Анализ моделей информационной безопасности

Э. В. Логин[1], А. И. Новикова[2]

Петербургский государственный университет путей сообщения Императора Александра I

[1]elinabeneta@yandex.ru, [2]an8234016@gmail.com

Аннотация. **Роль информации в современном мире значительно возросла вместе с развитием информационных систем. Между тем, возникла существенная проблема обеспечения ее защиты. Существуют различные модели информационной безопасности, которые позволяют определить текущее состояние информационной безопасности системы или спрогнозировать ее состояние в будущем. В данной статье рассматриваются самые распространённые модели безопасности.**

Ключевые слова: модель информационной безопасности; контроль доступа; целостность данных; конфиденциальность данных

I. Понятие об информационной безопасности

Под термином «информационная безопасность» (ИБ) (данных) понимается состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность, целостность, неотказуемость, где:

- Конфиденциальность – это состояние информационной системы, при котором информационные ресурсы предоставляются только тем пользователям, которые имеют на этот доступ разрешение;
- Доступность – это состояние информационной системы, при котором услуги, которая реализует данная система, могут быть гарантированно предоставлены пользователям, имеющие на это право;
- Целостность – это состояние информационной системы, при котором информация и процедуры ее обработки не могут быть изменены, удалены или дополнены неавторизованным образом.
- Неотказуемость – это состояние информационной системы, при котором обеспечивается невозможность отрицания пользователем, который выполнил какое-то определенное действие, факт их выполнения и/или отрицания пользователем факта отправки или получения информации.

Данный подход к рассмотрению понятия информационной безопасности как совокупность вышеперечисленных определений был предложен Зальцером и Шредером в 1975 году [1]. В русскоязычной литературе, этот метод имеет название: «Триада «конфиденциальность, целостность, доступность» (рис. 1).

Рис. 1. Триада «конфиденциальность, целостность, доступность»

Понятие «неотказуемость» была добавлена чуть позже, поскольку с развитием информационной системы необходимо было также расширить свойства ее безопасности.

Однако, дискуссии о том, какие свойства информационной системы можно считать исчерпывающими для определения ее безопасности, не утихают. Поэтому, существует еще один подход к рассмотрению понятия информационной безопасности: гексада Паркера [2]. Туда было включено еще три определения (рис. 2):

- Аутентичность – это состояния информационной системы, при котором пользователь не может выдать себя за другого.
- Владение – это состояние информационной системы, при котором физический контроль над устройствами или контроль над средой обработки информации предоставляются пользователям, имеющим на это право.
- Полезность – это состояние информационной системы, при котором обеспечивается удобство практического использования информации или процедур, которые связаны с обработкой этой информации.

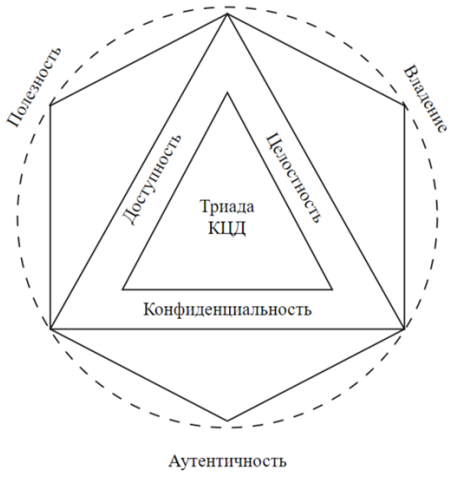

Рис. 2. Гексада Паркера

Именно на основе гексады Паркера было сформулировано полное определение информационной безопасности:

Информационная безопасность – это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации [3].

Далее в статье будут рассмотрены различные математические модели информационной безопасности. Для проведения сравнительного анализа будет использована триада КЦД, поскольку такой подход является самым простым и распространённым.

II. Модели информационной безопасности

Математическая модель информационной безопасности – это модель, которая позволяет определить эффективность использования системы обеспечения безопасности в какой-либо автоматизированной системе.

