookUp;
- Форма ACA_DAX_ChangeActivity;
- Форма ACA_DAX_StudentsListPage;
- Форма ACA_DAX_StudentParameters;
- Елемент меню ACA_DAX_StudentParameters;
- Елемент меню ACA_DAX_AllStudents;
- Елемент меню ACA_DAX_ExamScores;
- Елемент меню ACA_DAX_Certification;
- Елемент меню ACA_DAX_GraduatedStudents;
- Елемент меню ACA_DAX_StudentEditForm;
- Елемент меню ACA_DAX_ChangeActivityDropDialog;
- Елемент меню ACA_DAX_StudyingStudents;
- Клас ACA_DAX_StudentListPageInteraction;
- Клас ACA_DAX_NumberSeqModule;
- Розширений тип даних ACA_DAX_Score;
- Розширений тип даних ACA_DAX_Name;
- Розширений тип даних ACA_DAX_StudentId;
- Розширений тип даних ACA_DAX_ExamsId;
- Розширений тип даних ACA_DAX_StudentStatus;
- Розширений тип даних ACA_DAX_NewState;
- Розширений тип даних ACA_DAX_AcademyStudLevel;

Користувачі мають доступ до модулю з користувацього інтерфейсу, а саме через головне меню ERP – системи Dynamics AX 2012. Вибрати користувацький модуль можна з поміж списку вбудованих модулів системи.

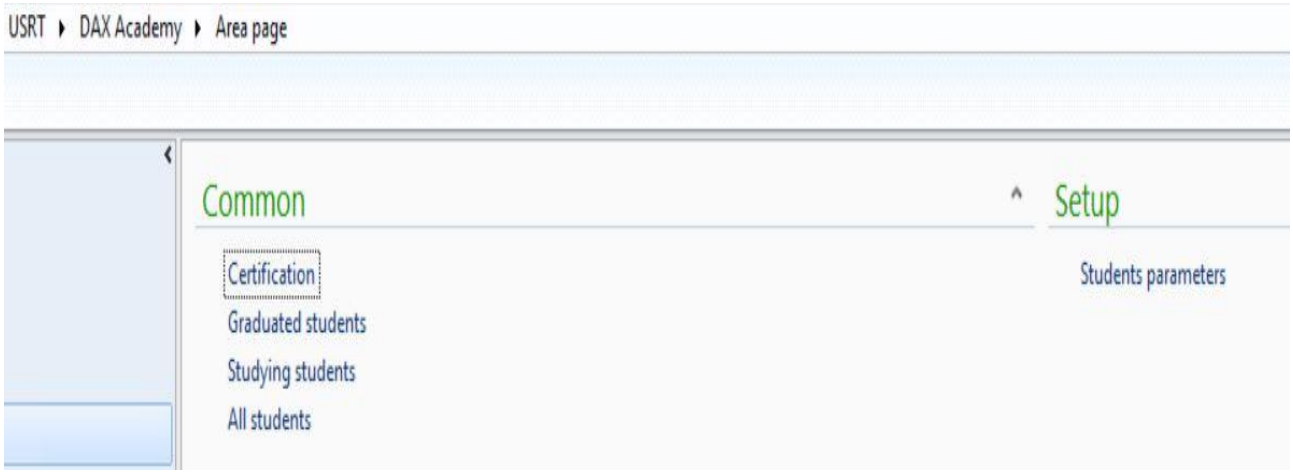


Рисунок 3.1 – Меню модуля «Академія»

В меню «Setup» розміщена форма Students parameters, яка містить налаштування номерних серій та параметрів які використовуються при створенні даних на інших формах модулю та впливають на бізнес – логіку(мінімальна кількість зданих екзаменів та рівень студента по замовчуванню).

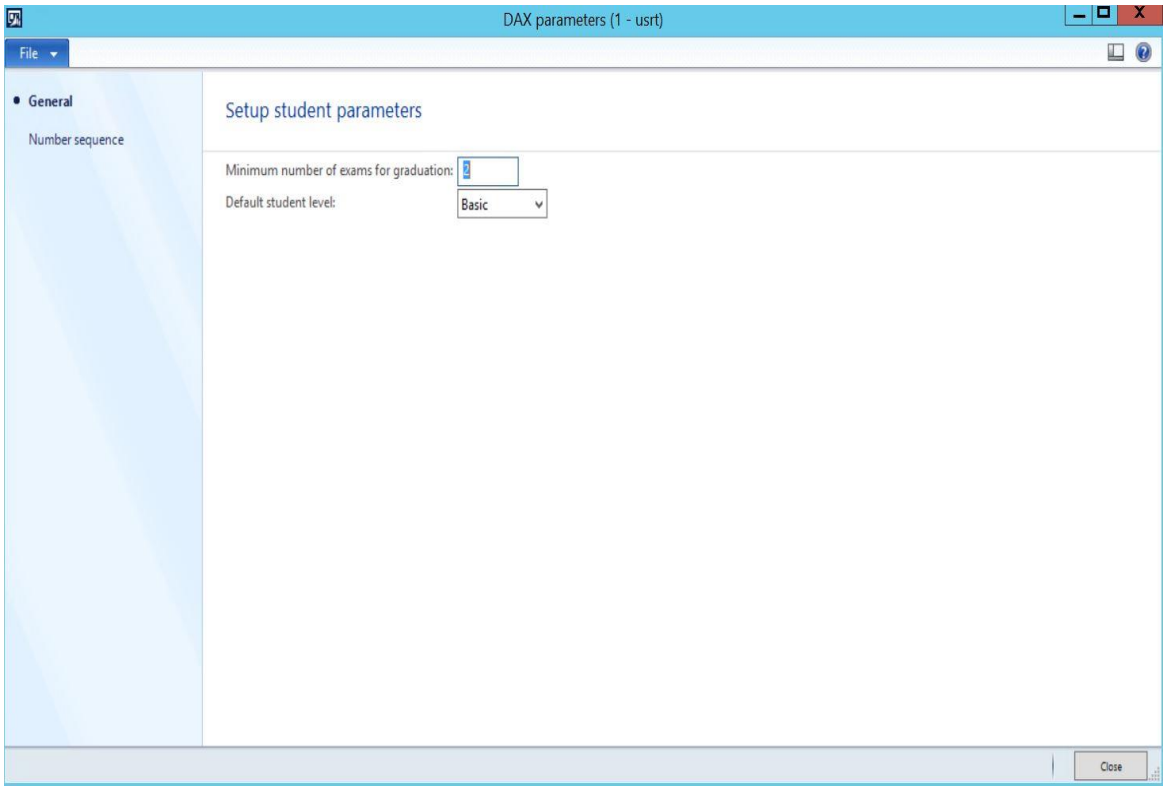


Рисунок 3.2 – Форма налаштування параметрів модулю

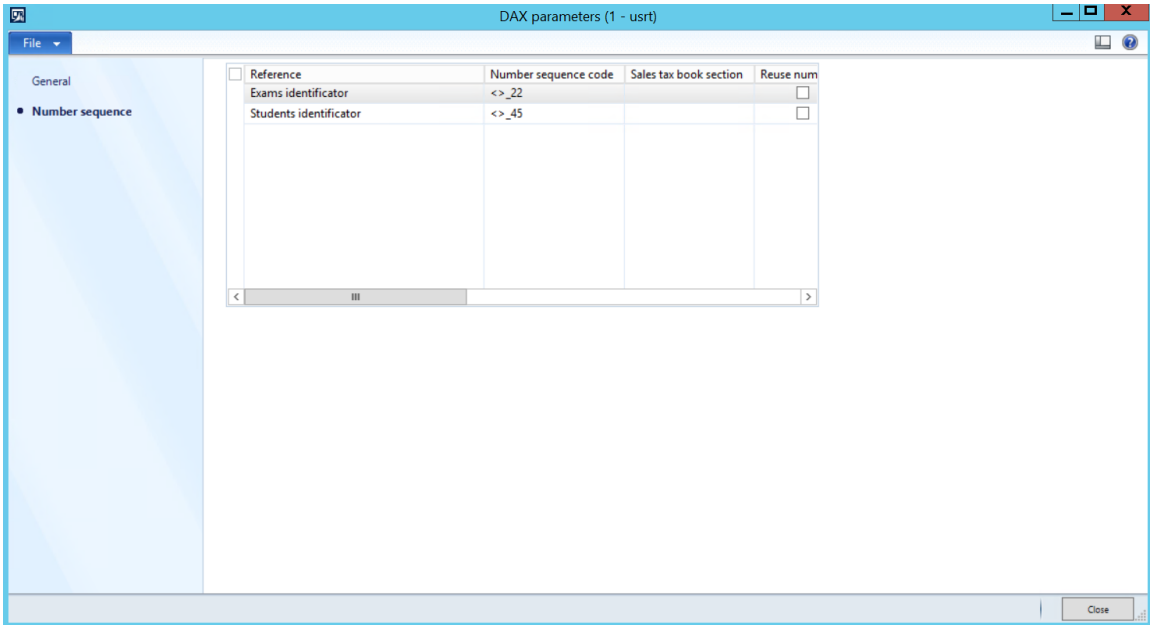


Рисунок 3.3 – Форма налаштування номерних серій модулю

Форма «Сертифікації» служить для відображення та створення дисциплін в навчальній академії, кожна дисципліна містить унікальний ідентифікатор, який генерується автоматично за допомогою номерних серій, ім’я, опис та поле «Статус дисципліни», яке вказує чи є дійсною дисципліна на даний час для академії. Ця інформація є надзвичайно важливою, так як успішність студента з не активних дисциплін не повинні впливати на показники його успішності. Для зміни статусу дисципліни використовується кнопка «Change activity drop dialog», котра викличе форму для активації чи деактивації дисциплін в академії.

