DOI: 10.18698/0236-3933-2016-2-125-137

УДК 621.396.9

# ОСНОВНЫЕ НАПРАВЛЕНИЯ РАСШИРЕНИЯ МОДЕЛИ ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**В.М. Сычев**

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: zi@bmstu.ru; dviu@mail.ru

*Рассмотрены недостатки концептуальной и логической интерпретаций модели внутреннего нарушителя в терминах "сущность–связь" и реляционной организации данных. Показано, что исследуемая предметная область по определению является динамичной. Процесс адаптации такой темпоральной базы данных к новым условиям ведет к необходимости перекачки данных и требует добавления новых объектов поверх старых с сохранением истории изменения темпоральных данных. При этом возможно увеличение избыточности хранения информации, рост базовой реляционной модели, усложнение составления и выполнения запросов. Предложен способ расширения модели внутреннего нарушителя информационной безопасности (инсайдера) за счет введения атрибута времени, для чего привлечен аппарат темпоральных баз данных.*

***Ключевые слова*:** информационная безопасность, инсайдер, модель нарушителя, темпоральность, классификация, анализ данных.

# THE MAIN DIRECTIONS OF EXPANDING THE INSIDER INFORMATION SECURITY MODEL

**V.M. Sychev**

Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: zi@bmstu.ru; dviu@mail.ru

*The article examines the shortcomings of the conceptual and logical interpretation of the insider model in terms of "entity–relationship" and relational data organization. The study shows, that the tested subject area is dynamic, by definition. The process of adapting a temporal database to the new environment makes it necessary to transfer the data and requires the new facilities over the old ones with the preservation of history changes of the temporal data. It is possible to increase the data storage redundancy, increase the basic relational model, and drawing up and executing queries can become more complex. As a result, we propose a method for expanding the model insider information security (insider) by introducing a time attribute, for that purpose we use a certain number of temporal databases.*

***Keywords*:** information security, insider, intruder model, temporality, classification, data mining.

Современные теория и практика обеспечения информационной безопасности (ИБ) оперируют понятием *нарушитель информационной безопасности*, под которым обычно понимают физическое лицо, умышленно или неумышленно реализующее угрозы ИБ организации.

В [1] предложена семантическая *модель внутреннего нарушителя* ИБ (инсайдера) — комплексная характеристика конкретного сотрудника, отражающая его функционально-должностной статус в организации, а также объективно существующую подготовленность к совершению нарушения (квалификация, оснащенность, осведомленность), возможное психологическое состояние, социологические и иные факторы, значимые для совершения нарушения. Модель может быть использована для мониторинга (оценки) *инсайдерского состояния* персонала организации [2] в целях профилактики реализации внутренних угроз безопасности. (Следует отметить, что в современных условиях профилактика внутренних угроз является актуальной задачей обеспечения безопасности организации в широком смысле. Трагическим примером недооценки ее актуальности, точнее недостаточно эффективной системы выявления инсайдерских состояний персонала, является крушение самолета компании Germanwings, ставшее способом суицида второго пилота Лубица [3, 4].) Для концептуальной и логической интерпретации модели внутреннего нарушителя ИБ использованы соответственно представление характеристик нарушителя в терминах "сущность–связь" (Entity Relationship) и реляционная организация данных.

При таком подходе модель внутреннего нарушителя ИБ может рассматриваться как один из компонентов традиционной модели данных, а именно: как логическая структура (модель) данных (*DS*). В классической теории баз данных модель данных дополняется набором операций (*OP*) над данными и ограничениями целостности (*C*) [5, 6,]:

$$M = (DS, OP, C). \qquad (1)$$

Эта модель отражает единственное (текущее) состояние предметной области, которое считается истинным. Соответственно, в базах данных, реализующих модель (1), хранятся текущие значения атрибутов модели. При изменениях состояния предметной области, происходящих в результате различных событий в объективном мире, значения атрибутов модели (1) заменяются новыми без фиксации времени изменения (события) и сохранения предшествующих значений. (Отметим, что в реальных СУБД обычно фиксируется системное (трансакционное) время изменения значений атрибутов.)

