DOI: 10.18372/2410-7840.20.12451
УДК 004.652.4

МОДЕЛИ МНОГОУРОВНЕВОЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ

Михаил Коломыцев, Светлана Носок, Анастасия Мазуренко

Многоуровневая безопасность - это политика безопасности, которая позволяет классифицировать объекты и пользователей на основе системы иерархических уровней безопасности и использовать такую классификацию для организации системы управления доступом. Как правило, такая политика безопасности используется при обработке информации с ограниченным доступом. В реляционных базах данных с многоуровневой безопасностью любому пользователю, читающему или обновляющему данные в таблице, должно быть разрешено обрабатывать только те строки, которые позволяет его уровень доступа, представленный меткой безопасности. Для каждой строки таблицы (или атрибута строки) устанавливается уровень конфиденциальности путем присвоения метки безопасности. Пользователь может читать или изменять строку, только если его метка доминирует над меткой строки. Это требование приводит к тому, что один и тот же объект предметной области может быть представлен в таблице несколькими записями, каждая из которых, доступна только пользователям с соответствующей меткой безопасности (свойство многозначности отношений). В свою очередь, фундаментальные принципы построения реляционных баз данных требуют уникальности каждого кортежа отношения. Способ разрешения этого противоречия определяется используемой моделью безопасности. Кроме этого, многозначность отношений приводит к появлению уязвимостей в виде скрытых каналов(covert channels), получения информации путем логических выводов (inference channels), семантической двусмысленности(semantic ambiguity)и других. В качестве направления исследований в области безопасности баз данных технология многоуровневой безопасной базы данных развивается достаточно интенсивно. На основе модели Белл-Лападула было разработано много моделей многоуровневой безопасности в реляционных базах данных, таких как модель SeaView, модель Jajodia-Sandhu, модель Smith-Winslett и другие, которые решали,в большей или меньшей степени, возникающие проблемы. Однако на сегодняшний день не предложено решения или модели, свободной от всех недостатков.

***Ключевые слова**: база данных, защита данных, контроль доступа, многоуровневая безопасность, модели многоуровневой безопасности.*

АКТУАЛЬНОСТЬ И ПОСТАНОВКА ЗАДАЧИ

Многоуровневая безопасность (MLS) - это политика безопасности, позволяющая организовать доступ к категорированной информации со стороны пользователей, имеющих разные уровни доступа. Такая политика безопасности формируется на основе как традиционных дискреционных средств контроля доступа, так и средств контроля, которые предотвращают доступ пользователей к информации с недоступной для них категорией, или к изменению категории информации, к которой у них имеется доступ.

Поскольку основным типом СУБД, используемых для обработки конфиденциальной информации являются реляционные (РСУБД), значительные усилия в области исследований и разработок были направлены на создание многоуровневых безопасных РСУБД, что привело к появлению множества решений РСУБД, в том числе коммерческих. В разных формах, многоуровневая безопасность поддерживается ведущими разработчиками СУБД – Oracle (Oracle label security), IBM (DB2 multilevel security). Используемые и предлагаемые решения основываются на определенных моделях разграничения доступа. Данная статья посвящена анализу этих моделей, их достоинствам и недостаткам.

Постановка задачи. Проанализировать существующие модели многоуровневой безопасности, выделить их характерные особенности и определить достоинства и недостатки.

Цель работы: анализ моделей многоуровневой безопасности, определение их достоинств и недостатков.

ОРГАНИЗАЦИЯ МНОГОУРОВНЕВОЙ БЕЗОПАСНОСТИ В РСУБД

Системы с многоуровневой безопасностью позволяют разграничивать доступ к объектам на основе классификационной метки безопасности, присвоенной данному объекту. Метка определяет уровень конфиденциальности объекта. Субъектам доступа так же присваивается метка безопасности, определяющая их уровень доступа. Метки связаны между собой иерархически, так что можно определить метку с низким или высоким уровнем безопасности. Контроль доступа в таких системах основан на доминировании меток.

Как правило, для определения условий доминирования используется известная модель Белл-ЛаПадула (Bell-LaPadula) [1]. Применительно к базам данных модель может быть представлена в следующем виде.