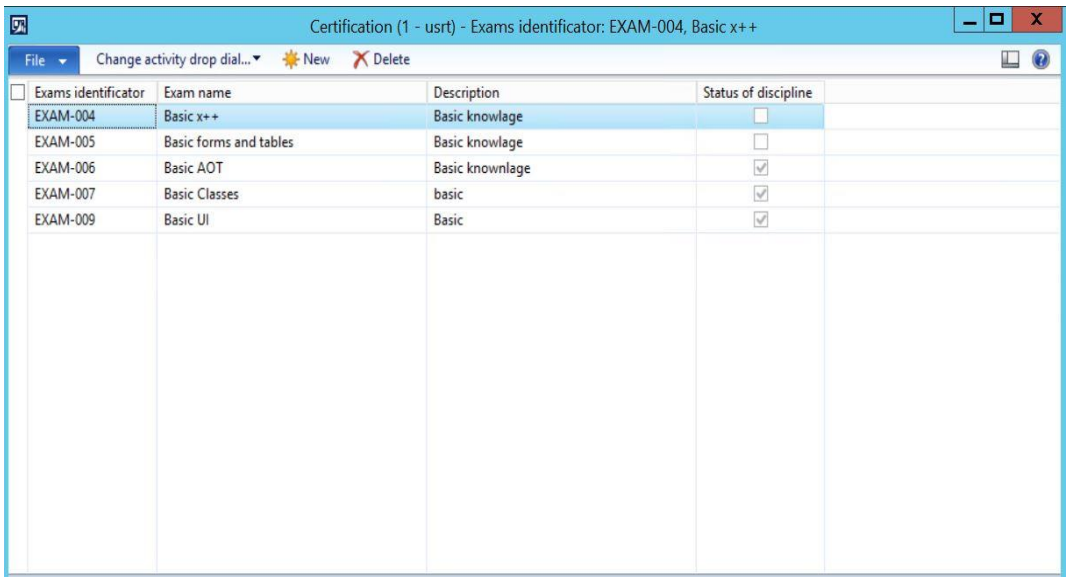


Рисунок 3.4 – Форма сертифікації

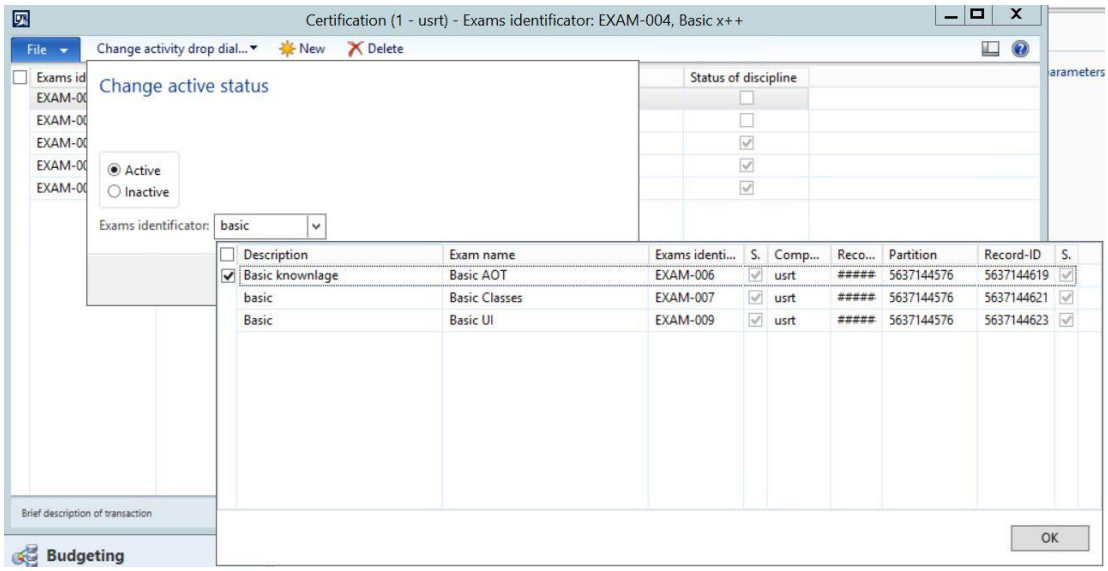


Рисунок 3.5 – Форма «Зміна статусу дисципліни»

Форма «Всі студенти», містить інформацію про всіх студентів, котрі навчаються чи навчались в академії. Так як дана форма, належить до типу форм «List Page», неможливо проводити редагування чи зміну даних безпосередньо на формі.

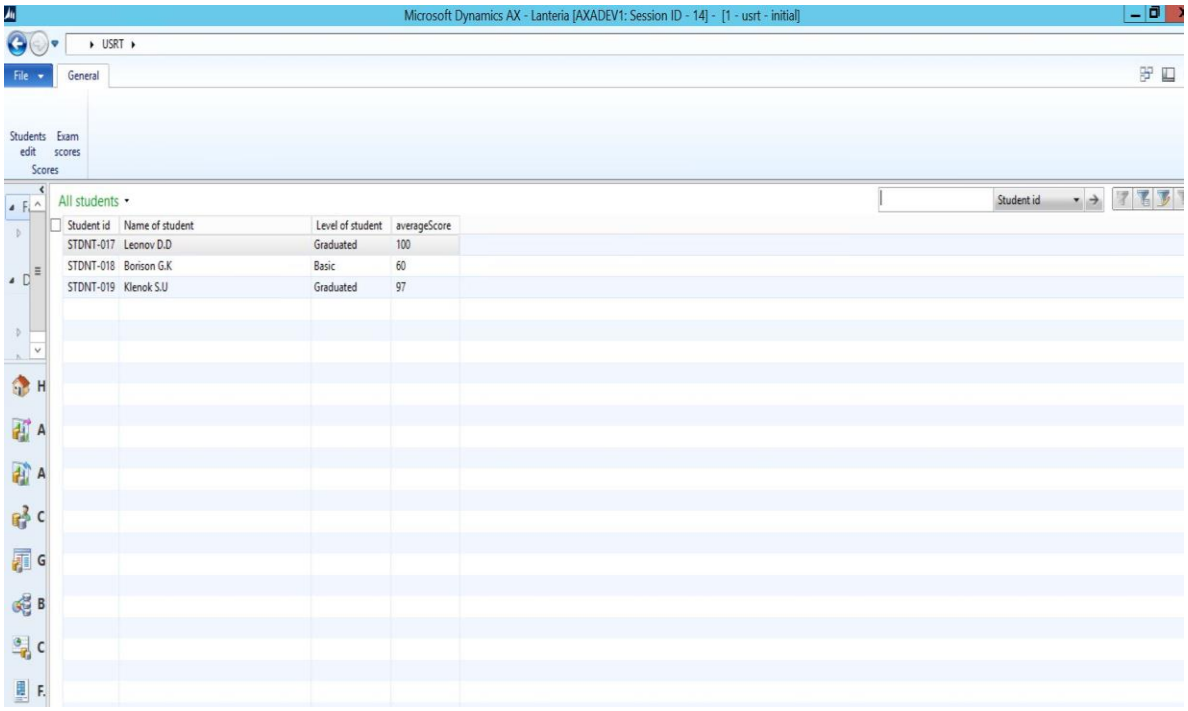


Рисунок 3.6 – Форма «Всі студенти»

Для редагування та вводу даних на цю форму використовується кнопка «Students edit», котра відкриває форму для редагування даних в сутності «Студенти».

