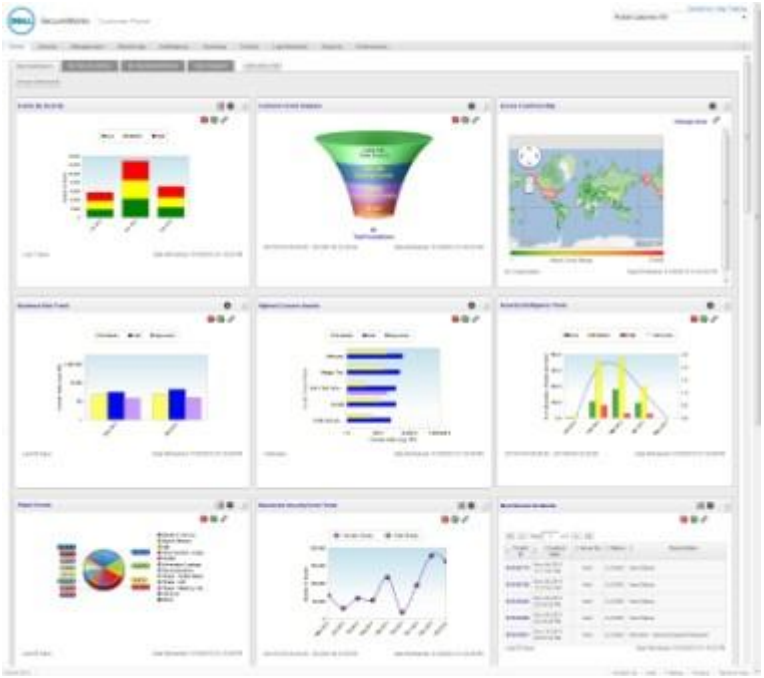
BI та інформаційна безпека – для керівника, спеціаліста та зовнішнього користувача



Dell SecureWorks BI dashboards for IT Security

Для покращання ділової-аналітики (Business Analytic) за допомогою систем підтримки прийняття рішень (Decision Support System) на передових підприємствах активно використовують засоби Business Intelligence (BI). При цьому, BI-засоби використовують також для підтримки інформаційної безпеки у різних застосуваннях, у тому числі для розмежування доступу різних категорій користувачів до первинних даних та до визначених форм агрегатованої інформації, ін.

Це підтверджують запити в Інтернеті, для прикладу dashboard designe BI for IT Security – цей запит повертає значну кількість спеціальних графіків (dashboards), які є кінцевою візуалізацією засобів Business Intelligence. На рисунку показаний приклад Dell SecureWorks BI dashboards.

У світі є значна кількість постачальників BI-платформ. Провідні постачальники BI-платформ визначаються консалтинговими компаніями IDC, Forrester, Gartner у платних звітах і відображаються в узагальненій формі за допомогою спеціальних діаграм, для прикладу: Forrester Wave™: Enterprise Business Intelligence Platforms та Gartner Magic Quadrant for Bl & Analytics Platforms.

Компанії IDC, Forrester, Gartner оновлюють свої звіти, як правило, щороку. На зображеннях у статті показані доступні в Інтернеті діаграми Forrester та Gartner – за 2015 рік.

Далі розглянуті деякі питання інформаційної безпеки в контексті збору, зберігання, аналізу та публікації даних.

Gartner Magic Quadrant for Bl & Analytics Platforms 2015

BI може застосовуватися для надання розмежов

ан
ог
о
до
ст
уп
у
до
ін
фо
рм
ац
ії
ко
ри
ст
ув
ач
ам
рі
зн
их
ка
те
го
рі
й,
дл
я
пр
ик
ла
ду
—
ке
рі
вн

ик
ам
,
сп
ец
іа
лі
ст
ам
,
зо
вн
іш
ні
м
ко
ри
ст
ув
ач
ам
.
Т
ак
ий
ва
рі
ан
т
ре
ал
із
ац
ії
we
b-
си

стеми розглянутий у російській публікації Business Intelligence и информацио

нн
ая
бе
зо
па
сн
ос
ть
(
ав
то
р
–
Не
кр
ас
ов
)
і
да
лі
ви
кл
ад
ає
ть
ся
то
чк
а
зо
ру
ав
то
ра
на
фу

нкціїціїєїсистеми.

