AN ANALYSIS OF ICAO REQUIREMENTS AND RECOMMENDATIONS FOR INFORMATION SECURITY OF THE ATN

Development and commissioning of the Aeronautical Telecommunication Network using standards and protocols for Internet Protocol Suite accompanied by the ICAO requirements and recommendations for the protection of communications against unauthorized access. These requirements, on the one hand, are conceptual in nature determining the levels of protection in accordance with the classification of the OSI/ISO, the general methodology of protection, on the other hand, have mandatory defining specific processes and technical solutions protect information resources. The problem boils down to the integration of various technical security solutions considering their possible deviance, where permitted by the conceptual nature of the requirements, and at the same time ensuring the necessary level of protection. Procedures for the protection of information resources in the implementation of digital communication sessions "ground-to-ground" and "air-to-ground" in the network ATN/IPS, recommended by the regulations of the ICAO, should be implemented in the network, transport, and application layers of digital aeronautical communications. There is not clearly specified strict criteria for the required (guaranteed) level of protection (evaluation criteria for information security from unauthorized access) and at the same time regulates the use of measures to protect the information based on IPsec, IKEv2 and ESP. Therefore the development of threat models and the definition of the functional profile of security for automated systems (AS) of aviation applications can be based on the experience of the development of threat models and definitions of functional profiles of protection for AS of the class "2" and class "3", the operation of which is based on standard telecommunication channels using the standards and protocols of the Internet protocol Suite.

Keywords: information security, aeronautical telecommunications, Aeronautical Telecommunication Network, protection of Internet protocols, Internet Key Exchange protocol.

Голубничий Олексій Георгійович, кадидат технічних наук, доцент, докторант Національного авіаційного університету.
E-mail: a.holubnychyi@nau.edu.ua
Голубничий Алексей Георгиевич, кандидат технических наук, доцент, докторант Национального авиационного университета.
Holubnychyi Alexei, PhD in Eng., Docent, Doctoral Student of the National Aviation University.

УДК 004.658.2

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ МЕТОДОМ МАСКИРОВАНИЯ

Михаил Коломыцев, Анатолий Южаков

Согласно закону о защите персональных данных, владельцы баз персональных данных обязаны обеспечить их защиту. Основным видом хранилища для персональных данных в информационной системе является база данных. Практика разработки информационных систем показывает, что, кроме производственной (основной) базы данных, возникает задача создания ее копий, непроизводственных (тестовых) баз данных. Использовать в тестовых базах данных такой универсальный механизм, как криптография, для защиты персональных данных не всегда представляется возможным. Причина тому не только известные законодательные ограничения, но и то, что тестовые базы данных должны быть функционально эквивалентными производственной базе данных. Это означает, что защищаемая информация должна быть представлена в виде, не нарушающем целостность базы данных (как целостность по ссылкам, так и по принадлежности данных к определенному домену). Для защиты персональных данных в такой ситуации можно использовать подход, который называется маскирование данных. В данной статье раскрывается суть данного метода, его актуальность, требования к реализации. Авторы предлагают разработанную ими в виде программного кода методику защиты персональных данных в среде MS SQL Server.

***Ключевые слова**: база данных, персональные данные, защита персональных данных, маскирование данных, конфиденциальные данные, информационная система.*

Актуальность задачи маскирования данных. Согласно закону о защите персональных данных [1], владельцы баз персональных данных (ПД) обязаны обеспечить их защиту. Особенно важно защищать данные, идентифицирующие конкретную личность. К таким данным можно отнести индивидуальный налоговый номер (ИНН), серию и номер паспорта, ФИО, почтовые адреса, телефоны, номера банковских карточек и другие.

Основным видом хранилища для персональных данных в информационной системе является

база данных (БД). Практика разработки информационных систем показывает, что, кроме производственной (основной) базы данных, возникает задача создания ее копий, непроизводственных (тестовых) баз данных. Связано это с необходимостью проведения работ по развитию информационной системы, ее тестированию, обучению пользователей. Такие копии могут использоваться для аналитической обработки (data mining) и других целей. По некоторым оценкам, число непроизводственных баз данных может достигать 6-8 копий. И если в производственной БД поддерживается адекватная политика безопасности, то в тестовых БД вопросам безопасности внимания уделяется меньше, что повышает риски утечки данных.