Для эффективной интеграции различных моделей в систему информационной безопасности, они должны обладать следующими свойствами:

- Универсальность – модель должна быть применима для анализа ряда однотипных систем в различных режимах функционирования.
- Практическая направленность – полученные результаты от этой модели могут быть использованы для анализа и решения ряда проблем информационной безопасности.
- Простота использования – модель отображает только существенные стороны исследуемого объекта.
- Адекватность – модель должна отражать реальные свойства объекта.
- Комплексность – модель должна охватывать и учитывать различные факторы воздействия на информационные ресурсы.

Существуют следующие виды математических моделей информационной защиты:

A. *Модель Белла–ЛаПадула*

Данная модель направлена на предотвращения несанкционированного доступа к секретной информации, гарантируя, что конфиденциальные данные не будут доступны лицам, которые не имеют доступ к этим данным. Такая модель является самой ранней моделью и наиболее популярной. В этой модели каждому объекту и субъекту (пользователю) системы назначается свой уровень допуска. Действуют два основных правила:

- Пользователь может читать только объекты с уровнем допуска не выше его собственного.
- Пользователь может изменять только те объекты, уровень допуска которых не ниже его собственного.

Сама модель представлена на рис. 3.

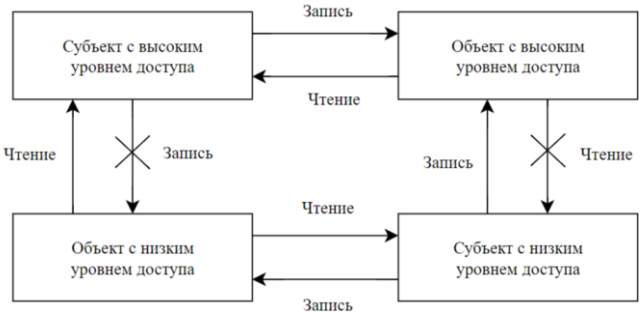

Рис. 3. Модель Белла–ЛаПадула

B. *Модель Биба (или модель целостности Биба)*

В отличие от модели Белла–ЛаПадулы, которая ориентирована на конфиденциальность, модель Бибы предназначена для предотвращения несанкционированного или ненадлежащего изменения данных, тем самым обеспечивая их точность и надёжность. Суть данной модели заключается в том, что субъекты не могут повредить данные на уровне, более высоком, чем уровень субъекта, или быть повреждёнными данными с более низкого уровня, чем уровень субъекта.

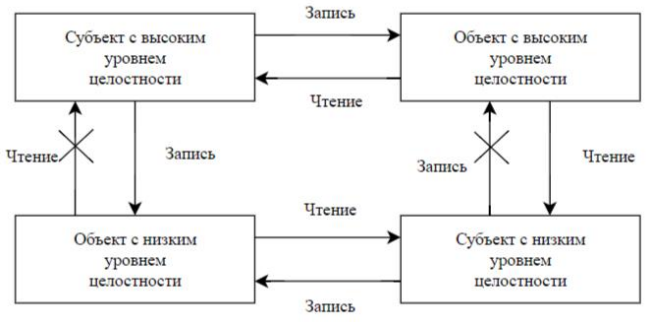

Рис. 4. Модель Биба

C. *Модель Кларка–Уилсона*

Предназначена для обеспечения целостности данных с помощью правильно оформленных транзакций и разделения обязанностей. Эта модель предназначена для предотвращения несанкционированных изменений и обеспечения правильного обращения с данными. Сама

модель основывается на взаимосвязи между аутентифицированным субъектом (т. е. пользователем) и набором программ (т. е. TP), которые работают с набором элементов данных (т. е. UDI и CDI, где CDI – ограниченные элементы данных, UDI – неограниченные элементы данных). Сама модель представлена двумя сводом правил: правила сертификации (C) и правила получения право доступа (E) (рис. 5 и рис. 6) [4].