РОБОЧЕ МІСЦЕ КЕРІВНИКА

Керівник повинен отримувати інформацію у стислому, агрегованому вигляді, в гранично ілюстративній формі – так, щоб з мінімальними часовими витратами помітити важливі обставини, що вимагають реагування і не витрачати час на несуттєву інформацію.

Сучасний спосіб подачі моніторингової інформації керівнику – це інтерактивна панель управління. Вона інтегрує на одному екрані дані на теми, що входять до сфери відповідальності керівника – у вигляді графіків, карт, яскраво ілюстрованих таблиць, спеціальних індикаторів у стилі панелі з індикаторами в автомобілі, ін. Дані гранично узагальнені, але є можливість заглибитися в деталі, скажімо, якщо цифри горять червоним.

Часткові діаграми (dashboards) у панелі управління керівника налаштовуються у візуальному інтерфейсі і дозволяють без програмування створювати набір інтегрованих екранів, що складаються з елементів загальної корпоративної бібліотеки звітів.

Особливість сучасного керівника – мобільність. Тому він повинен мати доступ до даних через Інтернет і використовувати для роботи будь-який з мобільних пристроїв – телефон, планшетний комп’ютер, ноутбук, а також мати можливість працювати і в офлайн, наприклад у літаках. Для управління доступом використовується спеціальний web-сервіс, який дає

можливість користувачеві отримувати проект, пакет звітів і працювати з ним онлайн. При необхідності користувач може отримати локальну копію у вигляді набору «мікрокубів» – сильно стиснутих звітів для автономної роботи.

У BI-системі розмежовуються права доступу, шифрується трафік. Додатково може застосовуватися захищене з'єднання, яке реалізується спеціальним програмно-апаратним комплексом, що включає апаратний модуль довіреного завантаження і програмним забезпеченням, що реалізує захищене VPN-з'єднання, шифрування даних при передачі, а також електронний підпис, що гарантує, що дані не були підмінені в процесі передачі.

ІНСТРУМЕНТИ ФАХІВЦІВ

Можна розрізнити кілька категорій фахівців, що працюють з BI:

- адміністратор;
- автор;
- експерт;
- звичайний користувач.