Таким образом, эта модель, которую иногда называют *снимок данных* (данных, зафиксированных в определенный момент времени — в момент события) [7], не предусматривает хранения истории изменений, что ограничивает ее практическое применение в исследуемой предметной области, поскольку мониторинг инсайдерского состояния персонала принципиально основывается на сравнениях данных *DS* во времени. Дело в том, что для решения задачи профилактики инсайдерской угрозы необходим анализ как текущих, так и исторических

предметных данных. Исторические предметные данные отражают инсайдерское состояние потенциального нарушителя в определенный момент времени и используются для сравнения, выявления трендов и прогноза инсайдерского поведения. Это обусловливает необходимость хранения прошлых состояний (истории) баз данных, т.е. осуществлять привязку данных ко времени. Поэтому в модель внутреннего нарушителя ИБ в качестве одного из атрибутов следует ввести время.

Известно, что время представляет собой непрерывную физическую величину, формально представляемую выражением

$$\forall t_1, t_2,\ t_1 < t_2,\ \exists t_3 : t_1 < t_3 < t_2. \tag{2}$$

Выражение (2) имеет следующую семантику: между любыми двумя временны́ми точками существует еще одна временна́я точка [8].

Однако аппаратные средства современной вычислительной техники, поддерживающие базы данных, работают с дискретным временем:

$$\forall t_1, t_2,\ \text{если } t_2 = \delta(t_1),\ \text{то не } \exists t_3 : t_1 < t_3 < t_2, \tag{3}$$

где $\delta$ — функция поиска следующего момента времени.

Семантика выражения (3): между точкой на оси времени и следующей за ней точкой других временны́х точек не существует [8]. При этом наименьшей неразложимой временно́й единицей на временно́й оси (*квантом времени*) для исследуемой предметной области являются сутки. Тогда для отражения временных характеристик в моделях данных внутреннего нарушителя ИБ в соответствии с [9] можно использовать:

— момент времени, соответствующий точке на оси времени, в которой произошло какое-либо событие, например, с учетом введенного кванта времени 1 августа YYYY года);

— период времени — конкретный отрезок времени, имеющий начальный момент времени $t_1$ и конечный $t_2$ момент времени, например, с 23 апреля YYYY года по 1 августа YYYY года;

— интервал времени — длительность временно́го отрезка, например 5 лет.

(В естественной языковой модели внутреннего нарушителя ИБ могут присутствовать описания интервалов времени (например, “2 года состоял на учете ...”). Интервальное время можно отражать, вводя в модель атрибут “Длительность”, который, строго говоря (с точки зрения теории баз данных), не является временны́м атрибутом (текстовое / числовое поле). Поэтому интервалы времени в смысле [9] в данном контексте далее не рассматриваются.) Это позволит рассматривать такую модель как отражение инсайдерского состояния сотрудников, а каждую запись — как некоторый факт, который является истинным в определенный момент или период времени.

Для этого в модели внутреннего нарушителя должны быть установлены связи между значениями данных и значениями времени. При этом значения данных могут меняться, что означает изменение истинности факта в определенные моменты времени.

В современных информационных технологиях отмеченная временна́я связь нашла отражение в понятии *темпоральные данные* (т.е. связаные с определенными датами или промежутками времени [10, 11]). В общем случае темпоральность данных *DS* предполагает определенную модификацию остальных компонент (1). Формально это может быть представлено записью (темпоральная модель данных)

$$M^t = (DS^t, OP^t, C^t). \tag{4}$$

Как указывается в публикациях, посвященных темпоральным данным, выражение (4) означает, что кроме адаптации структуры данных (для представления и хранения темпоральных данных) должны быть переопределены алгебра, операции модификаций и семантика темпоральных ограничений. Однако в настоящей статье предполагается сосредоточение внимания на темпоральных расширениях реляционной структуры данных модели внутреннего нарушителя ИБ.