Использовать в тестовых БД такой универсальный механизм, как криптография, для защиты ПД не всегда представляется возможным. Причина тому не только известные законодательные ограничения. Важной особенностью непроизводственных БД является то, что они должны быть функционально эквивалентными производственной БД. Это означает, что защищаемая информация должна быть представлена в виде, не нарушающем целостность БД (как целостность по ссылкам, так и по принадлежности данных к определенному домену). Все бизнес-процессы, реализуемые в информационной системе, должны функционировать нормально.

Для защиты ПД в такой ситуации можно использовать подход, который называется маскирование данных [2]. Цель статьи – раскрыть суть метода маскирования и требования к его реализации, а также предложить методику защиты персональных данных на основе этого метода в среде MS SQL Server.

Маскирование данных представляет собой процесс обезличивания или сокрытия определенных данных в таблицах базы. Маскирование данных по своей сути защищает конфиденциальные данные от неавторизованного доступа, изменяя их значения, но сохраняя при этом первоначальные параметры. Маскирование данных позволяет использовать их в интересах организаций, обеспечивая при этом выполнение требований законодательства и устраняя риск утечки данных.

При реализации процесса маскирования необходимо учитывать, что результат преобразования не должен быть обратимым в том смысле, что у лиц, не имеющих доступа к ключевой информации, не должно быть возможности восстановить оригинальный текст, используя маскированный. Маскировать открытую информацию нужно, только если она может быть использована для восстановления конфиденциальных данных [7]. Маскирование должно быть автоматизированным, легко повторяемым процессом. В случае, если данные в производственной БД меняются часто, маскирование должно быть простой и эффективной частью процесса создания непроизводственных БД.

Методы маскирования. Используются следующие методы маскирования [8]:

Подстановка. В этом случае используется замена одного значения другим. Например, фамилия субъекта заменяется случайно выбранной фамилией из таблицы подстановок, созданной на основе телефонного справочника.

Замена на символ-константу. Данный метод является частным случаем метода подстановки, когда все маскируемые символы заменяются одним и тем же символом, например, «X». В этом случае маскированный телефонный номер будет иметь вид «(XXX) XXX-XXXX». Это самый простой и быстрый метод маскирования, однако его ценность невелика.

Перестановка. Перестановка является методом рандомизации существующих значений вертикально в наборе данных, т.е. в столбце таблицы. Например, перестановка отдельных значений в столбце заработной платы таблицы сотрудников сделает бесполезной кражу информации о зарплате сотрудников. При этом статистические значения, вычисляемые с помощью агрегатных функций, не изменяются. Перестановка является распространенным методом маскирования, позволяющим скрыть взаимосвязи данных.

Размывание (bluring). Оригинальное значение заменяется случайным, но близким (в рамках определенного диапазона) значением.

Усреднение. В этом методе оригинальные числа заменяются случайными таким образом, что среднее значение по всему набору маскированных значений остается таким же, как и в оригинальном наборе.

Де-идентификация. Общее название для методов, позволяющих таким образом преобразовать исходную информацию, идентифицирующую личность, чтобы исчезла связь с данной личностью. Де-идентификация используется для маскирования сложных наборов данных, охватывающих несколько столбцов таблицы ПД.

Разбиения на лексемы (токены). В этом методе элементы данных заменяются случайными заполнителями (токенами). Представление данных в

виде токенов является необратимым, так как токен логически не связан с первоначальным значением.

Шифрование с сохранением формата. В этом методе маскирования данные преобразовываются в зашифрованную форму таким образом, что общий вид оригинального значения сохраняется.