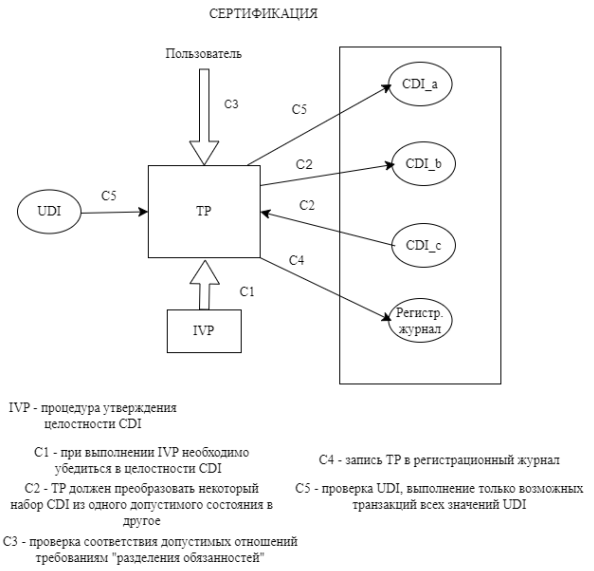

Рис. 5. Модель Кларка–Уилсона (C)

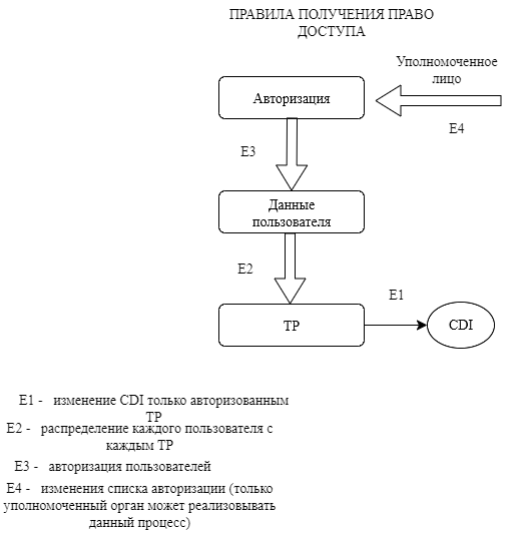

Рис. 6. Модель Кларка–Уилсона (E)

D. Модель Брюера и Нэша (модель «китайской стены»)

Данная модель предназначена для сохранения конфиденциальности, где необходимо контролировать действия пользователей и доступ к данным на основе их прошлых действий. Если пользователь получает доступ к определённым данным, то ему запрещается доступ к связанным с ней или конкурирующим данным, чтобы предотвратить конфликт интересов или нарушение конфиденциальности.

E. Модель Харрисона–Руццо–Уллмана (HRU)

Основной идеей данной модели является ограничение на выполнение определенных операций, которые может реализовывать пользователь (субъект) в отношении объекта. Права доступа реализованы с помощью матрицы доступов. Ее основными компонентами являются:

- Множество субъектов (S)
- Множество объектов (O)
- Множество прав доступа (R) – множество действий, которые субъекты могут совершать над объектами ($R= r_1, r_2,\ldots r_w$)
- Матрица доступа (M) – таблица, в строках которой расположены все субъекты системы, в столбцах – объекты, а в ячейках – соответствующие права доступа.

Пример матрицы доступа представлен в табл. I.

ТАБЛИЦА I.

	O_1	…	O_k	…	O_m
S_1					
… =					
S_k			$r_1, r_2, \ldots r_w$		
… -					
S_n					

Для управления правами доступа в данной модели используется набор из шести операций:

- Создать объект (op=create object o’)
- Удалить объект (op=destroy object o)
- Создать субъект (op=create subject s’)
- Удалить субъект (op=destroy s)
- Добавить право r в ячейку M[s,o] (op=enter r into M[s,o])
- Удалить право r из ячейки M[s,o] (op=delete r fro, M[s,o]).

III. Анализ моделей информационной безопасности

Рассмотрим все вышеперечисленные модели информационной безопасности с точки зрения свойств информационной системы.