Схему отношения реляционной базы данных без многоуровневой безопасности обозначим как

$$\mathbf{R(A_1; \ldots; A_n)}, \quad (1)$$

где $\mathbf{A_i}$ – атрибут отношения.

В реляционной базе данных с многоуровневой безопасностью (MLS) каждому атрибуту отношения присваивается метка безопасности. Кроме того, многоуровневая схема отношения может содержать дополнительный атрибут, который определяет уровень безопасности кортежа отношения в целом. Схему отношений с MLS (многоуровневого отношения) обозначим как:

$$\mathbf{R\ (A_1,\ C_1;\ ...;\ A_n,\ C_n;\ TC)}, \quad (2)$$

где $\mathbf{A_i}$ – атрибуты данных, $\mathbf{C_i}$ - метки безопасности для $\mathbf{A_i}$, а **TC** является меткой безопасности кортежа [2].

Если разделение полномочий доступа происходит только на уровне кортежей (row level security), то схема отношения принимает вид:

$$\mathbf{R\ (A_1,...\ A_n,\ TC)}. \quad (3)$$

Если разделение полномочий на уровне кортежей нет, то схема отношения принимает вид:

$$\mathbf{R\ (A_1,\ C_1;\ ...;\ A_n,\ C_n)}. \quad (4)$$

Пример отношения с MLS приведен в табл. 1. Используется набор меток вида **L**, **M**, **H** (в порядке возрастания иерархии **L < M < H**). Первичный ключ отношения составной (Сотрудник, Должность).

Согласно простому свойству безопасности модели Bell-LaPadula, многоуровневое отношение должно быть доступно разными пользователями в зависимости от их уровня доступа (метки безопасности). Например, пользователь с меткой **L** увидит экземпляр отношения, как показано в табл. 2, Пользователь с меткой **M** увидит экземпляр отношения как показано в табл. 3, в то время как пользователь с меткой **H** увидит все кортежи отношения.

Таблица 1

Пример отношения с MLS

Сотрудник	$\mathbf{C_1}$	**Должность**	$\mathbf{C_2}$	**Зарплата**	$\mathbf{C_3}$	**TC**
Іваненко І.І.	L	Лаборант	L	1000	L	L
Іваненко І.І.	M	Програміст	M	3000	M	M
Петренко П.П.	L	Інженер	L	2000	M	L
Сидоренко С.С.	H	Системний адміністратор	H	10000	H	H

Таблица 2

Видимая часть отношения для пользователя с меткой **L**

Сотрудник	$\mathbf{C_1}$	**Должность**	$\mathbf{C_2}$	**Зарплата**	$\mathbf{C_3}$	**TC**
Іваненко І.І.	L	Лаборант	L	1000	L	L
Петренко П.П.	L	Інженер	L	Null	L	L

Таблица 3

Видимая часть отношения для пользователя с меткой **M**

Сотрудник	$\mathbf{C_1}$	**Должность**	$\mathbf{C_2}$	**Зарплата**	$\mathbf{C_3}$	**TC**
Іваненко І.І.	L	Лаборант	L	1000	L	L
Іваненко І.І.	M	Програміст	M	3000	M	M
Петренко П.П.	L	Інженер	L	2000	L	L

УГРОЗЫ БЕЗОПАСНОСТИ В МНОГОУРОВНЕВЫХ ОТНОШЕНИЯХ

Непосредственная реализация отношения со схемой (2) приводит к возникновению скрытых каналов. Скрытый канал возникает в силу того, что пользователь более низкого уровня может узнать некоторую информацию с более высокого уровня безопасности [3].

Возможные нарушения безопасности возникают в следующий случаях:

1. Когда пользователь с низким уровнем доступа (низкой меткой безопасности) вставляет кортеж, значения атрибутов которого совпадают с существующим кортежем с более высокой меткой безопасности. Например, если пользователь с меткой безопасности **L** попытается вставить в таблицу 1 кортеж с ключевыми атрибутами *Сотрудник = 'Сидоренко С.С.', Должность = 'Системний адміністратор'*.