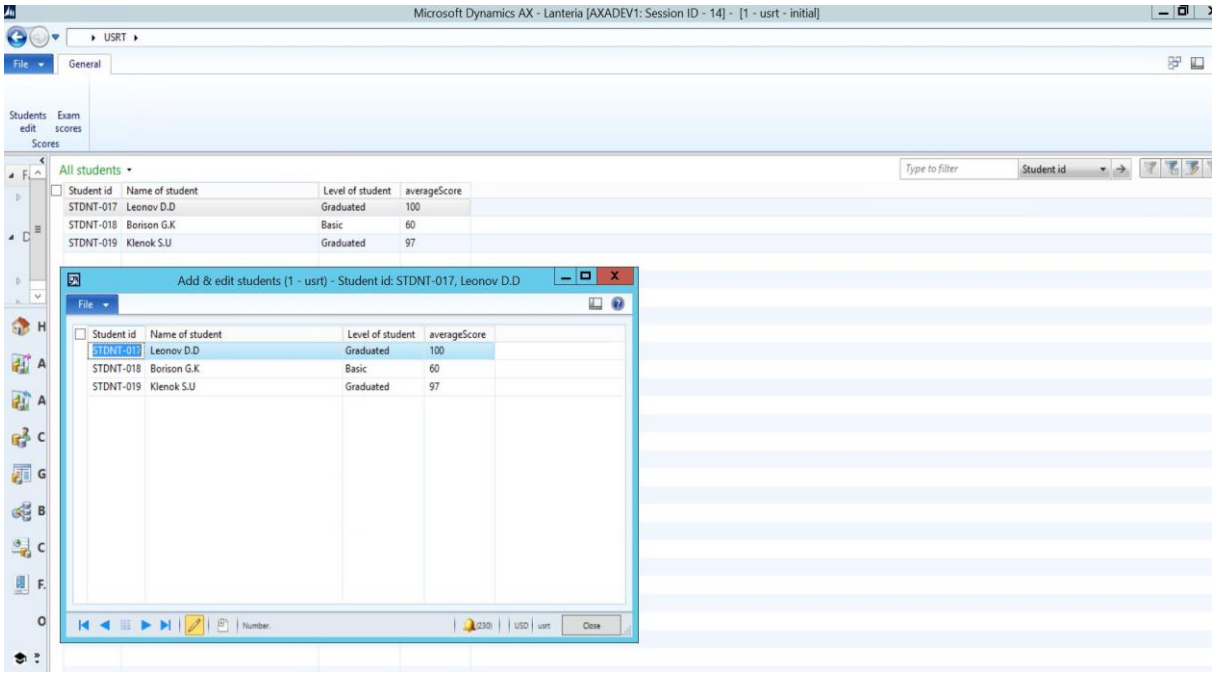


Рисунок 3.7 – Форма редагування сутності «Всі студенти»

Окрім цього, на формі «Всі студенти» є можливість перейти на форму «Оцінки з іспитів», яка дає можливість вносити дані про іспити для студента, проставляти бали (в діапазоні від 0 до 100), статус ж екзамену(зданий чи не зданий), система автоматично проставляє сама в залежності від балу за іспит(70 балів – прохідний бал по замовчуванню).

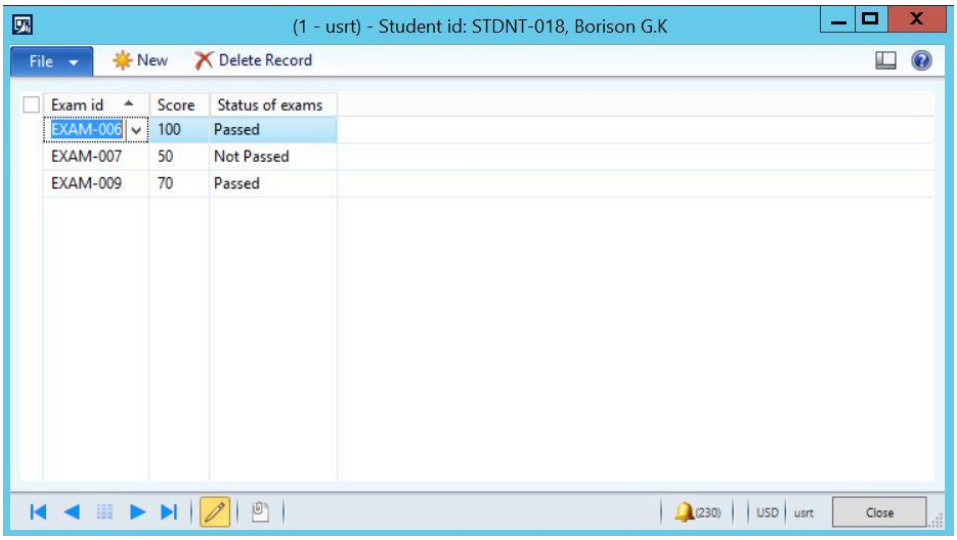


Рисунок 3.8 – Форма «Оцінки за іспити»

Окрім перегляду списку всіх студентів на формі, модуль дозволяє відкрити цю ж форму про з іншим фільтром по студентам. (Лише випускники, або чинні студенти академії). Це доступно зробити з меню модулю за допомогою елементів меню «Graduated students» або «Studying students».

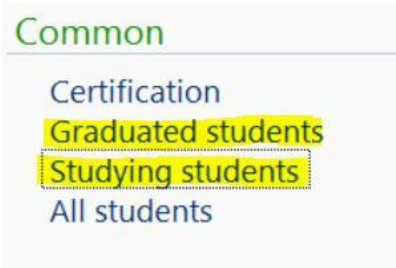


Рисунок 3.9 – Елементи меню, котрі відкривають відфільтровану форму студентів

Модуль автоматично переводить студентів в статус «Graduated» (випускник), якщо студент здав необхідну мінімальну кількість екзаменів з активних дисциплін (котра налаштовується в меню параметрів) на оцінку вище 70 балів(за замовчуванням).

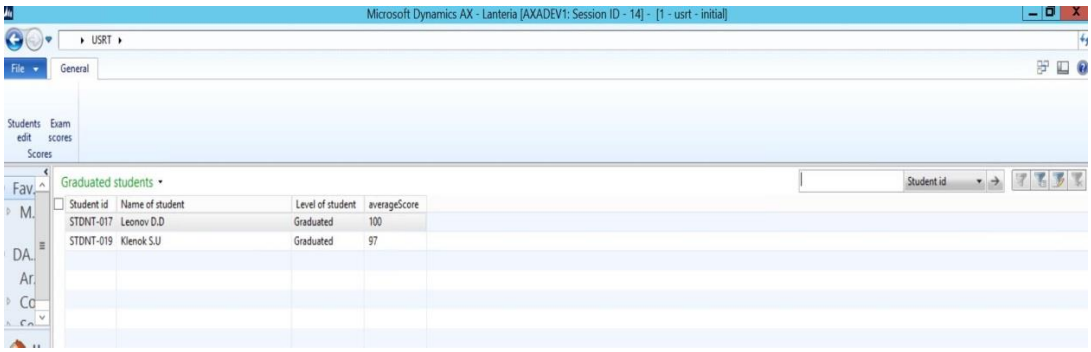


Рисунок 3.10 – Форма студентів - випускників

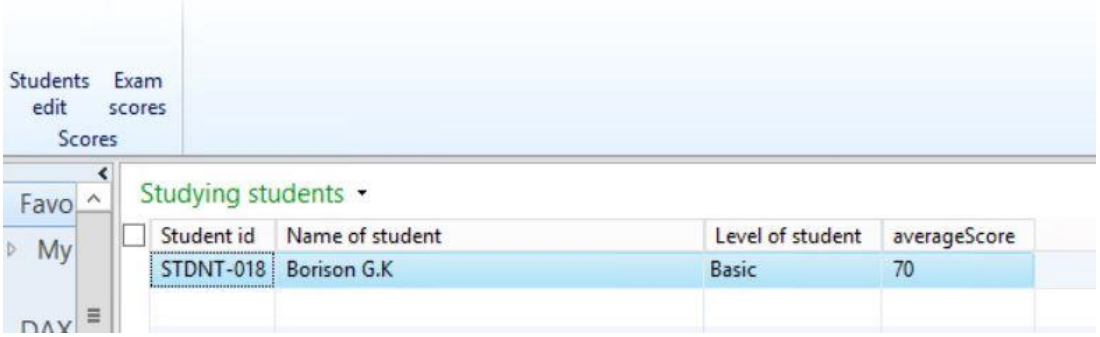


Рисунок 3.11 – Форма чинних студентів

3.2 Специфікація вимог до політики безпеки

Хоча й функціонально модуль «Академії» працює коректно, проте без проведення розмежування доступу до об’єктів – його не можна вважати повноцінно завершеним. Проте, перед проведенням розмежування доступу до об’єктів користувацького інтерфейсу необхідно визначити, які типи користувачів в системі повинні бути в зв’язку з специфікою призначення модуля. Даний модуль передбачає створення наступних користувачів:

- Студент академії;
- Викладач (ментор);
- Директор.

Повноваження даних користувачів можна розділити на 3 групи:

- Перегляд;
- Редагування записів;
- Видалення записів;

Користувач «Студент» повинен мати повноваження тільки на перегляд наступних сутностей модуля «Академія»:

- Студенти;
- Оцінки з іспитів;
- Сертифікації;

Видалення чи редагування даних в цих сутностях є забороненим для студентів академії. Для них вищезазначені сутності повинні нести виключно інформативний характер.

Користувач «Викладач» повинен мати наступні повноваження:

- Студенти (перегляд та редагування);
- Оцінки з іспитів (перегляд, редагування, видалення);
- Сертифікації (перегляд).