Модель Белла–ЛаПадула в основном сосредоточена на обеспечении конфиденциальности информации, в то же время, она не рассматривает свойства целостности и доступа. Исходя из этого, такая модель чаще всего используется в военных и правительственных информационных системах, где конфиденциальность данных имеет огромное значение. Основным недостатком модели Белла–ЛаПадула является тот факт, что для систем, где обмен данными происходит между различными уровнями безопасности, ее применение будет неэффективным.

Противоположностью вышесказанной модели является модель Биба, которая, в свою очередь, сосредоточена на обеспечении целостности данных и препятствии несанкционированного воздействия. Такая модель прекрасно проявит себя в финансовых системах, где целостность данных играет значительную роль. Однако другие свойства информационной системы она не рассматривает.

В свою очередь модель Кларка–Уилсона уже сосредотачивается на двух составляющих информационной безопасности: целостность и доступность. Целостность информации обеспечивается путем правильно оформленных транзакций и разделения обязанностей, а доступность информации возможна только авторизованным пользователям через правила получения право доступа. Однако к недостаткам можно отнести то, что внедрение распределения обязанностей и их последующее согласование является сложным процессом.

Модель Брюева–Нэша обычно используется в информационных системах коммерческих организаций, поскольку она позволяет смягчить конфликт интересов, поскольку информация не может передаваться таким образом, что это способствует появлению конфликта интересов. Данная модель достаточно эффективна при управлении конфиденциальной информацией в конкурентной среде. Однако возникает сложность управления доступом на основе предыдущих действий пользователя.

Последняя модель применяется уже в крупномасштабных системах со сложным требованием к доступу. Модель Харрисона–Руццо–Уллмана обеспечивает целостность данных, путем введения ограничений операций, которые пользователь (субъект) может проводить в отношении объекта, а права доступа реализованы с помощью «матрицы доступа». С помощью такой модели можно гибко управлять доступом в зависимости от конкретных ситуаций. Также она способна адаптироваться при изменении ролей пользователей или системных требований.

IV. Заключение

Модели информационной безопасности являются важным инструментом для понимания состояния системы обеспечения безопасности, а также прогноз ее состояния после введения новых входных данных. Были рассмотрены самые популярные модели информационной безопасности, был проведен их сравнительный анализ.

Если рассматривать вопрос о применении какой-либо модели на железнодорожном транспорте, то следует отдать предпочтение модели Харрисона–Руццо–Уллмана, поскольку вся информационная система ОАО «РЖД» представляет собой сложную структуру, где требуется разграничение доступа к определенной информации между сотрудниками. Поэтому данная модель подойдет лучше всего, поскольку она позволяет гибко управлять и изменять право доступа. Однако модель Харрисона–Руццо–Уллмана не рассматривает вопрос конфиденциальности, что, безусловно, является недостатком данной модели, поскольку защита данных от доступа к ней посторонних лиц также является важным аспектом защиты для информационной системы железнодорожного транспорта. Однако данную модель можно интегрировать, например, с моделью Белла–Лапауды, основная направленность которой является как раз обеспечение конфиденциальности информации.

Список литературы

[1] Jerry H. Saltzer, Mike D. Schroeder «The protection of information in computer systems» [Электронный ресурс] – Режим доступа: https://ieeexplore.ieee.org/document/1451869/metrics#metrics (Дата обращения: 01.03.2025)

[2] Fighting Computer Crime: A New Framework for Protecting Information/ Donn B. Parker – Wiley, 1998. 528 с.

[3] ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Электронный ресурс]. – М.: Национальный стандарт российской федерации. – Режим доступа: http://files.stroyinf.ru/Data1/57/57161/. (Дата обращения 01.03.2025)

[4] Secure Databases: An Analysis of Clark-Wilson Model in a Database Environment/ Xiaocheng Ge, Fiona Polack, Regine Laleau – Department of Computer Science, University of York. 14 с.