Требования к методам маскирования. В общем виде задача маскирования выглядит достаточно простой. Однако необходимость соблюдать различного рода ограничения делает задачу маскирования гораздо более сложной, чем может показаться на первый взгляд. К типичным ограничениям процесса маскирования данных можно отнести:

Сохранение формата. Маскированные данные должны иметь такую же структуру, что и исходные данные. Это означает, что если исходные данные имеют, например, размер от 2 до 30 символов, маскированные данные должны также отвечать этому условию. Типичным примером является маскирование даты, которое должно происходить в правильных диапазонах для дня, месяца и года. Это означает, что алгоритм маскирования должен определить «смысл» исходных данных, таких как «31.03.2013», «31 марта 2013», и «03.31.2013», а также генерировать подходящую дату в том же формате.

Сохранение типа данных. Результаты маскирования должны соответствовать исходным данным. Применительно к базам данных это означает принадлежность маскированных данных к тому же домену, что и оригинальные данные.

Сохранение гендерных признаков. Например, при замене имен мужские имена должны заменяться на мужские, а женские – на женские.

Семантическая целостность. Исходя из семантики предметной области, на значения отдельных полей таблицы с помощью условия *check* накладываются ограничения. Для поддержания бизнес-процессов в информационной системе, маскированные значения должны отвечать таким же ограничениям.

Ссылочная целостность. Маскированные данные не должны нарушать ссылочную целостность таблиц БД. Например, если ИНН является первичным ключом, то все маскированные экземпляры одного и того же значения ИНН в связанных таблицах должны быть одинаковыми.

Сохранение обобщенных значений. Суммарные и средние значения по маскированной колонке таблицы должны совпадать с оригинальными (в точности, либо с определенным допуском).

Статистическое распределение значений. В некоторых случаях важно сохранить информацию о таких статистических характеристиках, как характер распределения. Например, если в БД содержится информация о географическом распределении онкобольных по почтовым индексам, то произвольная замена почтовых индексов может исказить результаты анализа.

Уникальность. Маскированные значения должны быть уникальными. Это особенно важно для поддержания ссылочной целостности.

Маскирование данных в MS SQL Server. В некоторых СУБД (например, Oracle [4]) средства маскирования данных уже реализованы. В данной статье авторы предлагают методику маскирования данных методом подстановки в СУБД MS SQL Server.

Основным элементом предлагаемой методики является таблица подстановок. Таблица подстановок создается для защищаемого поля в таблице персональных данных и состоит из трех колонок. Для каждой позиции в защищаемом поле в таблице подстановок указывается номер позиции, символ, который может быть в этой позиции, и символ, который его заменяет. Например, размер поля для хранения ИНН составляет 10 символов. Для каждой из 10-ти позиций задается пара «значение – замена» по всем возможным символам в этой позиции. Фрагмент таблицы подстановок для маскирования поля, хранящего ИНН, показан на рис. 1.

Results | Messages

	PositionNumber	OriginalText	MaskText
1	1	0	8
2	1	1	7
3	1	2	6
4	1	3	5
5	1	4	4
6	1	5	3
7	1	6	2
8	1	7	1
9	1	8	0
10	1	9	9
11	2	0	9
12	2	1	0
13	2	2	2
14	2	3	6
15	2	4	4
16	2	5	7
17	2	6	5
18	2	7	1
19	2	8	3
20	2	9	8

Рис. 1. Фрагмент таблицы подстановок

Такая структура таблицы позволяет лицам, имеющим доступ к ней, восстанавливать оригинальный текст. Если включить в таблицу символы, то можно маскировать серию и номер паспорта, телефонный номер и другие данные. Ключевое ограничение на таблицу связано с требованием возможности восстановления оригинального текста – каждому маскированному символу

должен соответствовать только один оригинальный символ. Конечно, символы замены должны быть такими, чтобы указанное выше требование целостности выполнялось.

Такая таблица может быть создана как временная таблица в базе данных *tempdb* сервера, табличной переменной в составе хранимой процедуры, либо в виде другого объекта БД с ограниченным доступом. Права доступа к такому объекту должны быть максимально ограниченными, в соответствии с требованиями политики безопасности.