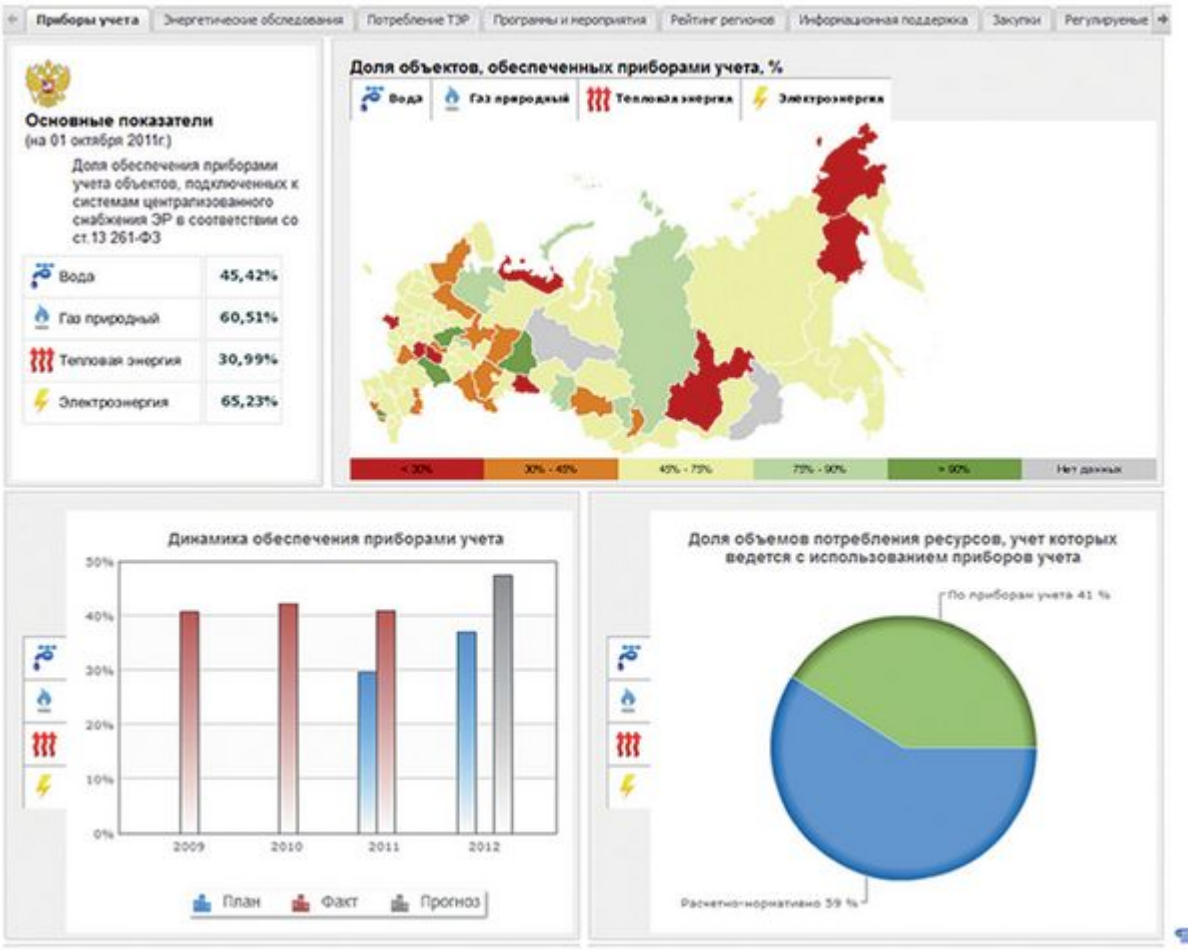
Адміністратор – це IT-спеціаліст, що налаштовує доступ до джерел даних, словник даних, запити. Практично неможливо забезпечити технічну захист даних від нього. Організаційно можна реалізувати такий сценарій, коли розділяються функції налаштування системи та розмежування прав. Налаштування виконується на тестових даних, а розмежуванням прав займається інший адміністратор, без доступу до даних.

Автор – це експерт, який створює аналітичні звіти для себе і (або) для інших користувачів. Доступ учасника може бути обмежений до певної області даних, а також до певних функцій системи. Автор звітів працює в онлайн з вихідним сховищем даних або корпоративними БД.

Експерт – кваліфікований користувач, що виконує незаплановані запити, заздалегідь не визначені маршрути серфінгу по даним.

Звичайний користувач – співробітник, що переглядає кінцевий набір звітів на регулярній основі з цілком певною метою. Для нього готуються звіти, що містять вузький набір даних, а його інтерфейс спрощений.

Одним з організаційних заходів захисту даних є ізоляція звітів від вихідної бази даних. Експерти і звичайні користувачі працюють із звітами, дані яких зберігаються в періодично оновлюваних «мікрокубах» і не мають доступу до вихідної БД.



Індикаторна панель Contour Business Intelligence (РФ)

ПУБЛІКАЦІЇ У ВІДКРИТОМУ ДОСТУПІ

BI може використовуватися для публікації на сайті організації річних звітів, статистики, курсів валют, вартості цінних паперів і так далі – для широкого кола користувачів .