2. Когда пользователь с высоким уровнем доступа вставляет кортеж, значения атрибутов которого совпадают с существующем кортежем с более низкой меткой безопасности. Например, если пользователь с меткой безопасности **H** попытается вставить в таблицу кортеж с ключевыми атрибутами *Сотрудник = 'Іваненко І.І.', Должность = 'Лаборант'*.

В первом случае возможны такие варианты поведения базы данных [4]:

– информирование пользователя о том, что новый кортеж существует с более высоким уровнем безопасности, и поэтому вставка нового кортежа будет отклонена. Выбор этого варианта приводит к появлению скрытого канала, поскольку пользователь с низким уровнем доступа не санкционированно получает информацию с высоким уровнем безопасности;

– замена существующего кортежа с высоким уровнем безопасности на новый кортеж с низким уровнем безопасности. Этот выбор позволяет пользователю с низким уровнем доступа перезаписывать данные, невидимые ему и, таким образом, нарушать целостность данных.

Во втором случае так же возможны два варианта поведения [5]:

– уведомление пользователя о том, что существует такой же кортеж с более низким уровнем безопасности, и поэтому вставка нового кортежа будет отклонена. Выбор этого варианта приводит к проблеме отказа в обслуживании, поскольку новый кортеж, который должен быть вставлен пользователем с высоким уровнем доступа отклоняется пользователем с низким уровнем доступа;

– замена существующего кортежа с низким уровнем безопасности новый кортеж с высоким уровнем безопасности. Выбор этого варианта приводит к появлению скрытого канала, потому что пользователь с низким уровнем доступа получает информацию с высоким уровнем безопасности.

МНОГОЗНАЧНЫЕ МОДЕЛИ MLS

В определенной степени проблему скрытых каналов можно решать через нормализацию таблиц, разбивая их на связанные таблицы, уровень конфиденциальности которых, или конфиденциальность части записей которых, будет различным (вертикальная и горизонтальная декомпозиция). В СУБД DB2 Multilevel Security можно использовать возможность запрета записи в низ (write-down option).

Другие подходы основываются на расширении реляционной модели в сторону многозначности и допущения существования в таблицах кортежей с одинаковыми значениями ключевых полей.

В работе [6] расширяется понятие первичного ключа, добавляя к нему метку безопасности. При таком подходе более одного кортежа может обладать одним и тем же первичным ключом, если они имеют разные метки безопасности. Такой способ организации многоуровневых отношений называется многозначностью отношения (polyinstantiation). В многоуровневой реляционной базе данных отношение является многозначным, если оно содержит два или более кортежей с одинаковыми значениями первичного ключа.

В первом рассмотренном выше случае нарушения безопасности механизм многозначности позволяет вставить новый кортеж с низкой меткой безопасности без изменения существующего кортежа на высокой меткой.

Во втором случае механизм многозначности позволяет вставить новый кортеж с высокой меткой безопасности без изменения существующего кортежа с низкой меткой. И в этом случае в базе данных будут два кортежа в отношении с одним и тем же первичным ключом, но с разными уровнями безопасности.

В зависимости от используемой схемы отношений (3) или (4), многозначность может быть реализована как [7]:

– многозначность сущности: отношение содержит более одного кортежа с одинаковыми значениями первичного ключа, но с разными значениями метки безопасности для первичного ключа;

– многозначность атрибута: отношение содержит два или более кортежей с идентичным первичным ключом и значениями метки безопасности, но с разными значениями метки безопасности для одного или нескольких оставшихся атрибутов.

Рассмотри известные модели многоуровневой безопасности РСУБД.

Модель Secure Data Views (SeaView)

В этой модели метки безопасности присваиваются каждому атрибуту в кортеже, как в схеме (4). Данные хранятся в виде набора отношений с одним уровнем доступа (одноуровневые отношения), а многоуровневые отношения реализуются как представления (view) над этим одноуровневым отношениям [8].

При реализации модели SeaView используются два алгоритма:

– декомпозиции многоуровневого отношения на фрагменты с одним уровнем безопасности;

– восстановления исходного многоуровневого отношения из фрагментов.