Ниже приводится пример хранимой процедуры, маскирующей значения поля ИНН в таблице персональных данных. Текст процедуры снабжен комментариями.

```
USE [Имя_Базы_ПД]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE PROCEDURE [dbo].[INN_Mask]
-- Параметры: Оригинальный ИНН и маскированный ИНН
        @INN_IN varchar(10),
        @INN_OUT varchar(10) OUTPUT
AS
/*Объявление переменных для оригинальных (@P)и маскированных (@N) символов */
DECLARE
 @P1 char(1),@P2 char(1),@P3 char(1),@P4 char(1),@P5 char(1)
,@P6 char(1),@P7 char(1),@P8 char(1),@P9 char(1),@P10 char(1)
,@N1 char(1),@N2 char(1),@N3 char(1),@N4 char(1),@N5 char(1)
,@N6 char(1),@N7 char(1),@N8 char(1),@N9 char(1),@N10 char(1)

BEGIN
        SET NOCOUNT ON;
        --Извлекаем отдельные символы из оригинального ИНН
        SET @P1  = SUBSTRING(@INN_IN,1,1)
        SET @P2  = SUBSTRING(@INN_IN,2,1)
        SET @P3  = SUBSTRING(@INN_IN,3,1)
        SET @P4  = SUBSTRING(@INN_IN,4,1)
        SET @P5  = SUBSTRING(@INN_IN,5,1)
        SET @P6  = SUBSTRING(@INN_IN,6,1)
        SET @P7  = SUBSTRING(@INN_IN,7,1)
        SET @P8  = SUBSTRING(@INN_IN,8,1)
        SET @P9  = SUBSTRING(@INN_IN,9,1)
        SET @P10 = SUBSTRING(@INN_IN,10,1)
        --Находим маскированный символ, соответствующий оригинальному
        SET @N1 = (
        SELECT MaskText
        FROM dbo.##Masking_Table
        WHERE PositionNumber = 1 AND OriginalText = @P1)
        SET @N1 = ISNULL(@N1,@P1)
        SET @N2 = (
        SELECT MaskText
        FROM dbo.##Masking_Table
        WHERE PositionNumber = 2 AND OriginalText = @P2)
        SET @N2 = ISNULL(@N2,@P2)
-- Далее повторяются фрагменты кода для переменных @P, @N с
-- индексами 3…9
--
        SET @N10 = (
        SELECT MaskText
        FROM dbo.##Masking_Table
        WHERE PositionNumber = 10 AND OriginalText = @P10)
        SET @N10 = ISNULL(@N10,@P10)
        SET @INN_OUT = @N1 + @N2 + @N3 + @N4 + @N5 + @N6 + @N7 + @N8 + @N9 + @N10
        -- Вывод на экран оригинального и маскированного ИНН
        Print @INN_IN
        PRINT @INN_OUT
END
GO
```

Обращение к процедуре происходит следующим образом:

```
DECLARE @INN_IN varchar(10)
DECLARE @INN_OUT varchar(10)
EXECUTE [dbo].[INN_Mask] '078051120',
@INN_OUT OUTPUT
```

Результат:

078051120 — оригинальный ИНН

813026553 — маскированный ИНН

Заключение. Сегодня компании понимают важность обеспечения конфиденциальности своих клиентов. Согласно отчету о независимом исследовании фирмы Forrester Research, озаглавленного «Protecting Private Data with Data Masking» («Защита конфиденциальной информации с помощью маскирования данных») в ближайшие не-

сколько лет до 35% компаний начнут использовать технологию маскирования данных в тестовом режиме для контрольных данных. Ведущие производители программного обеспечения, такие как IBM, Oracle, выпускают на рынок средства маскирования данных [3-6]. В нашей стране, в связи с принятием закона о защите ПД, необходимость в разработке аналогичных средств очевидна.

ЛИТЕРАТУРА

[1]. Закон України «Про захист персональних даних» від 01.06.2010 №2297-VI (редакція станом на 09.06.2013) [Електронний ресурс]. – Режим доступу http://zakon.rada.gov.ua/go/2297-17

[2]. Data masking [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Data_masking.