В модулі академії користувач «Викладач» виконує заповнення та редагування структур даних про успішність студентів з екзаменів. Проте в нього нема повноваженнь на видалення студентів та редагування форми параметрів та номерних серій.

Користувач «Директор» повинен володіти наступними повноваженнями:

- Студенти (перегляд, видалення, редагування);
- Сертифікації (перегляд, видалення, редагування);
- Оцінки з іспитів(перегляд, видалення, редагування);
- Параметри модуля(перегляд, видалення, редагування);

Даний користувач повинен бути наділений максимальними повноваженнями щодо маніпуляції з всіма структурами даних модуля, так як саме користувач «Директор» приймає рішення про активацію чи деактивацію дисципліни в академії та мінімальну кількість дисциплін, необхідну для отримання студентом статусу «Випускник».

Всі вище перелічені вимоги, щодо політики безпеки модулю повинні бути реалізовані за допомогою рольового розподілення, яке здійснюється за допомогою створення та налаштування артефактів безпеки в системі. Для кожного з користувачів повинна бути створена своя унікальна роль в системі, до якої в свою чергу будуть відноситись необхідні привілегії на об’єкти модуля «Академія».

Окрім цього, необхідно встановити, якій кількості фізичних користувачів необхідно надати роль «Директор», «Вчитель», «Студент» й створити цих користувачів в системі надавши їм відповідну роль. Кількість фізичних користувачів може залежити від специфіки академії та її структурної будови.

Проте, кількість директорів не повинна перевищувати кількість студентів та вчителів. Оптимальним рішенням буде розробка політики безпеки з 1-3 користувачами типу «Директор», 3-10 користувачами типу «Вчитель» та 5-20 користувачами типу «Студент», проте ці рамки не є конкретними й можуть змінюватись по мірі розвитку та розширення академії.

3.3 Реалізація політики безпеки модуля «Академія»

Впершу чергу необхідно створити 3 ролі в системі: «Студент», «Директор», «Вчитель». Це можливо здійснити прямо в проекті модуля, за допомогою дерева об’єктів в системі. За для полегшення налаштування артефактів безпеки необхідно створити директорію об’єктів Security.

Рисунок 3.13 – Ролі для модуля «Академія»

Налаштування нових ролей та модифікація існуючих в ERP – системі Dynamics можлива за допомогою функціонального модуля System Administration.

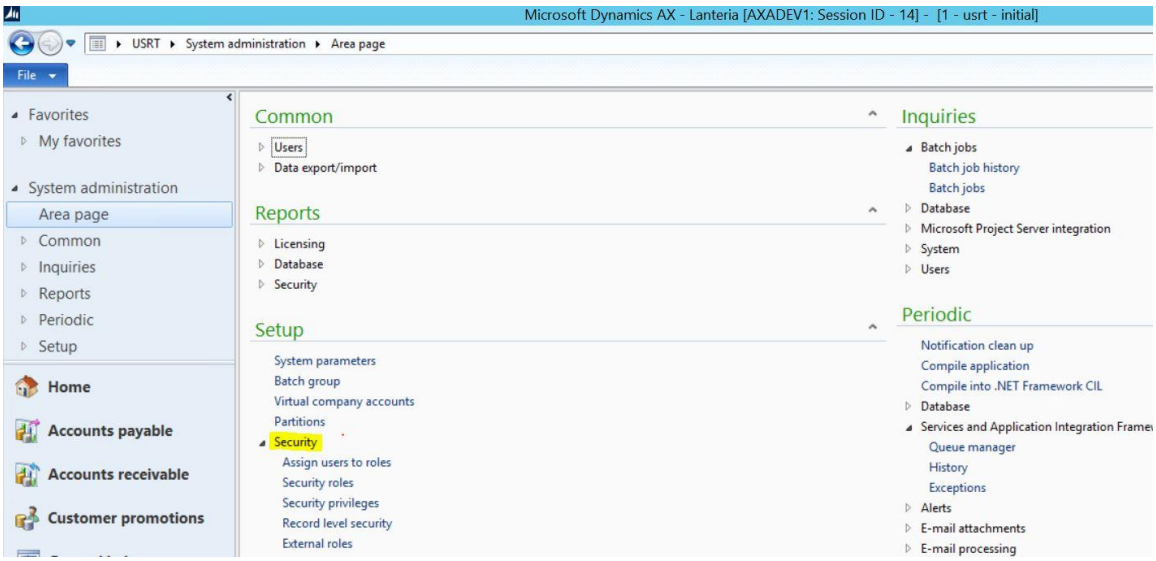


Рисунок 3.14 – Налаштування безпеки в системі

Завдяки цьому модулю, ми здійснюємо додавання необхідних нам користувачів до відповідної ролі (Вчитель, Директор, Студент). На прикладі ролі «Студент» розглянемо створення політики безпеки в системі:

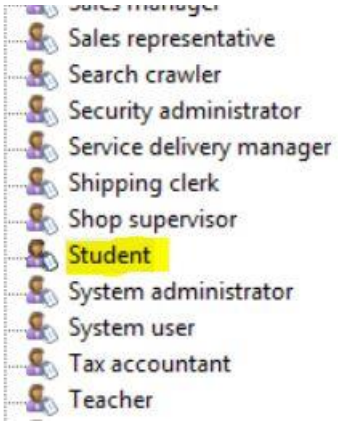


Рисунок 3.15 – Роль «Студент» в списку всіх ролей в системі

Після вибору ролі, переходимо в її налаштування та додаємо користувачів, яких хочемо додати до даної ролі. На формі додання користувачів, можна як додати користувачів до ролі, так і видалити користувачів, котрі були додані раніше.

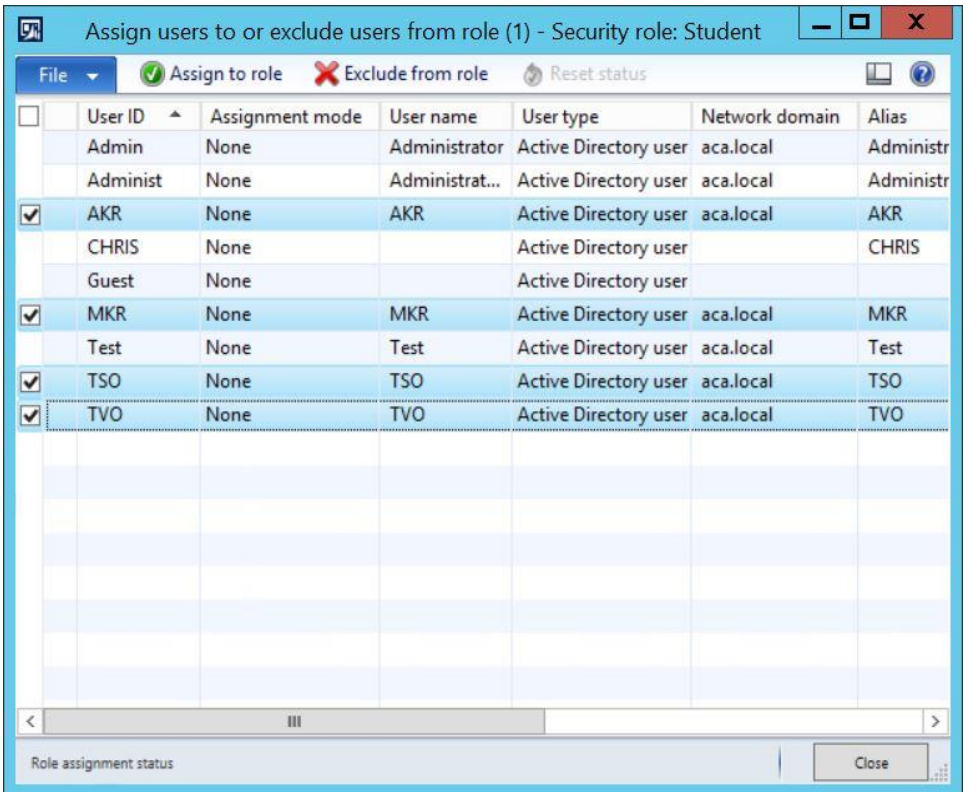


Рисунок 3.16 – Форма додавання користувачів до ролі

Після закінчення даного етапу створення політики безпеки, необхідно повернутись до дерева об’єктів проекту та створити необхідні згідно вимог до розмежування доступу – артефакти захисту.

Для кожної з ролей додаємо об’єкти, доступ до яких треба розмежувати, об’єкти додаються до артефакту «Permissions» (дозволи).