Декомпозиция многоуровневых отношений на одноуровневые выполняется путем применения двух типов фрагментации: горизонтальной и вертикальной. При этом создаются отношения для первичных ключей (отдельно для каждого уровня доступа) и отношения для пар Ключ-Атрибут так же отдельно для каждого уровня безопасности.
Например, отношение с ключевым атрибутом **Сотрудник** (таблица 4), в результате декомпозиции будет разделено на 5 отношений (таблицы 5-9).

Таблица 4

Исходное отношение в модели SeaView

Сотрудник	C_1	**Должность**	C_2	**Зарплата**	C_3
Іваненко І.І.	L	Лаборант	L	1000	L
Іваненко І.І.	L	Програміст	M	3000	M

Таблица 5

Декомпозиция исходного отношения для первичного ключа

Сотрудник	**C_1**
Іваненко І.І.	L

Таблица 6

Декомпозиция исходного отношения для пары Сотрудник -Должность (метка **L**)

Сотрудник	**C_1**	**Должность**	**C_2**
Іваненко І.І.	L	Лаборант	L

Таблица 7

Декомпозиция исходного отношения для пары Сотрудник -Должность (метка **M**)

Сотрудник	**C_1**	**Должность**	**C_2**
Іваненко І.І.	L	Програміст	M

Таблица 8

Декомпозиция исходного отношения для пары Сотрудник -Зарплата (метка **L**)

Сотрудник	**C_1**	**Зарплата**	**C_3**
Іваненко І.І.	L	1000	L

Таблица 9

Декомпозиция исходного отношения для пары Сотрудник -Зарплата (метка **M**)

Сотрудник	**C_1**	**Зарплата**	**C_3**
Іваненко І.І.	L	3000	M

Недостатки модели SeaView связаны с реализацией алгоритмов декомпозиции и восстановления [9]:

– ложные кортежи: при восстановлении многоуровневых отношений из одноуровневых появляются дополнительные кортежи. Эти дополнительные кортежи называются ложными кортежами и являются результатом повторных соединений между одноуровневыми отношениями;

– ограниченность: в работе [9] приведены примеры отношений, к которым нельзя применить алгоритм декомпозиции SeaView;

– ресурсоемкость: алгоритм восстановления многоуровневого отношения в модели SeaView основан на левом внешнем соединении отношений. Из-за вертикальной фрагментации, которая используется в модели SeaView, запрос, который включает несколько атрибутов, будет использовать много левых внешних соединений между несколькими одноуровневыми отношениями. Хорошо известно, что соединение является дорогостоящей в смысле затрат ресурсов операцией.

Модель Jajodia–Sandhu

Модель Jajodia-Sandhu получена из модели SeaView. В этой модели усовершенствованы алгоритмы декомпозиции и восстановления [9].

В модели Jajodia-Sandhu используется только горизонтальная фрагментация. Это позволяет улучшить алгоритм восстановления, поскольку можно восстановить многоуровневое отношение без необходимости выполнять операции соединения (join), для восстановления многоуровневой связи требуются только операции объединения (union).

Исходное отношение будет разделено на набор отношений, в котором все не ключевые атрибуты имеют одинаковый уровень доступа:

$$\mathbf{R_i\ (PK,\ C_{PK};\ A_1,\ C_i;\ \ldots;\ A_n,\ C_i)}. \qquad (5)$$

Например, отношение (таблица 4), после декомпозиции примет вид (таблицы 10-11).