Рассмотрим применимость введенных временных атрибутов — момента и периода для темпорального расширения логической модели данных внутреннего нарушителя ИБ.

Для привязки данных о наступлении событий к определенным моментам времени можно использовать *событийную модель*, в которой время учитывается в виде временны́х меток изменения значений атрибутов. Это точечное представление времени по [11]. Соответствующие отношения в [7] называют *таблицами событий*. В этом случае предполагается, что данные являются истинными только в заданный момент времени, т.е. в момент времени совершения события.

Событийная (реляционная) модель формально может быть представлена выражением

$$R = (A_1, A_2, \ldots, A_n, V), \tag{5}$$

где $R$ — темпоральное отношение; $A_1, \ldots, A_n$ — набор предметных атрибутов; $V$ — временно́й атрибут типа “Дата”.

При разработке модели внутреннего нарушителя ИБ событийная модель не является доминирующей. Она может быть использована для представления регулярных транзакций, например, для описания таких характеристик субъекта мониторинга, как проведение системным администратором регламентных работ на автоматизированной информационной системе (табл. 1).

Таблица 1

**Событийная модель представления исторических данных**

| Подразделение | Аппаратное/программное средство | Вид работы | Основание | Плановая дата проведения | Фактическая дата проведения |
|---|---|---|---|---|---|
| A | ПЭВМ YYYY | Дефрагментация диска | План | xxxx.02.01. | xxxx.02.01. |
| C | ПЭВМ ZZZZ | Инсталляция ППО | Вне плана | — | xxxx.02.13 |
| B | ПЭВМ XXXX | Проверка наличия вредоносного ПО | Заявка подразделения | xxxx.03.07 | xxxx.03.07 |

Инсайдерским признаком в данном примере может быть нарушение регламента проведения работ.

Эта модель может также быть использована для представления событий, носящих иногда разовый и случайный характер, например, повышение квалификации работника или первичное обращение к врачу за психиатрической помощью. Не является ли это изменением статуса? Если мы рассматриваем статус как кортеж атрибутов, то любое событие — изменение атрибута — изменение статуса. Таким образом, можно считать, что статус — это точка в $n$-мерном пространстве.

Система, реализующая событийную модель, должна хранить исторические данные, отражающие значения набора атрибутов (факторов), которые определяют инсайдерское состояние сотрудника на некоторый фиксированный момент времени и обновляются (добавляются) не в реальном масштабе времени или периодически (ежедневно, еженедельно и т.д.), а, вероятнее всего, по мере поступления данных. При этом должна быть обеспечена *инвариантность предметных данных* во времени. Для этого в ключи таблиц может быть введен атрибут “Время” — в терминах баз данных атрибут “DATE” с форматом “YYYY-MM-DD”.

Очевидно, что в объективном мире каждому факту, ассоциированному с субъектом мониторинга, можно поставить в соответствие промежуток времени, в течение которого факт является истинным. Поэтому в модели данных должны поддерживаться *периоды* времени, в течение которых данные являются *актуальными*, или, правильнее, *истинными*.

Подобное представление времени, когда с данными связывается период времени их истинности, называется *модельным*, или *действительным* (valid) *временем* [9–11]. Нетрудно видеть, что действительное время однозначно отражает определенное *состояние* (*статус*) объекта

моделирования, под которым в данном контексте следует понимать инсайдерское состояние сотрудников предприятия. Таким образом, *статусная модель* может использоваться для моделирования состояния (поведения, динамики) объектов во времени [8]. В этом случае предполагается, что данные являются истинными в течение некоторого периода времени, начало и окончание которого может обозначаться, соответственно, атрибутами $V_s$ ($s$ — start) и $V_e$ ($e$ — end) типа "Дата".

В некоторых источниках данный подход называется *интервальным представлением* времени [11], а соответствующие отношения — *таблицами состояний* [8].