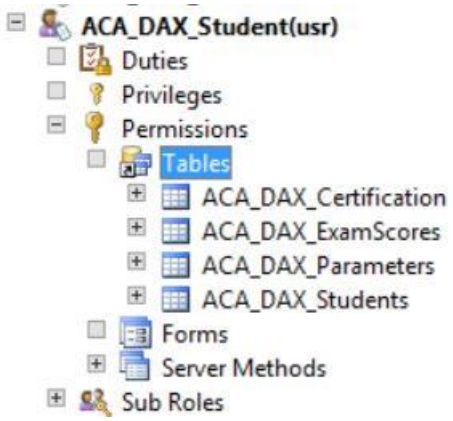


Рисунок 3.17 – Список дозволів для користувача «Студент»

Після створення всіх дозволів, необхідно визначити рівень доступу, котрий буде в даної ролі до цієї сутності. Рівень доступу необхідно вибирати відповідно до вимог політики безпеки.

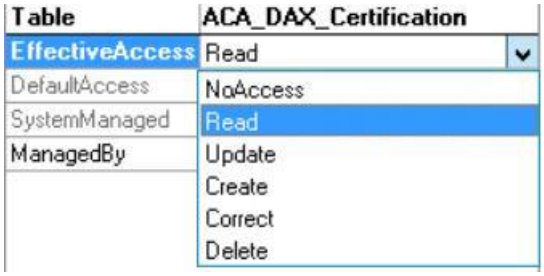


Рисунок 3.18 – Вибір рівня доступу до таблиці «Сертифікації» для користувача «Студент»

Рівень доступу «Read» дає змогу користувачеві, який знаходиться в даній ролі переглядати всі елементи користувацього інтерфейсу, де джерелом даних служить дана таблиця, проте на цьому його повноваження закінчуються. Даний рівень доступу ідеально підходить в ситуації коли нам треба дати користувачеві можливість бачити дані що циркулюють на формі, проте заборонити їх редагування та видалення.

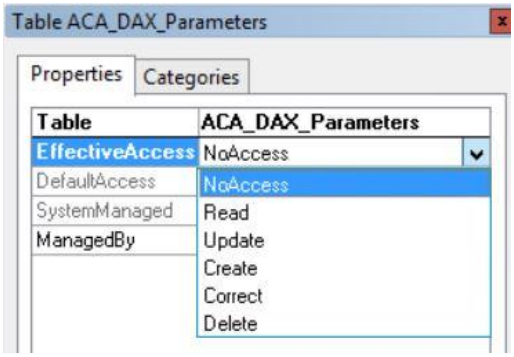


Рисунок 3.19 – Вибір рівня доступу до таблиці «Параметри» для користувача «Студент»

Рівень доступу «No Acsess» забороняє користувачеві, будь які дії з елементами користувацього інтерфейсу, які використовують дану таблицю в якості джерела даних. Даний рівень доступу ідеально підходить в ситуації коли нам заборонити користувачеві будь – який доступ до даних.

Для інших двох таблиць (Студенти та оцінки за іспити) був обраний рівень доступу «Read».

Для ролей «Вчитель та Директор» здійснюється аналогічне створення артефактів – дозволів. Якщо, необхідно дати право на редагування та створення нових записів вибирається рівень доступу «Create», якщо ж необхідний дозвіл на повну модифікацію структур (для директора), тоді вибирається рівень доступ до об’єкту «Delete».

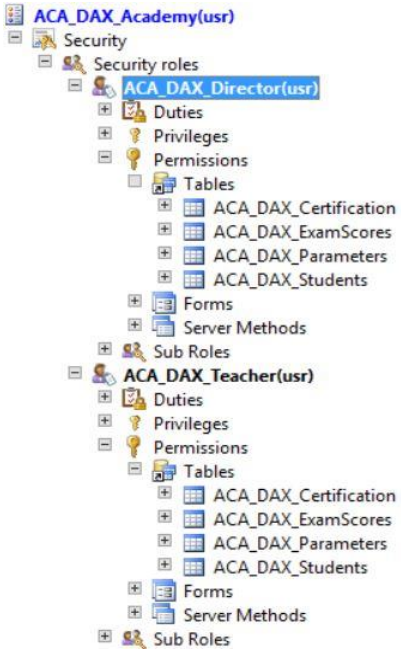


Рисунок 3.20 - Список дозволів для користувачів «Директор» та «Вчитель»

Після цього, слід впевнитись в тому користувач в системі був доданий до певної ролі, здійснити це можна завдяки модулю System Administration.

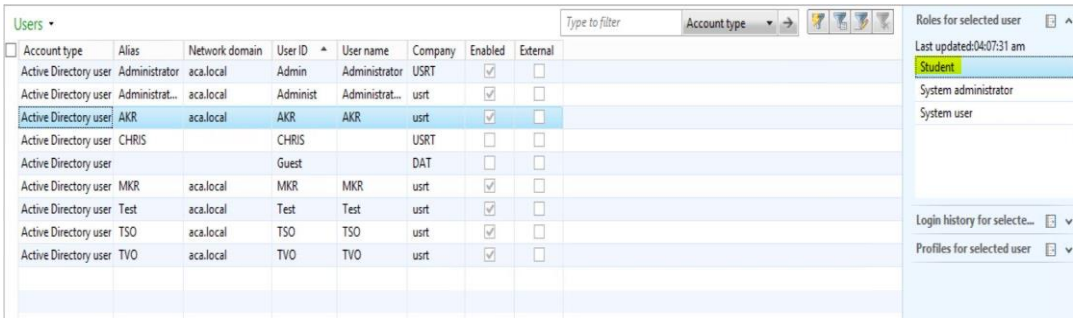


Рисунок 3.21 – Список користувачів в системі

На рисунку 3.21, ми можемо бачити, що до активного користувача(авторизацію під котрим було здійснено) дійсно була додана нова роль. Необхідно відзначити що один користувач, може належати до безлічі ролей. При розробці політики безпеки надзвичайно важливо проводити розмежування доступу до об’єктів таким чином, щоби уникнути конфліктних ситуацій серед ролей.

Після виконання, всіх перевірок необхідно впевнитись що артефакти – дозволів дійсно були присвоєні ролям. Для цього, використаємо налаштування ролей з модуля System Administration.

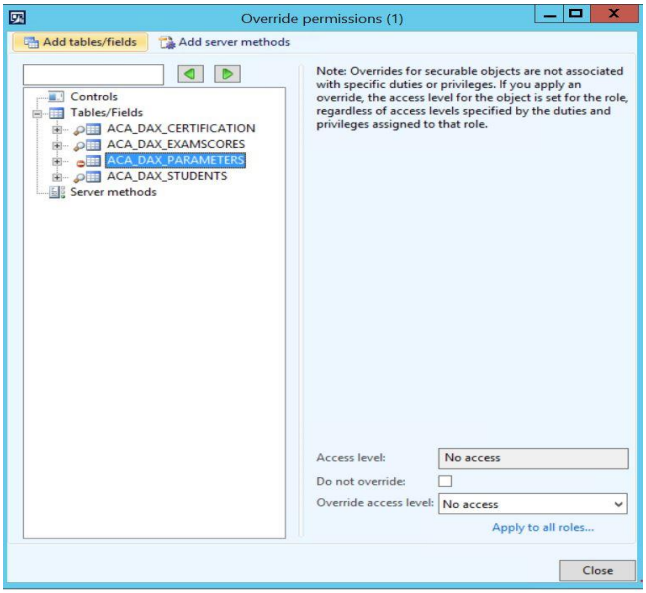


Рисунок 3.22 – Дозволи для ролі «Студент»

Тепер, необхідно перевірити коректне відпрацювання політики безпеки на прикладі користувача «Студента».

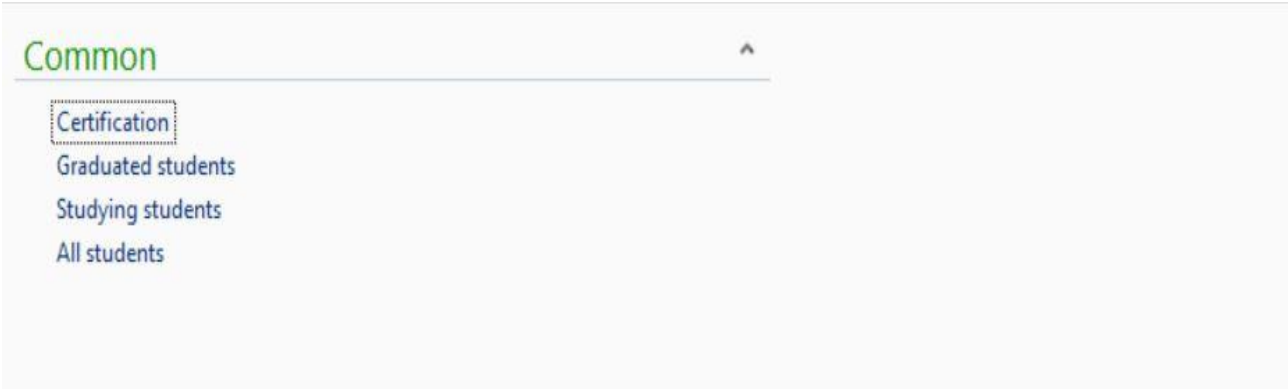


Рисунок 3.23 – Меню модуля «Академії» для користувача «Студент»

Так, як до структури «Параметри студента» був обмежений доступ для користувача «Студент», меню елемент даної структури тепер недоступний з модуля «Академії».