[3]. Data Masking [Электронный ресурс]. – Режим доступа: http://www.datamasking.com/solutions/products/datamasking.

[4]. Data Masking Best Practice [Электронный ресурс]. – Режим доступа: http://www.oracle.com/us/products/database/data-masking-best-practices-161213.pdf.

[5]. Dynamic Data Masking [Электронный ресурс]. – Режим доступа: http://www.data-integration.ru/products/section323/section331.

[6]. IBM представила ПО для маскировки закрытых данных [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/301841.php.

[7]. The Five Laws of Data Masking [Электронный ресурс]. – Режим доступа: https://securosis.com/blog/the-five-laws-of-data-masking.

[8]. Understanding and Selecting Data Masking Solutions: Creating Secure and Useful Data [Электронный ресурс]. – Режим доступа: https://securosis.com /assets/library/reports/UnderstandingMasking_FinalMaster_V3.pdf.

REFERENCES

[1]. A law of Ukraine «On the protection of the personal data» by 01.06.2010 №2297- VI (a release is by the state on 09.06.2013) [electronic resource]. – Mode access: http://zakon.rada.gov.ua/go/2297-17.

[2]. Data masking [electronic resource]. – Mode access: http://en.wikipedia.org/wiki/Data_masking.

[3]. Data Masking [electronic resource]. – Mode access: http://www.datamasking.com/solutions/products/datamasking.

[4]. Data Masking Best Practice [electronic resource]. – Mode access: http://www.oracle.com/us/products /database/data-masking-best-practices-161213.pdf.

[5]. Dynamic Data Masking [electronic resource]. – Mode access: http://www.data-integration.ru/products /section323/section331.

[6]. IBM presented products for data protection [electronic resource]. – Mode access: http://www. securitylab.ru/news/301841.php.

[7]. The Five Laws of Data Masking [electronic resource]. – Mode access: https://securosis.com/blog/the-five-laws-of-data-masking.

[8]. Understanding and Selecting Data Masking Solutions: Creating Secure and Useful Data [electronic resource]. – Mode access: https://securosis.com/assets/library/reports/UnderstandingMasking_FinalMaster_V3.pdf.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ МЕТОДОМ МАСКУВАННЯ

Згідно закону про захист персональних даних, власники баз персональних даних зобов'язані забезпечити їх захист. Основним видом сховища для персональних даних у інформаційній системі є база даних. Практика розробки інформаційних систем показує, що крім виробничої (основної) бази даних виникає задача створення її копій, невиробничих (тестових) баз даних. Використовувати в тестових базах даних такий універсальний механізм, як криптографія, для захисту персональних даних не завжди є можливим. Причина цьому не лише відомі законодавчі обмеження, але й те, що тестові бази даних мають бути функціонально еквівалентними виробничій базі даних. Це означає, що інформація, яка захищається, має бути подана у вигляді, що не порушує цілісність бази даних (як цілісність за посиланнями, так і за належністю даних до певного домену). Для захисту персональних даних в такій ситуації можна використати підхід, який має назву маскування даних. У даній статті розкривається суть цього метода, його актуальність, вимоги до реалізації. Автори пропонують розроблену ними у вигляді програмного коду методику захисту персональних даних в середовищі MS SQL Server.

Ключові слова: база даних, персональні дані, захист персональних даних, маскування даних, конфіденційні дані, інформаційна система.

PROTECTION OF THE PERSONAL DATA BY DATA MASKING METHOD

In accordance to a law on the protection of the personal data, proprietors of bases of the personal information are under an obligation to provide their defence. By the basic type of depository for the personal information there is a database in the informative system. Practice of development of the informative systems shows that except for a productive (basic) database there is a task of creation of its copies, unproductive (test) databases. To use such universal mechanism in test databases, as cryptography, for the protection of the personal data is not always possible. Reason to that not only the known legislative limitations but also that test databases must be functionally equivalent a production database. It means that the protected information must be presented in a kind, not defiat integrity of database (both integrity on references and on belonging of information to the certain domain). For the protection of the personal data it is possible to take approach in such situation, which is named data masking

method. Essence of this method, his actuality, requirements to realization, opens up in this article. Authors offer developed by them as a programming code of protection of the personal data in the environment of MS SQL Server.
Keywords: data base, personal data, protection of the personal data, data masking, confidential data, information system.