Статусная модель интервального представления формально может быть представлена выражением

$$R_t = (A_1, A_2, \ldots, A_n, V_s, V_e). \tag{6}$$

Таким образом, темпоральные модели данных позволяют хранить информацию об эволюции инсайдерского состояния: для любого сотрудника, который был принят на должность в момент времени $v_1$ и уволен/снят с учета в момент времени $v_2$, в базах данных могут быть сохранены все его характеристики на временно́м интервале $[v_1, v_2]$.

**Битемпоральная модель данных.** При мониторинге и последующем анализе инсайдерского состояния сотрудников могут оказаться полезными сведения не только о действительном времени, но и сведения о моменте выявления и фиксации предметных данных в базах данных. Такое время называется *транзакционным* [10, 12]. Будем обозначать это время $T(T_{start})$. Тогда, например, "Время (период) нахождения сотрудника за границей — 2015.02.01–2015.03.15" — действительное время, а "Дата внесение данных в базу данных — 2015.05.19" — транзакционное время. Транзакционное время можно моделировать атрибутом "TIMESTAMP".

При оперировании как модельным, так и транзакционным временем, обычно говорят о *битемпоральной* модели данных. (В работе [11] отмечается, что возможны иные подходы к моделированию времени, но все они могут быть сведены к одному из рассмотренных типов, возможно, через дополнительные отношения.)

Следует отметить, что в транзакционное время обычно включают и моменты удаления данных из баз данных, $T_e(T_{end})$.

Поддержка битемпорального времени позволяет реализовать "откаты" — исправления некорректных данных с фиксацией времени изменений в базе данных. При обновлении предметных данных в битемпоральной системе интервал транзакционного времени также обновляется, создавая список изменений.

Однако, как представляется, в исследуемой задаче для обеспечения неизменности данных и поддержки хронологии в модели "рабочим"

атрибутом должна быть только “Дата ввода” (TIMESTAMP). Операторы удаления $T_e$ — технологические и используются для исправления ошибок и полного удаления данных.

Таким образом, временны́е метки действительного времени хранят информацию об изменении некоторых параметров моделируемого инсайдерского состояния сотрудников, а метки транзакционного времени предоставляют информацию о времени изменения данных или исправления ошибок.

Введение временны́х характеристик в модель внутреннего нарушителя ИБ, разработанную на основе реляционного подхода к организации данных, можно рассматривать как ее темпоральное расширение. Это наиболее используемый метод представления временны́х данных (другие методы представления временны́х данных, см., например, [10]), поскольку реляционная модель данных предоставляет широкие возможности хранения и обработки данных, представления результатов запросов; тривиально расширяется путем введения соответствующих темпоральных характеристик (атрибутов).

В настоящее время известно два подхода к темпоральному расширению: “кортежный” — на уровне кортежа; “атрибутный” — на уровне отдельных атрибутов.

Кратко рассмотрим [10, 12] эти подходы и проведем анализ возможности их применения в исследуемой предметной области (обозначения элементов кортежей приведены по первоисточникам).

1. В “кортежной” модели представления темпоральных данных, предложенной Р. Снодграсом, битемпоральное отношение $R$ представляется следующей записью:

$$R = (A_1, \ldots, A_n, V_s, V_e, T_s, T_e), \tag{7}$$

где $A = \{A_1, \ldots, A_n\}$ — набор предметных атрибутов; $V_s, V_e, T_s, T_e$ — темпоральные атрибуты времени, содержащие дату начала и окончания соответственно действительного и транзакционного времени.

Развернутая семантика темпоральных атрибутов заключается в следующем: $V_s, V_e$ — временно́й период актуального состояния предметных атрибутов $A_1, \ldots, A_n$. Если $V_e$ не определено, то состояние актуальное, текущее; $T_s$ — момент включения данных (запись) в базу данных; $T_e$ — исключение данных (записи). Если $T_e$ не определено, *null* (в нашем случае, как правило), то кортеж хранится. Если $T_e$ определено, то кортеж удаляется.