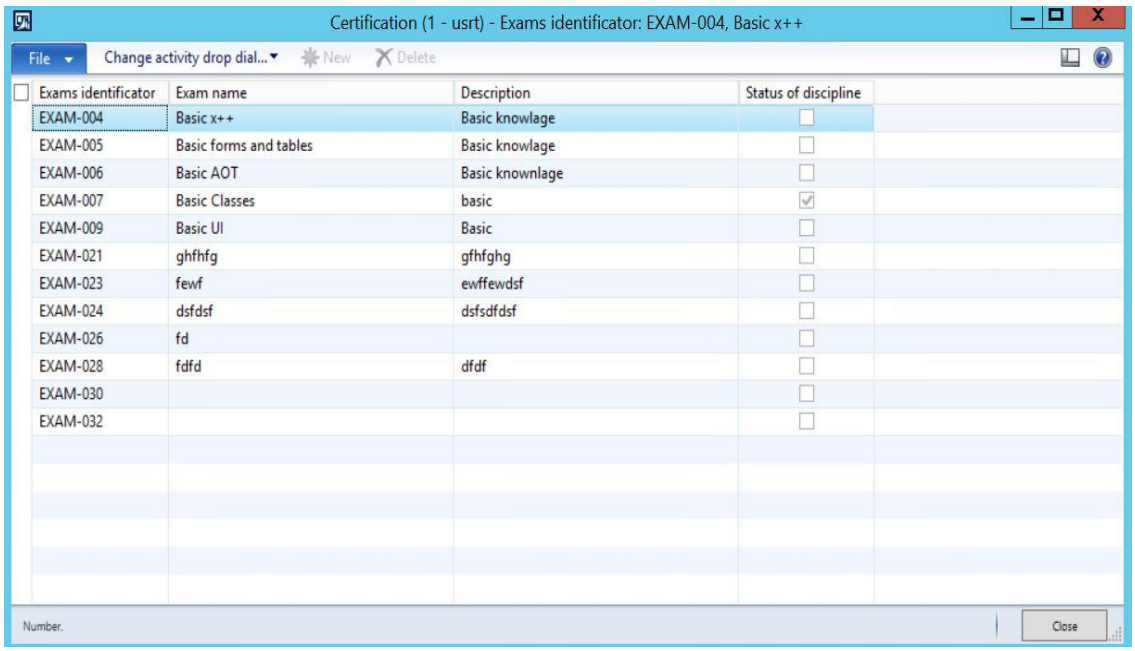


Рисунок 3.24 – Форма «Сертифікації» після проведення розмежування доступу

Тепер для користувача «Студент» є недоступним додавання, видалення та редагування записів, які містяться в таблиці «Сертифікації». Система реалізувала це завдяки закриттю доступу до елементів користувацького інтерфейсу, а саме кнопок «New» та «Delete». А сама форма закрита для

редагування, що робить неможливим завдання редагування вже існуючих даних.

Висновки до третього розділу

Можливості безпекової моделі ERP – системи Dynamics AX 2012 дозволяють створити гнучку політику безпеки для нового модуля системи або змінити існуючий модуль. При створенні політики безпеки для певного модуля системи необхідно враховувати функціональне призначення даного модуля, а також володіти інформацією про кількість користувачів котрі використовуватимуть цей модуль.

Артефакти безпеки в системі дозволяють провести розмежування доступу як виключно до елементів користувацького інтерфейсу, так й до системних та користувацьких таблиць та інших структур даних. При створенні даних артефактів необхідно чітко дотримуватись вимог політики безпеки модуля, інакше створення артефактів безпеки може привести до виникнення конфліктів серед користувачів системи.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Недотримання основних положень охорони праці, що визначені Законом України «Про охорону праці» може призвести до зниження продуктивності працівників компанії, а також до погіршення стану здоров'я серед штату підприємства, що в свою чергу веде до матеріальних збитків компанії, котра займається ERP – розробкою.

Згідно Закону України «Про охорону праці» кожен працівник має право на трудову діяльність в умовах, котрі є сприятливими для збереження здоров'я людини[9]. Саме цей закон регулює відносини між працівником та роботодавцем в питанні безпеки виробничого середовища. В даному розділі зазначені вимоги щодо облаштування робочого середовища, санітарії та мікроклімату приміщення для працівника, який займається ERP – розробкою.

Ергономіка робочого місця

Облаштування робочого місця повинне сприяти:

- правильному розміщенню робочого місця у виробничому приміщенні, де проводиться ERP - розробка ;
- належним умови освітлення в приміщенні та відсутності відблисків;
- створенню належних ергономічних характеристик елементів робочого місця;

Робоче місце працівника з ЕОМ , повинне бути обладнане робочим столом, стільцем та підставкою для ніг. Висота стола має бути в межах від 60 до 80 см, а ширина стола повинна створювати умови комфортні для здійснення операцій в зоні досяжності моторного поля.

Клавіатура повинна бути розташована на поверхні столу на відстані 2 см від краю. Конструкції клавіатури має передбачати в собі пристрій для регулювання куту нахилу клавіатури. Оптимальні параметри робочого місця працівника з ЕОМ зображені на рисунку 4.1:

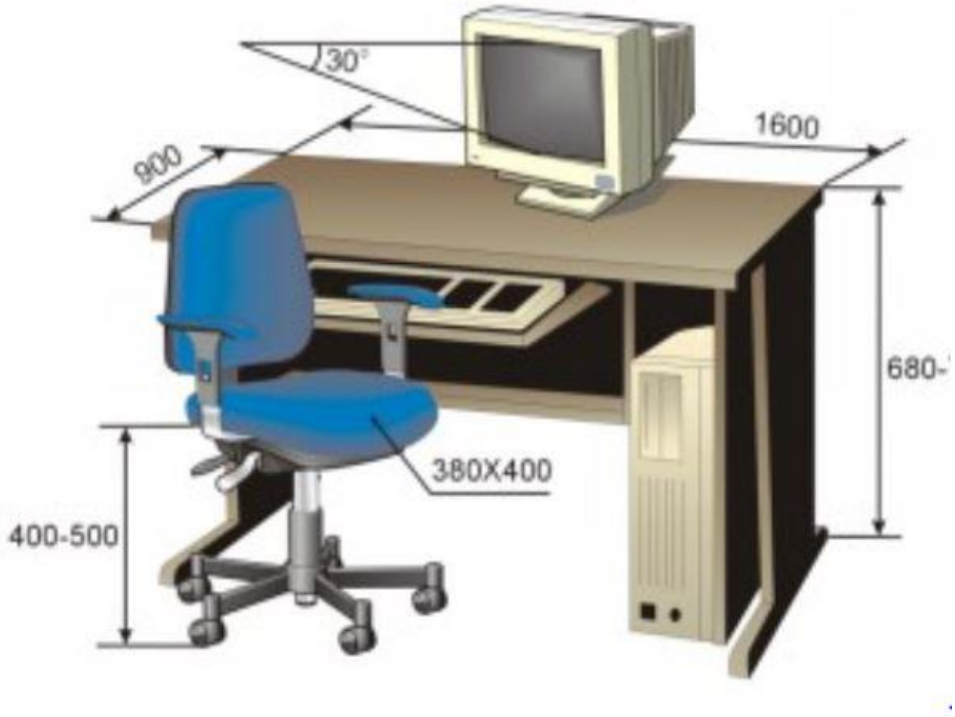


Рисунок 4.1 – Оптимальні параметри робочого місця працівника з ЕОМ

Шум та вібрація

Джерелом шуму в приміщенні є комп'ютер. Вентилятори (кулери) системного блоку, процесора, відеокарти і блоку живлення є сучасними і мають низький рівень шуму. Згідно з технічною документацією шум, зумовлений кулером в блоці живлення складає 25 дБ, кулером процесора - 30 дБ, загальний, - 34 дБ. Враховуючи незначний рівень шуму від персонального комп'ютера і незначний рівень фонового шуму від іншого устаткування, можна стверджувати, що сумарний рівень шумового забруднення приміщення не перевищує максимально допустимий рівень коригованої звукової потужності і складає не більше 50 дБ. При роботі з персональним комп'ютером в робочому приміщенні значення характеристик вібрації на робочих місцях не повинна

перевищувати допустимих значень.

Освітлення

Природне освітлення зумовлюють прямі сонячні промені й дифузне світло небосхилу. Природнє освітлення поділяється на: бокове (одно – або двостороннє), що здійснюється через світлові отвори (вікна) в зовнішніх стінах; верхнє – через ліхтарі та отвори в дахах і перекриттях; комбіноване – поєднання верхнього та бокового освітлення. Штучне освітлення може бути загальним та комбінованим. Загальним називають освітлення, при якому світильники розміщуються у верхній зоні приміщення (не нижче 2,5 м над підлогою) рівномірно (загальне рівномірне освітлення) або з урахуванням розташування робочих місць (загальне локалізоване освітлення).