Таблица 10

Декомпозиция отношения (таблица 4) в модели Jajodia-Sandhu (метка **L**)

Сотрудник	**C_1**	**Должность**	**C_2**	**Зарплата**	**C_3**
Іваненко І.І.	L	Лаборант	L	1000	L

Таблица 11

Декомпозиция отношения (таблица 4) в модели Jajodia-Sandhu (метка **M**)

Сотрудник	**C_1**	**Должность**	**C_2**	**Зарплата**	**C_3**
Іваненко І.І.	L	Програміст	M	3000	M

В модели Jajodia-Sandhu есть две основные проблемы: [10]:

– семантическая двусмысленность. Предположим, что после декомпозиции, существуют отношения с уровнями безопасности **L** и **M**, и нет отношения с уровнем безопасности **H**. Если пользователь с уровнем доступа **H** захочет получить информацию из отношений, то, вследствие многозначности он не может решить, какой из кортежей является правильным;

– операционная неполнота: предположим, что существуют два различных уровня безопасности: $\mathbf{M_1}$ и $\mathbf{M_2}$, чья наименьшая верхняя граница - уровень безопасности **M**, а наибольшая нижняя граница - уровень безопасности **L**. У пользователя с уровнем доступа **M** нет возможности вставлять кортежи, которые содержат атрибуты с уровнями безопасности **L**, $\mathbf{M_1}$ и $\mathbf{M_2}$.

Модель Smith–Winslett

В модели Smith-Winslett многоуровневая реляционная база данных рассматривается как набор

обычных реляционных баз данных с одной и той же схемой, но разными уровнями безопасности. Модель не поддерживает разделение доступа на уровне каждого отдельного атрибута. Метка безопасности может быть присвоен только атрибутам первичного ключа и кортежам в целом [11].

Многоуровневая реляционная схема задается как

$$\mathbf{R\ (PK, C_{PK}, A_1 \ldots, A_n, TC)}, \quad (6)$$

где **PK** – первичный ключ, $\mathbf{C_{pk}}$ – метка безопасности первичного ключа, $\mathbf{A_1 \ldots A_n}$ атрибуты данных, а **TC** – метка безопасности кортежа, $\mathbf{TC \geq C_{PK}}$.

В соответствии с этой моделью, отношение из таблицы 1 (без последнего кортежа), будет представлена в виде (таблица 12):

Таблица 12

Представление отношения (таблица 1) в модели Smith-Winslett

Сотрудник	$\mathbf{C_{pk}}$	**Должность**	**Зарплата**	**TC**
Іваненко І.І.	L	Лаборант	1000	L
Іваненко І.І.	L	Програміст	3000	M
Петренко П.П.	L	Інженер	2000	L

Пользователь может видеть кортежи своего уровня безопасности и кортежей всех более низких уровней безопасности. Например, пользователь с уровнем доступа **M** будет видеть первый и второй кортеж отношения, но доверять (считать истинным) будет только второй кортеж. Пользователь с уровнем доступа **H** будет видеть все кортежи, но доверять не будет ни одному из них. Пользователь может изменять кортежи только собственного уровня безопасности и. те кортежи, которым он доверяет. Поэтому, модель Smith-Winslett иногда называют основанной на доверии (belief-based). Модель проста и эффективна.

Механизм обновления устраняет проблемы, существующие в модели Jajodia-Sandhu, но ограничивает область обновления одним объектом. Объектом определяется парой (**PK**, $\mathbf{C_{PK}}$). Таким образом, командами Insert, Update или Delete можно изменить только один кортеж. Данное свойство является основным недостатком модели.

Модель MultiLevel Relation (MLR)

Модель многоуровневого отношения (MLR) реализует концепцию целостности данных, путем организации восходящий потоков информации. Модификации данных на более низком уровне безопасности могут автоматически распространяться на более высокие уровни безопасности, которые наследуют эти данные [12].

Многоуровневая реляционная схема имеет вид:

$$\mathbf{R\ (PK, C_{PK}, A_1, C_1, \ldots, A_n, C_n, TC)},$$

где **PK** – первичный ключ, $\mathbf{C_{pk}}$ – метка безопасности первичного ключа, $\mathbf{A_1 \ldots A_n}$ – атрибуты данных, $\mathbf{C_1 \ldots C_n}$ – метки безопасности атрибутов, **TC** – метка безопасности кортежа.