В соответствии с [10, 12] выражение (7) является естественным и наиболее часто используемым способом представления битемпоральных отношений. Рассмотрим возможность применения модели Снодграса для мониторинга инсайдерских состояний. Предполагается, что изменение текущего значения любого (одного, нескольких или всех

предметных) из атрибутов $A_i \to A_i^+$ происходит в действительном времени и означает изменение $V_e \to V_s^+$. Эти изменения, в свою очередь, должны вести к изменению транзакционного времени $T_e \to T_s^+$, т.е. в базе данных меняется весь кортеж (7). При этом, исходя из формального прочтения выражения (7), наличие $T_e$ предполагает штатную операцию удаления записей из базы данных, т.е. возможны два варианта:

- $T_s \to T_e$, $T_s^+$ — кортеж $A_i$ удаляется, появляется новая запись $A_i^+$, соответствующая $V_s^+$;
- $T_s \to T_e$ (null), $T_s^+$ — кортеж $A_i$ не удаляется, появляется новая запись $A_i^+$, соответствующая $V_s^+$, т.е. поддерживается ведение истории изменений $A$ (общая схема приведена далее):

$$\begin{array}{ccccc} A_i & \to & A_i^+ & & \\ \downarrow & & \downarrow & & \\ V(A_i)_s & \to & V(A_i)_l & \to & V(A_i^+)_{z+} \\ \downarrow & & \downarrow & & \downarrow \\ T(A_i)_j & \to & T(A_i)_i & \to & T(A_i^+)_{z+} \end{array}$$

Первый вариант ведения транзакционного времени (наличие $T_e$) означает формальное соответствие (7), но невозможность ведения истории, что исключает мониторинг инсайдерских состояний сотрудников.

Второй вариант ведения транзакционного времени ($T_e$ не определяется, *null*) означает, что в базе данных накапливается множество записей, не соответствующих формальной модели, а ведение истории обеспечивается не моделью данных, а специальными решениями разработчиков приложения (компонент пол *OP* в (1)). Это означает необходимость поиска других решений.

Очевидно, что применение модели (7) в исследуемой задаче возможно по второму (не штатному) варианту модификации $T_e$. В этом случае атрибут $T_e$ может быть применен только для удаления записи / кортежа, например, при увольнении сотрудника. Данная идея нашла отражение в модели К. Дженсена.

2. В модели представления темпоральных данных, предложенной К. Дженсеном, историчные кортежи не обновляются. В терминах баз данных это означает режим доступности данных только для чтения. Поэтому эта модель может быть применена для создания архива инсайдерских состояний, ассоциированных с временем. Формально по К. Дженсену битемпоральное отношение $R$ может быть представлено в виде

$$R = (A, V_s, V_e, T, O_p), \tag{8}$$

где $A = \{A_1, \ldots, A_n\}$ — набор предметных атрибутов; $V_s, V_e$ — атрибуты, обозначающие период (даты начала и окончания) актуальности

предметных данных; $T$ — атрибут времени фиксации кортежа (внесения в журнал изменений); $O_p$ — атрибут, отражающий запросы на создание и удаление кортежей соответственно символами — $I$ (*Insert*) и $D$ (*Delete*). Эта пара запросов формируется с одинаковым временны́м атрибутом $T$.

В общем случае в этой модели модификация данных допускается как исключение, например, для исправления ошибочных записей. Однако при моделировании инсайдерского состояния сотрудника ошибочность (неточность) данных весьма вероятна (норма). Поэтому процедура их исправления (модификации) также является штатной.

Исходя из возможности хранения исторических данных, модель К. Дженсена представляется весьма перспективной для создания темпоральных баз данных в исследуемой области.