За недостатнього природного освітлення у світлу пору доби використовують люмінесцентні лампи з використанням системи суміщеного освітлення. Для проведення ERP – розробки оптимальним рішенням буде освітлення, котре відповідає підрозряду зорових робіт *в*.

Мікрокліматичні умови

Мікроклімат виробничих приміщень - умови внутрішнього середовища цих приміщень, що впливають на тепловий обмін працюючих з оточенням шляхом конвекції, кондукції, теплового випромінювання та випаровування вологи. Ці умови визначаються поєднанням температури, відносної вологості та швидкості руху повітря, температури оточуючих людину поверхонь та інтенсивністю теплового (інфрачервоного) опромінення[10].

Для приміщення в якому проводяться роботи із ERP - системою на підприємстві, обираємо категорію важкості робіт за фізичним навантаженням – легка Іб. Повітря робочої зони активно забруднюється завдяки роботі ЕОМ, тому необхідно слідкувати за концентрацією канцерогенів та шкідливих речовин в повітрі, котрі не повинні бути вище гранично допустимих концентрацій (ГДК). Для встановлення необхідних за нормативами

параметрів мікроклімату і складу повітря робочої зони передбачено встановити систему кондиціонування та витяжну систему.

4.2 Безпека в надзвичайних ситуаціях

Надзвичайна ситуація - порушення нормальних умов життя та діяльності людей на окремій території чи об'єкті, спричинене аварією, катастрофою, стихійним лихом чи іншою небезпечною подією, зокрема епідемією, пожежею, що призвело (може призвести) до виникнення великої кількості постраждалих, загрози життю та здоров'ю людей, їх загибелі, значних матеріальних втрат, а також до неможливості проживання населення на території чи об'єкті, ведення там господарської діяльності. Надзвичайні ситуації різняться за характером джерела на техногенні, природні та інші. Саме техногенні ситуації є найбільш поширеними на підприємствах, де відбувається розробка та впровадження програмних продуктів[11].

Працівники підприємств зобов'язані знати і виконувати правила техніки безпеки на підприємстві, у випадку надзвичайної ситуації працівники повинні оперативно проінформувати керівництво підприємства і негайно вжити заходів щодо ліквідації наслідків події. Працівники повинні усвідомлювати, що особисто несуть відповідальність за своєчасне вжиття заходів щодо запобігання надзвичайних ситуацій.

Про кожний нещасний випадок або надзвичайну ситуацію на виробництві потерпілий очевидець або учасник події після надання першої допомоги негайно, використовуючи всі доступні засоби зв'язку, повідомляє керівника.

Недотримання цієї вимоги може призвести до погіршення стану здоров'я потерпілого через відсутність кваліфікованої медичної допомоги, а також може бути причиною несвоєчасного прийняття оперативних заходів з контролю за ситуацією, тобто з мінімізації її наслідків.

Кожне підприємство повинне мати інструкцію щодо поведінки в надзвичайних ситуаціях й котра повинна бути розроблена згідно з Законом України «Про захист населення і території від надзвичайних ситуацій техногенного та природного характеру». Працівники підприємства забов’язані знати та дотримуватись даної інструкції, а сама інструкція повинна бути затверджена керівником підприємства. В інструкції повинна міститись

інформація про потенційно можливі надзвичайні ситуації на виробництві, методи оповіщення керівництва про надзвичайну ситуацію, заходи щодо збереження матеріальних цінностей підприємства та маршути евакуації персоналу підприємства.

Одною з найпоширеніших надзвичайних ситуацій на малих та середніх підприємствах, що займаються розробкою та впровадженням ERP – систем є пожежа. Основні причини пожежі: несправності в електроустановках та мережах, порушення вимог технологічних регламентів проведення вогневих робіт, недотримання заходів пожежної безпеки (паління, розведення відкритого вогню, застосування несправного обладнання і т. п.), необережне поводження з вогнем. Основні небезпечні фактори пожежі: теплове випромінювання, висока температура, отруйний вплив продуктів горіння (окис вуглецю та ін.), зниження видимості при задимленні.

Вибух - це горіння, що супроводжується звільненням великої кількості енергії в обмеженому об’ємі за короткий проміжок часу. Вибух призводить до 44 утворення та розповсюдженню ударної хвилі з надлишковим тиском (більше 5 кПа), що має механічний вплив на навколишні предмети.

Тому, крім інструкції щодо поведінки в надзвичайних ситуаціях, підприємство повинне мати план евакуації у випадку пожежі або вибуху.

Реагувати на надзвичайні ситуації означає організувати й координувати роботи й заходи, аби:

- припинити вплив небезпечних чинників, що спричинила надзвичайна ситуація;
- урятувати персонал, населення, обладнання та майно;
- локалізувати зону надзвичайної ситуації;
- ліквідувати або мінімізувати наслідки надзвичайної ситуації, які загрожують життю або здоров’ю персоналу, населення, шкодять території, довкіллю або майну.

ВИСНОВКИ

В наш час, бізнес росте максимально стрімко, й тому питання його автоматизація, покращення та спрощення стоїть максимально гостро. В ході виконання кваліфікаційної роботи мною було встановлено, що використання ERP – систем може справді покращити матеріальний стан підприємства.

Безпекова модель в ERP – системі Dynamics AX являє собою багаторівневу структуру, котра призначена для тонкого налаштування доступу до всіх елементів системи. Знання тонкощів роботи безпекової архітектури може оптимізувати загальні роботу ERP – системи, а також унеможливити ризики втрати інформації, її спотворення чи знищення.

В ході виконання роботи була розроблена політика безпеки для існуючого модуля системи, було здійснено розмежування доступу до об'єктів модулю «Академія». Розмежування доступу було здійснено завдяки артефактам безпеки та параметрам безпекової моделі.

Окрім цього були описані основні компоненти безпекової моделі, такі як: ролі, користувачі, повноваження, привілегії та була представлена їх ієрархія в системі. Був проведений огляд основних модулів системи, наданий їх опис призначення, структурну будову та інші особливості функціонування. Також, були що описані основні аспекти функціонування даної системи та проаналізовані основні вимоги до її роботи на підприємстві. При виявленні конфліктів в роботі системи необхідно звернутись до адміністратора системи або її розробника. Впроваджуючи політику безпеки в модуль системи або ж модифікуючи існуючу політику безпеки необхідно брати до уваги специфіку діяльності підприємства, провести аналіз штату підприємства та встановити особливості виробничного процесу за для мінімізації виникнення конфліктних ситуацій при доступі до певних об'єктів системи. Правильне використання та налаштування ERP – систем здатне максимально покращити продуктивність роботи підприємства та його штату, а налаштування політики безпеки здатні зробити дані на підприємстві максимально захищеними.

СПИСОК ЛІТЕРАТУРИ

1. Кареліна О. В. Використання технології RFID в ERP - системах [Електронний ресурс] / О.В Кареліна // ТНТУ. – 2019. – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/10550/2/ConfTNTU_2011_Karelina_O-Avtomatyzatsiia_dokumentoobihu_73.pdf.

2. Козак Р. О. До питання метрики якості програмного забезпечення [Електронний ресурс] / Р. О. Козак. // ТНТУ – 2010. – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/10808/2/Conf_2010v1_Kozak_R-Do_pytannia_metryky_yakosti_prohramnoho_19.pdf.

3. Кареліна О. В. Автоматизація документообігу підприємства засобами 1с:8 [Електронний ресурс] / О. В. Кареліна // ТНТУ. – 2011. – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/10550/2/ConfTNTU_2011_Karelina_O-Avtomatyzatsiia_dokumentoobihu_73.pdf.

4. Козак Р. О. Системи управління безпекою [Електронний ресурс] / Р. О. Козак // ТНТУ. – 2013. – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/123456789/8902/2/Conf_2013_Kozak_R-Systemy_upravlinnia_bezpekoiu_49.pdf.

5. Кареліна О. В. Виклики і загрози кібербезпеки [Електронний ресурс] / О. В. Кареліна // ТНТУ. – 2018. – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/lib/27177/2/IMST_2018_Karelina_O-Vyklyky_i_zahrozy_kiberbezpetsi_104.pdf.

6. Carepton R. Inside Microsoft Dynamics AX 2012 R3 / Rosemary Carepton., 2014.

7. Mounla R. Microsoft Dynamics 365 Extensions Cookbook / Rami Mounla., 2012.

8. Lushak A. Using Microsoft Dynamics AX: The New Dynamics ‘AX 7‘ / Andreas Lushak., 2016.

9. НАКАЗ Про затвердження Загальних вимог стосовно забезпечення роботодавцями охорони праці працівників [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0226-12#Text.