В этой модели устранены проблемы семантической двусмысленности, присущие модели Jajodia-Sandhu. Пользователь с заданным уровнем доступа может получать данные, состоящие из двух частей: данные с таким же как у него уровнем безопасности и данные, которые наследованы от пользователей с более низким уровнем доступа. Наследование аналогично операции "запись вверх", но без перезаписи кортежей с более высоким уровнем безопасности. Наследованные данные могут быть изменены их владельцем с более низким уровнем доступа. Пользователь может видеть данные своего уровня и более низких уровней. Для этого в модели добавлена команда UPLEVEL, с помощью которой пользователь может указать, каким кортежам с более низкой меткой безопасности он доверяет.

Модель свободна от недостатка модели Smith-Winslett по количеству обновляемых кортежей в одной команде. Ограничением модели является отсутствие возможности указать, каким кортежем нельзя доверять.

Модель Belief-Consistent Multilevel Secure Data Model (BCMLS)

В модели данных BCMLS каждому атрибуту присваивается метка безопасности [13]. Метка безопасности может состоять из одной или несколько букв, и каждая буква определяет уровень безопасности. Первая буква определяет уровень безопасности, на котором было создано значение атрибута, и называется первичным уровнем безопасности этого атрибута. Модель BCMLS определяет первичный уровень безопасности как уровень, на котором кортеж был вставлен в отношение и такой кортеж называется первичным кортежем. Считается, пользователь доверяет информации, если его метка безопасности равна первичному уровню безопасности атрибута данных.

Буквы, которые следуют за первой буквой метки, называются вторичными уровнями, и они определяют уровни безопасности пользователей, которые доверяют этой информации. Каждая следующая буква в метке должна задавать уровень безопасности больший, чем задает буква, стоящая в метке слева от нее (доминирует над предыдущей буквой). Если перед буквой нет символа отрицания (–), то пользователи с такой меткой безопасности

доверяют информации. Если перед буквами есть символ (–), это означает, что пользователи с такими уровнями доступа этой информации не доверяют.

Помимо меток безопасности атрибутов, кортеж в целом также помечен меткой безопасности. Кортеж виден пользователю, только если метка его метка безопасности содержится в метке безопасности кортежа. Так же, как и атрибутам, пользователь может доверять либо не доверять кортежу. Если кортеж более низкого уровня представляет собой ту же сущность предметной области, что и другие кортежи более высокого уровня безопасности, то он определяется пользователем с более высоким уровнем безопасности как ложный кортеж.

Например, данные в таблице 13 считаются истинными для пользователей с уровнем доступа **L** и **M** и ложными для пользователей уровня **H.**

Пользователь видит и доверяет содержимому базы данных на своем уровень доступа, а также может получить доступ к содержимому базы данных на более низких уровнях. Пользователи, каждый на своем уровне доступа, могут решить, какой информации можно доверять. Большим преимуществом модели BCMLS является то, что информацию не нужно тиражировать, если метки атрибутов кортежа одинаковые.

Теоретически модель BCMLS является наиболее полной, но она никогда не была полностью реализована, потому что она очень сложна.

Таблица 13

Пример отношения в модели BCMLS

Сотрудник	**C_1**	**Должность**	**C_2**	**Зарплата**	**C_3**	**TC**
Іваненко І.І.	L	Лаборант	L	1000	L	L
Петренко П.П.	LM-H	Інженер	LM-H	2000	LM-H	LM-H

ЗАКЛЮЧЕНИЕ

РСУБД с многоуровневой безопасностью позволяют организовать доступ к категорированной информации. Однако, организация многоуровневой безопасности затрагивает все компоненты информационной системы – ОС. СУБД, прикладное ПО, аппаратную часть. При успешной реализации всех составляющих многоуровневой безопасности, следует учитывать особенности используемых моделей безопасности, а также присущие всем им недостатки:

1. Избыточность хранимых данных. Все рассмотренные модели предполагают избыточность хранения данных. В одних моделях (SeaView, MLR) это свойство выполняется для многоуровневых отношений любого вида. В других моделях (BCMLS) избыточность возникает, если метки безопасности атрибутов имею разный уровень.

2. Проблема логического вывода по значениям Null. Ограничение доступа к значениям атрибутов с более высокой меткой безопасности решается путем вывода значения Null для соответствующего атрибута. Это в свою очередь, приводит к возникновению скрытых каналов [15].