3. В модели С. Гадии битемпоральные метки устанавливаются для каждого атрибута кортежа. Тогда формально битемпоральное отношение можно представить кортежем из $n$ элементов:

$$R = (\{([V_s, V_e]\,[T_s, T_e]A_1)\}, \ldots, \{([V_s, V_e]\,[T_s, T_e]A_n)\}). \qquad (9)$$

В (9) каждый элемент представляет собой тройку значений: действительное время [$V_s$, $V_e$], транзакционное время [$T_s, T_e$] и значение атрибута $A_i$.

В части представления транзакционного времени к данной модели можно отнести замечания и выводы по модели Снодграса. Тем не менее, идея связывания темпоральных атрибутов с предметными атрибутами представляет интерес, поскольку обеспечивает большие возможности, позволяет исследовать отдельные (событийные) аспекты личности, поведения и статуса субъекта мониторинга. Еще одним аргументом в пользу “атрибутной” темпоральной модели является необходимость работы с реляционной базой данных с изменяемой структурой (см. далее), множественность источников интерпретации одного факта и необходимость формирования агрегатных состояний.

4. “Атрибутная” модель, предложенная Дж. Бен-Зви, включает в битемпоральное отношение $R$ ранее определенный набор атрибутов $(A_1, \ldots, A_n, T)$. Расширенная запись отношения следующая:

$$R = (A_1, \ldots, A_n, T_{es}, T_{rs}, T_{ee}, T_{re}, T_d), \qquad (10)$$

где $T_{es}$ — время актуализации атрибута кортежа; $T_{rs}$ — время фиксации значения $T_{es}$ в базе данных; $T_{re}$ — время утраты актуальности факта моделируемой области; $T_{ee}$ — время фиксации значения $T_{re}$ в хранилище (базе данных); $T_d$ — время логического удаления записи из базы данных.

Данная модель позволяет хранить исторические данные, обеспечивая возможность их удаления (атрибут $T_d$).

Представляется, что модель Дж. Бен-Зви наиболее полно соответствует предметным особенностям работы с инсайдерскими данными сотрудников. Поэтому ее можно рассматривать в качестве основы при построении темпоральной базы данных инсайдерских состояний.

**Версионное расширение темпоральной модели.** В исследуемой предметной области (мониторинг инсайдерских состояний) важной для моделирования спецификой является множественность источников данных, одномоментно формирующих значения предметных атрибутов $A$, и, соответственно, истинных по версии источника значений атрибутов модели. Например, для моделирования сущности $S_i$ "Девиантное поведение сотрудника" могут использоваться атрибуты: $A_i^1, A_i^2, A_i^3, A_i^4$ и др.

В табл. 2 приведен пример значений этих атрибутов, полученных из различных источников.

Таблица 2

**Пример многозначности атрибутов по различным источникам данных**

| | Предметные атрибуты | | | | Темпоральные атрибуты | | | |
|---|---|---|---|---|---|---|---|---|
| Источник ($I^q$) | $A_i^1$ | $A_i^3$ | $A_i^3$ | $A_i^4$ | $V_s$ | $V_e$ | $T_s$ | $T_e$ |
| Автобиография ($I^1$) | 1 | – | – | – | – | – | – | – |
| Служебная проверка ($I^2$) | 1 | 1 | – | – | – | – | – | – |
| Заявление коллеги ($I^3$) | – | – | 1 | – | – | – | – | – |
| Иной ($I^4$) | – | – | 0 | 1 | – | – | – | – |

Значения атрибутов: (1) — "истина", (0) "ложь", (–) — "не определено", т.е. неизвестно.

Из табл. 2 следует, что значения атрибута $A_i^3$ по версиям источников $I^3$ и $I^4$ противоречат друг другу.

Отмеченная особенность может быть учтена в модели отношений: $R = (R^q, T^q)$, где $R^q$ — отношение и $T^q$ — темпоральный атрибут по версии источника $I^q$ $q = \{1, \dots w\}$. Развернутая запись:

$R^1 = (A_1, \dots, A_n, V_s, V_e, T_s, T_e, I^1)$ (по версии источника $I^1$);

. . . . . .