Коломыщев Михаил Владимирович, кандидат технических наук, доцент, доцент кафедры информационной безопасности Национального технического университета Украины «Киевский политехнический институт».
E-mail: box144a@ukr.net
Коломицев Михайло Володимирович, кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут».
Kolomytsev Mykhailo, PhD, reader of Information Security Cathedra, National Technical University of Ukraine «Kiev Polytechnic Institute».

Южаков Анатолий Михайлович, техник отдела информатизации департамента перспективного развития Национального технического университета Украины «Киевский политехнический институт».
E-mail: conf@pti.kpi.ua
Южаков Анатолій Михайлович, технік відділу інформатизації департаменту перспективного розвитку Національного технічного університету України «Київський політехнічний інститут».
Yuzhakov Anatoly, technician of Informatization Department, National Technical University of Ukraine «Kiev Polytechnic Institute».

УДК 004.056.53:004.492.3 (045)

МЕТОД ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ПОРУШНИКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Анна Корченко, Світлана Казмірчук, Андрій Гізун, Владислава Волянська, Сергій Гнатюк

Забезпечення безпеки державних інформаційних ресурсів нерозривно пов'язане з виявленням діяльності порушника інформаційної безпеки (ІБ) в інформаційно-комунікаційних системах (ІКС), в яких циркулює інформація з обмеженим доступом. Недоліком сучасних систем виявлення порушника ІБ, побудованих на евристичних правилах (ЕП) в тому, що вони в основному орієнтовані на використання таких математичних моделей, які вимагають багато часу на підготовку статистичних даних. Математичні моделі, засновані на експертних підходах, у цьому відношенні є більш ефективними. Пропонується метод, що дозволяє на основі суджень експерта в нечітких умовах розв'язати задачу виявлення та ідентифікації порушника (ВІП) в ІКС. У методі використовуються елементи нечіткої логіки для попереднього прийняття рішення про порушення та ідентифікацію особи порушника, а також базис звичайної чіткої логіки, що забезпечує уточнюючу інформацію. Метод включає етапи: формування коефіцієнтів важливості, множин категорій порушника та параметрів, еталонів нечітких параметрів, множини ЕП, зв'язок категорії порушника з параметрами; формування та фазифікації параметрів, обробки і формування кортежів параметрів; формування результату. Робота методу організована у 3 фази: підготовча; робота з нечіткими параметрами; робота з чіткими параметрами. Засновуючись на цьому методі може бути синтезована система ВІП, що базується на ЕП і характеризується високою ефективністю роботи в умовах нечіткості.
***Ключові слова**: системи виявлення порушника, порушник інформаційної безпеки, ідентифікація, виявлення аномалій в інформаційно-комунікаційних системах, метод, нечітка логіка, базова модель ідентифікації порушника, логіко-лінгвістична зв'язка, евристичні правила, експертна оцінка.*

Однією з головних складових національної безпеки держави є інформаційна безпека (ІБ), яка визначається сукупністю різноманітних характеристик та категорій у сфері захисту інформації. У цьому аспекті вагоме місце займає такий напрям як захист державних інформаційних ресурсів (ДІР). Враховуючи стрімкий розвиток інформаційних технологій, що впливає як на захисні механізми, так і на засоби проведення інформаційних атак, набір можливих дій порушника значно збільшується. Безперервно зростає кількість порушників (неавторизованих сторін – НАС), загроз ІБ, а також проводяться принципово нові кібератаки на інформаційні ресурси, що ускладнює реалізацію ефективного захисту. Досягнення максимального ефекту захищеності ДІР можливе за умови того, що потенційні порушники ІБ (ППБ) відомі і це створює передумови для підбору та застосування