3. Проблема конфиденциальности значений первичного ключа. Первичные ключи отношений принято делить на естественные и суррогатные. Если первичный ключ не является суррогатным, и семантически связан с содержимым кортежа, то для многоуровневого отношения нельзя использовать подход на основе многозначности [16].

ЛИТЕРАТУРА

[1]. Д. Зегжда, А. Ивашко, *Основы безопасности информационных систем*, М.: Горячая линия, Телеком, 2000, 452 с.

[2]. W. Rjaibi, P. Bird, "A multi-purpose implementation of mandatory access control in relational database management systems", *Proceedings of the 30th VLDB Conference*, Toronto, Canada, pp. 1010-1020, 2004.

[3]. I. Ray, W. Huang, "Event detection in multilevel secure active databases", *Proceedings of the International Conference ICISS 2005*, pp. 177-190, 2005.

[4]. R. S. Sandhu, S. Jajodia, "Polyinstantiation for cover stories", *Proceedings of Second European Symposium on Research in Computer Security,* Toulouse, France, pp. 307-328, 1992.

[5]. S. Jajodia, R. S. Sandhu, B. T. Blaustein, "Solutions to the polyinstantiation problem, in information security", *An integrated collection of essays, ed. M. Abrams*, IEEE Computer Society Press, pp. 493-529, 1995.

[6]. A. Galinovi and V. Anton, "Polyinstantiation in relational databases with multilevel security", *Proceedings of the ITI 2007 29th International Conference on Information Technology Interfaces,* pp. 128-132, 2007.

[7]. D. Nelson, C. Paradise, "Using polyinstantiation to develop an MLS application", *Proceedings of the Seventh Annual Computer Security Applications Conference*, pp. 12-22, 1991.

[8]. M. Heckman, W. R. Shockley, "Te SeaView security model", *IEEE Transactions on Software Engineering*, no. 6 (6), pp. 593-607, 1990.

[9]. S. Jajodia, R. S. Sandhu, "A novel decomposition of multilevel relations into single-level relations", *IEEE Symposium on Security and Privacy,* Oakland, California, pp. 300-313, 1991.

[10]. S. Jajodia, R. Sandhu, "Toward a multilevel secure relational data model", *Proceedings of ACM SIGMOD International Conference on Management Data,* Denver, Colorado, pp. 50-59, 1991.

[11]. J. Biskup, L. Wiese, "Combining consistency and confdentiality requirements in frst-order databases", *Proceedings of International Conference ISC* 2009, pp. 121-134, 2009.
[12]. R. Sandhu, F. Chen, "Te multilevel relational (MLR) data model", *ACM Transactions on Information and System Security,* no. 1 (1), pp. 93-132, 1998.
[13]. N. Jukic, S. V. Vrbsky, A. Parrish, B. Dixon, B Jukic, "A belief-consistent multilevel secure relational data model", *Information Systems,* no. 24 (5), pp. 377-402.
[14]. P. Chen, L. Wang, "The Multilevel Relational Data Model Based on Trust-label Semantics", *Journal of Computational Information Systems,* no. 11, pp. 3949-3956, 2015.
[15]. S.Jajodia, C. Meadows, "Inference Problems in Multilevel Secure Database Management Systems", *DRAFT, The MITRE Corporation, McLean*, june 1992.
[16]. V. Atluri, S. Jajodia, E. Bertino, "Transaction processing in multilevel secure databases with kernelized architecture: Challenges and solutions", *IEEE Transactions on Knowledge and Data Engineering,* no. 9 (5), pp. 697-708, 1997.