$R^q = (A_1, \dots, A_n, V_s, V_e, T_s, T_e, I^q)$ (по версии источника $I^q$);

. . . . . .

$R^w = (A_1, \dots, A_n, V_s, V_e, T_s, T_e, I_w)$ (по версии источника $I^w$).

Очевидно, что множественность источников противоречивых актуальных данных (записей в базе данных) создает трудности при обработке запросов. Возможным решением этой проблемы является формирование нечетких агрегатов — сущностей в семантической модели

внутреннего нарушителя, представляющих некую обобщенную инсайдерскую характеристику нарушителя [13].

В заключение следует отметить, что исследуемая предметная область по определению является динамичной, т.е. имеющей изменяемую во времени структуру *DS*. Процесс адаптации такой темпоральной базы данных к новым условиям ведет к необходимости перекачки данных и требует добавления новых объектов поверх старых с сохранением истории изменения темпоральных данных. При этом возможно увеличение избыточности хранения информации, рост базовой реляционной модели, усложнение составления и выполнения запросов [14].

Начало данному направлению исследований положено в [14]. Однако моделирование такой структуры продолжает оставаться нетривиальной задачей, которая требует специальных исследований, направленных на развитие предложенной модели внутреннего нарушителя ИБ.

## ЛИТЕРАТУРА


1. *Карпычев В.Ю.*, *Сычев В.М.*, *Минин Ю.В.* Новые подходы к моделированию внутреннего нарушителя информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2013. № 7. С. 32–39.
2. *Сычев В.М.* Формализация модели внутреннего нарушителя информационной безопасности // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2015. № 2. С. 92–106. DOI: 10.18698/0236-3933-2015-2-92-106
3. *Что известно* об Андреасе Лубице, который управлял разбившимся Airbus A320? [Электронный ресурс], 2015. URL: http://www.aif.ru/dontknows/file/Andreas_Lubittc_dosie 27.03.15 (дата обращения 25.06.2015).
4. *Самоубийство* пилота Germanwings — не первый случай // Портал Иносми, 2015. URL: http://inosmi.ru/world/20150327/227156413.html#ixzz3fBpWJTlu (дата обращения 25.06.2015).
5. *Гарсиа–Молина Г.*, *Ульман Дж.*, *Уидом Дж.* Системы баз данных. Полный курс. М.: Вильямс, 2003. 1088 с.
6. *Дейт К.* Введение в системы баз данных. М.: Вильямс, 2006. 1328 с.
7. *Лисянский К.* Архитектурные решения и моделирование данных для хранилищ и витрин данных. 2015. URL: http://www.olap.ru/basic/diasoft1.asp (дата обращения 25.06.2015).
8. *Балдин А.В.*, *Елисеев Д.В.*, *Агаян К.Г.* Обзор способов построения темпоральных систем на основе реляционной базы данных // Наука и образование. МГТУ им. Н.Э. Баумана. 2012. № 8. С. 309–316. URL: http://technomag.edu.ru/doc/441884.html DOI: 10.7463/0812.0441884
9. *Snodgrass R.* Developing Time-Oriented Database Applications in SQL. Morgan Kaufmann Publishers, 1999.
10. *Базаркин А.Н.* Разработка темпоральной модели данных в медицинской информационной системе // Программные продукты и системы. 2009. № 2.
11. *Костенко Б.Б.*, *Кузнецов С.Д.* История и актуальные проблемы темпоральных баз данных. 2007. URL: http://citforum.ru/database/articles/temporal/l (дата обращения 25.05.2015).

12. *Christian S. Jensen.* Temporal Database Management. Aalborg University, 2000. 1323 с. URL: http://people.cs.aau.dk/ csj/Thesis/ (дата обращения 01.08.2015).
13. *Карпычев В.Ю.*, *Сычев В.М.* Применение байесовых сетей в задачах анализа внутренних угроз информационной безопасности // Вестник Воронежского института МВД России. 2015. № 1. С. 12–19.
14. *Елисеев Д.В.* Методика обработки темпоральной реляционной базы данных в миварном пространстве. Автореф. дисс. . . . канд. техн. наук. М.: МГТУ им. Н.Э. Баумана, 2011. 149 с.