Завдання поєднання потужних аналітичних можливостей BI з одночасним виключенням доступу користувачів до інформаційної системи організації та до її баз даних – вирішується публікацією даних у вигляді заздалегідь розрахованих і збережених «мікрокубів».

Російська Contour BI, чия Індикаторна панель Business Intelligence показана на зображенні у статті, є мультиплатформеною системою ім може бути встановлена безпосередньо на сервері інтернет-провайдера.

ЗБІР ДАНИХ

Розглянемо дві ситуації – автоматизований збір даних з інформаційних систем у центральне сховище даних і ручне введення звітних даних.

Автоматизований збір даних

Постачальник даних передає інформацію в web-сервіс одержувача даних. На його комп'ютер встановлюється програмно-апаратний комплекс, що забезпечує захищене VPN-з'єднання, електронний підпис, шифрування даних.

На сервері одержувача кожне повідомлення перевіряється на наявність вірусів, неприпустимих вкладень, коректності формату даних і електронного підпису.

Ручний збір даних

У ряді випадків потрібно використовувати ручне введення даних для передачі їх в центральне сховище даних. Для захищеного збору даних може бути запропоновано спеціальний програмно-апаратний пристрій, який виглядає, як USB-накопичувач. У цьому пристрої в області «тільки для читання» містяться операційна система і програмне забезпечення для введення даних – інтерпретатор форм, програми шифрування і електронного підпису, програма захищеного з'єднання, сертифікат підпису.

Комп’ютер завантажується з пристрою, тому воно фізично не може бути заражений вірусом або шпигунською програмою. В область читання-запису поміщаються XML-опис форм і необхідні класифікатори та довідники. Описи нових форм надходять в пристрій з центрального сховища і записуються в його пам’ять. Вводяться дані підписуються електронним підписом, шифруються і передаються через захищене з’єднання в web-сервер сховища даних.

Така технологія гарантує надійну аутентифікацію і захист даних від спотворень і крадіжки.

Висновки.

1. Реалізація систем підтримки прийняття рішень на основі Business Intelligence є обов`язкови елементом для всіх сфер діяльності сучасних підприємств, у тому числі для сфери інформаційної безпеки.

2. При реалізації проекту Business Intelligence особливо ретельно необхідно підходити до вибору постачальника платформи Business Intelligence. Адже для прикладу, у разі порушення безпеки встановленого програмного забезпечення для Business Intelligence на web-сервері , може стати доступною для несанкціонуваного аналізу чи пошкодження вся інформація підприємства на сервері. Особливо велика інформаційна небезпека виникає, коли керівники та фахівці підприємства, у тому числі з IT-безпеки не знають про аналітичні hi-tech можливості засобів Business Intelligence (OLAP, Data Mining, Text Mining, Web-Mining, Social Media Web Mining).

Джерела:

1. *Запит в Інтернеті: dashboard designe for IT Security.*
2. *Сайт: Dell SecureWorks BI dashboards for IT Security.*

3. *Стаття: Forrester Wave™: Enterprise Business Intelligence Platforms, 2015.*
4. *Стаття: Gartner Magic Quadrant for Bl & Analytics Platforms.*
5. *Стаття: IDC MarketScape: Worldwide Business Analytics Services 2015 Vendor Assessment.*
6. *Конференція: IDC IT Security Roadshow 2016 in Kyiv.*
7. *Стаття: Business Intelligence и информационная безопасность.*
8. *Оголощення: IDC IT Security Roadshow 2016 in Kyiv.*
9. *Сайт: Business Intelligence + KMS: концепція, технологія і засоби підтримки рішень не тривіальними знаннями з первинних даних(2011 р).*
10. *Сторінка сайту: Business Intelligence + KMS: для керівників.*
11. *Сторінка сайту: Business Intelligence + KMS: для аналітиків.*
12. *Сторінка сайту: Business Intelligence + KMS: для IT-працівників.*