МОДЕЛІ БАГАТОРІВНЕВОЇ БЕЗПЕКИ БАЗ ДАНИХ

Багаторівнева безпека - це політика безпеки, яка дозволяє класифікувати об'єкти і користувачів на основі системи ієрархічних рівнів безпеки і використовувати таку класифікацію для організації системи управління доступом. В реляційних базах даних з багаторівневою безпекою будь-якому читаючому або оновлюючому дані в таблиці користувачеві, має бути дозволено обробляти тільки ті рядки, які дозволяє його рівень доступу, представлений міткою безпеки. Для кожного рядка таблиці (або атрибута рядка) встановлюється рівень конфіденційності шляхом присвоєння мітки безпеки. Користувач може читати або змінювати рядок, тільки якщо його мітка домінує над міткою рядка. Ця вимога призводить до того, що один і той же об'єкт предметної області може бути представлений в таблиці декількома записами, кожна з яких, доступна тільки користувачам з відповідною міткою безпеки (властивість багатозначності відносин). У свою чергу, фундаментальні принципи побудови реляційних баз даних вимагають унікальності кожного кортежу відносини. Спосіб вирішення цієї суперечності визначається моделлю безпеки, що використовується. Крім цього, багатозначність відносин призводить до появи вразливостей в вигляді прихованих каналів (covert channels), отримання інформації шляхом логічних висновків (inference channels), семантичної двозначності (semantic ambiguity) та інших. Як спрямовуюча сила досліджень в області безпеки баз даних технологія багаторівневої безпечної бази даних розвивається стрімко. На основі моделі Белл-Лападула було розроблено багато моделей багаторівневої безпеки в РСУБД, таких як модель SeaView, модель Jajodia-Sandhu, модель Smith-Winslett і інші, які вирішували повністю або частково виникаючі проблеми у вигляді прихованих каналів, семантичної двозначності та інших. Однак на сьогоднішній день не запропоновано вирішення або моделі, вільного від недоліків. Мета роботи: аналіз моделей багаторівневої безпеки, визначення їх переваг та недоліків.

Ключові слова: база даних, захист даних, контроль доступу, багаторівнева безпека, моделі багаторівневої безпеки.

MODELS OF MULTILEVEL DATABASES SECURITY

Multilevel security - is a security policy that allows to classify objects and users based on a system of hierarchical security levels and use this classification to organize an access control system. In relational data bases with multi-level security, any user reading or updating data in a table should be allowed to process only those lines that allow its access level represented by the security label. For each row in the table (or row attribute), the privacy level is set by assigning a security label. The user can read or modify the row only if its label dominates over the label of the row. This requirement leads to the fact thatthe same domain object can be represented in the table by several records, each accessible only to users with the corresponding security label (the property of multi-valued relations). Whereas the fundamental principles of relational databases building require the uniqueness of each tuple relationship. The way to resolve this contradiction is determined by the security model used. In addition, the multi-valued relationship leads to the emergence of vulnerabilities in the form of hidden channels (covert channels), obtaining information through inference channels, semantic ambiguity and others. As an investigation direction in the field of database security, the technology of a multilevel secure database is developing rapidly. Many models of multilevel security in RDBMSs have been developed based on the Bell-Lapadul model, such as the SeaView model, the Jajodia-Sandhu model, the Smith-Winslett model and others that would completely or partially solve arising problems like hidden channels, semantic ambiguity, and others. However, no flawless solution or model has been proposed to date. Objective: SeaView, Jajodia-Sandhu, Smith-Winslett models analysis, identification of their advantages and disadvantages.

Keywords: database, data protection, access control, multilevel security, multilevel security models.

Коломиец Михайло Володимирович, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: box144.85@gmail.com.
Коломыцев Михаил Владимирович, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».
Kolomytsev Myhailo, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Носок Світлана Олександрівна, кандидат технічних наук, доцент Фізико-технічного інституту НТУУ «КПІ».
E-mail: nos.sv.ol@gmail.com.
Носок Светлана Александровна, кандидат технических наук, доцент Физико-технического института НТУУ «КПИ».
Nosok Svitlana, candidate of technical sciences, associate professor of Institute of Physics and Technologies of the NTUU "KPI".

Мазуренко Анастасія Євгенівна, студентка Фізико-технічного інституту НТУУ «КПІ».
E-mail: 061071ks@gmail.com.
Мазуренко Анастасия Евгениевна, студентка Физико-технического института НТУУ «КПИ».
Mazurenko Anastasiia, student of the Institute of Physics and Technologies of the NTUU "KPI".