## REFERENCES

[1] Karpychev V.Yu., Sychev V.M., Minin Yu.V. New approaches to the modeling of insider information security. *Pribory i sistemy. Upravlenie, kontrol', diagnostika instruments and systems* [Management, monitoring, diagnostics], 2013, no. 7, pp. 32–39 (in Russ.).
[2] Sychev V.M. The formalization of models insider information security. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2015, no. 2, pp. 92–106 (in Russ.). DOI: 10.18698/0236-3933-2015-2-92-106
[3] What is known about Andreas Lubits who ruled crashed Airbus A320? Available at: http://www.aif.ru/dontknows/file/Andreas_Lubittc_dosie 27.03.15 (accessed 06.25.2015).
[4] Suicide pilot Germanwings — not the first time. Inosmi, 2015. Available at: http://inosmi.ru/world/20150327/227156413.html# ixzz3fBpWJTlu (accessed 06.25.2015).
[5] Garcia-Molina G., Ullman J., Widom J. Database systems. The Complete Book. Pearson Prentice-Hall. Pearson Education Inc., 2002.
[6] Date K. An Introduction to Database Systems. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 2003.
[7] Lisyansky K. Architectural solutions and modeling of data warehouse and data marts. Available at: http://www.olap.ru/basic/diasoft1.asp (accessed 06.25.2015).
[8] Baldin A.V., Eliseev D.V., Aghayan K.G. Overview of methods of creating systems based on temporal relational database. *Nauka i obrazovanie. MGTU im. N.E. Baumana* [Science & Education of the Bauman MSTU. Electronic Journal], 2012, no. 8. Availlable at: http://technomag.bmstu.ru/en/doc/441884.html DOI: 10.7463/0812.0441884
[9] Snodgrass R. Developing Time-Oriented Database Applications in SQL. Morgan Kaufmann Publishers, 1999.
[10] Bazarkin A.N. The development of temporal data model in the medical information system. *Programmnye produkty i sistemy* [Software products and systems], 2009, no. 2 (in Russ.).
[11] Kostenko B.B., Kuznetsov S.D. The history and current problems of temporal databases. Available at: http://citforum.ru/database/articles/temporal/1 (accessed 05.25.2015).
[12] Christian S. Jensen Temporal Database Management. Aalborg University, 2000. 1323 p. Available at: http://people.cs.aau.dk/csj/Thesis/ (accessed 01.08.2015).
[13] Karpychev V.Yu., Sychev V.M. The Use of Bayes Networks in Problems of Analysis Internal Threats to Information Security. *Vestnik Voronezhskogo instituta MVD Rossii* [Vestnik of Voronezh Institute of the Ministry of Interior of Russia], 2015, no. 1, pp. 12–19 (in Russ.).

[14] Eliseev D.V. Metodika obrabotki temporal'noy relyatsionnoy bazy dannykh v mivarnom prostranstve. Avtoreferat diss. kand. tekhn. nauk [Methods of treatment of temporal relational database mivarny space. Cand. tech. sci. diss. abstr.]. Moscow, 2011.

Статья поступила в редакцию 29.10.2015

Сычев Владимир Михайлович — ассистент кафедры "Защита информации" МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5).

Sychev V.M. — Assistant Lecturer of Information Security Department, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation).

**Просьба ссылаться на эту статью следующим образом:**

Сычев В.М. Основные направления расширения модели внутреннего нарушителя информационной безопасности // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2016. № 2. С. 125–137. DOI: 10.18698/0236-3933-2016-2-125-137

**Please cite this article in English as:**

Sychev V.M. The main directions of expanding the insider information security model. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2016, no. 2, pp. 125–137. DOI: 10.18698/0236-3933-2016-2-125-137