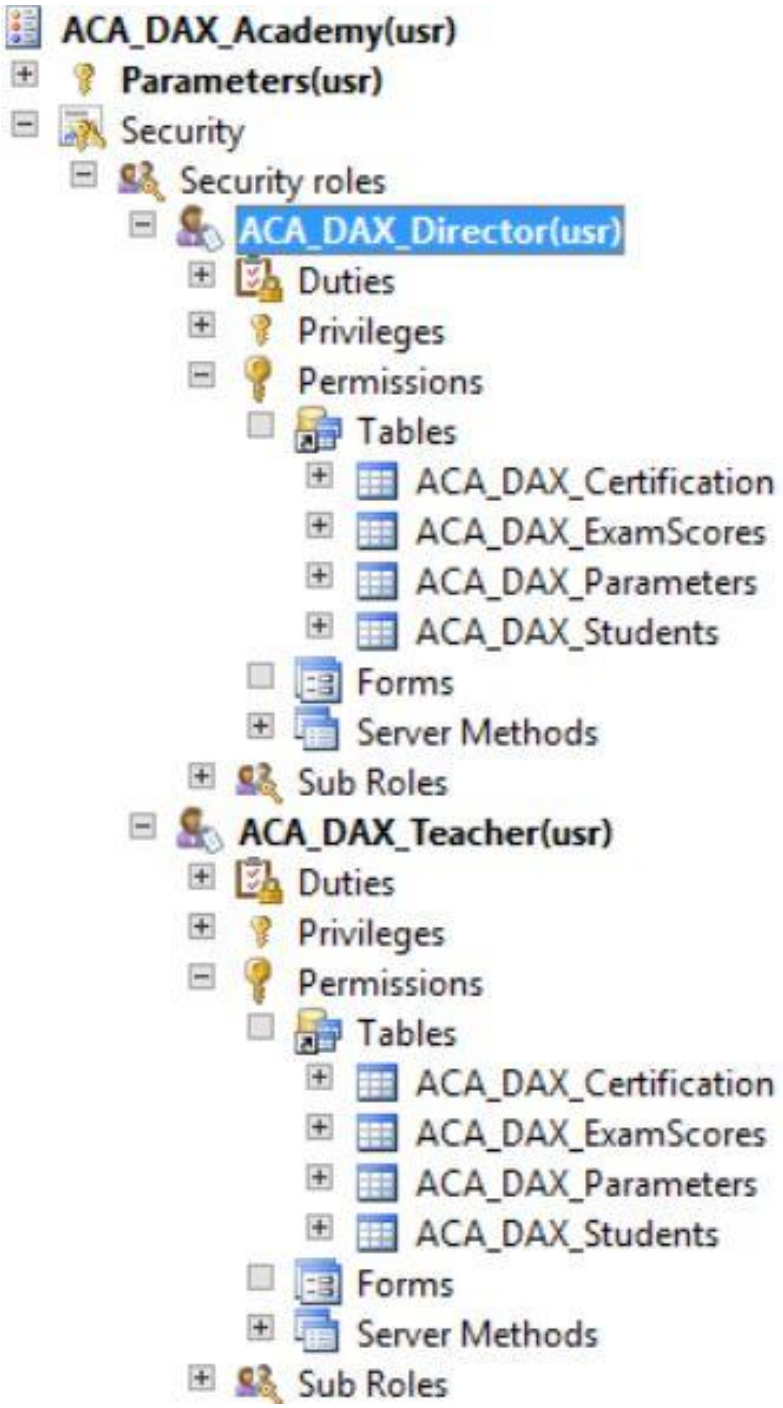
10. Охорона праці та безпека в надзвичайних ситуаціях [Електронний ресурс] – Режим доступу до ресурсу: http://inmad.vntu.edu.ua/portal/static/60D6D00C-3419-4907-9009-0343E953423B.pdf.

11. Надзвичайні ситуації та події на підприємстві [Електронний ресурс] – Режим доступу до ресурсу: https://uteka.ua/ua/publication/commerce-12-dokumentooborot-2-chrezvychajnye-situacii-i-opasnye-sobytiya-na-predpriyatii-pravovye-aspekty.

ДОДАТКИ

Додаток А

Список дозволів користувачів «Директор» та «Вчитель»



Додаток Б

УДК 004.056.3
Карпешко А. – ст. гр. СБм-61
Тернопільський національний технічний університет імені Івана Пулюя

БЕЗПЕКОВА МОДЕЛЬ В ERP - СИСТЕМІ DYNAMICS AX

Karpeshko A.

SECURITY MODEL IN ERP SYSTEM DYNAMICS AX

В наш час робота великого підприємства неможлива без використання ERP – систем, котрі допомагають автоматизувати завдання обліку та контролю різноманітних ресурсів та процесів на підприємстві. Починаючи від автоматичного створення документації на покупку чи продаж, завершуючи обліком відпусток у персоналу використання ефективних й сучасних ERP – систем значно спрощує виконання всіх вищеперелічених завдань та мінімізує затрати часу на документування всіх процесів підприємства.

ERP - система (з англ. Enterprise Resource Planning System) - система планування ресурсів підприємства або корпоративна інформаційна система яка, призначена для автоматизації обліку і управління. Як правило, ERP-системи будуються за модульним принципом і в тому або іншому ступені охоплюють усі ключові процеси діяльності компанії. Також можна сказати що, ERP-система є методологією ефективного планування і управління усіма ресурсами підприємства, які потрібні для здійснення продажів, виробництва, закупівлі і обліку при виконанні замовлень клієнтів в сферах виробництва і надання послуг. З усіх наявних ERP – систем, саме Dynamics AX є всесвітнім лідером ринку ERP – систем й оскільки містить найбільш широкий спектр інструментів для автоматизації великих виробництв, дозволяє розширювати її стандартний функціонал створюючи окремі системні модулі або змінюючи вбудований функціонал.[2]

При дослідженні задачі створення додаткового та розширеного функціоналу виникає питання про розмежування доступу до різноманітних модулів та об’єктів, так як проблема є породженою тим, що існує велика кількість користувачів з різноманітними правами доступу до важливої інформації та доступними функціональностями. Ігнорування налаштувань моделі безпеки може призвести до надзвичайно великих збитків для компанії, як метеріальних так й репутаційних. Одна з найбільш поширених помилок при розробці нових модулів системи – надання невірних привілегій до об’єктів системи.[1] Це може спричинити як витік конфіденційних даних за межі підприємства, так й витік даних в середині підприємства.

Для гарантування захисту даних у системі, Microsoft Dynamics пропонує модель безпеки, засновану на суворому розподілі ролей. Це означає, що це не окремі користувачі, які мають певний рівень доступу до даних, а швидше ролі безпеки. Це економить час адміністраторам, яким згодом не потрібно керувати доступом для кожного окремого користувача. Користувачі отримують доступ лише до рівня інформації, необхідної для своєї робочої діяльності. Це досягається за допомогою категоризації ролей користувача, розробленої відповідно до структури вашого бізнесу.

Усі користувачі повинні бути призначені щонайменше для однієї ролі захисту (у разі необхідності їх може бути більше однієї), і, якщо є потреба, команди можуть бути призначені власниками певних записів чи організацій, тим самим забезпечуючи всім членам команди однаковий рівень доступу. Рольова модель безпеки є ієрархічною. З одного боку, існує ієрархія ролей, що означає, що деякі з них (звані "дочірніми ролями") можуть бути безпосередньо пов'язані з іншими (називаються "батьківські ролі"). Завдяки Dynamics 365

Finance and Operations, ролі безпеки, необхідні для виконання будь-якого завдання, можна було визначити лише за допомогою набору інструментів розвитку безпеки, який вимагав встановлення системними адміністраторами. Тепер вони можуть використовувати вбудований інструмент діагностики безпеки, який визначає всі ролі, обов'язки та привілеї, необхідні для виконання певного завдання.[3]

Кожна роль має набір покладених на неї обов'язків. Обов'язки відображають бізнес-процеси, характерні для кожної компанії, які призначаються адміністратором. Один обов'язок може відповідати більш ніж одній ролі. Коли пов’язані обов'язки покладаються на окремі ролі, вони "відокремлюються". Розподіл обов'язків допомагає компанії слідувати нормативним вимогам, таким як міжнародні стандарти фінансової звітності, серед інших, специфічні для кожної компанії, галузі та місця розташування. Модель безпеки дає можливість гнучкого розмежування доступу до даних серед персоналу підприємства. Знання тонкощів роботи моделі безпеки здатне покращити загальну роботу ERP – системи, а також унеможливити ризики втрати інформації, її спотворення чи знищення, що в свою чергу сприяє підвищенню ефективності підприємства.

Література

1. Acuna E. Workflow Essentials: Dynamics 365 for Finance and Operations [Електронний ресурс] / Esteban Acuna – Режим доступу до ресурсу: https://global.hitachi-solutions.com/blog/workflow-essentials-dynamics-365-finance-and-operations.

2. An overview of the different modules of Microsoft Dynamics 365 [Електронний ресурс] – Режим доступу до ресурсу: https://gestisoft.com/en-ca/an-overview-of-the-different-modules-of-microsoft-dynamics-365/

3. Security role in D365 Finance and operation [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudfronts.com/create-security-role-in-d365-finance-and-operation.