ПОДГОТОВКА К CISSP: МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Барабанов Александр Владимирович**, кандидат технических наук, CISSP, CSSLP, г. Москва*

Публикация продолжает серию статей для специалистов по информационной безопасности, готовящихся сдать экзамен на получение статуса CISSP (Certified Information Systems Security Professional) [1–5]. В статье рассмотрены базовые концепции и модели безопасности домена «Архитектура безопасности» («Security Architecture and Design»). Основное внимание уделено моделям разграничения доступом и скрытым каналам.

***Ключевые слова**: сертификация специалистов, CISSP, архитектура безопасности, модели разграничения доступом, скрытый канал.*

GETTING CISSP: INFORMATION SECURITY MODELS

***Aleksandr Barabanov**, Ph.D., CISSP, CSSLP, Moscow*

This publication continues a series of articles for information security specialists, preparing to take the exam for the status CISSP (Certified Information Systems Security Professional) [1–5]. The basic concepts and models Domain Security «Security Architecture and Design» are described. The focus is on models of access control and hidden channels are considered.

***Keywords**: specialists certification, CISSP, Security Architecture, access control model, covert channel.*

Введение

Данная статья является продолжением публикаций, посвященных подготовке к сдаче экзамена по CISSP [1-5], и касающимся домена «Архитектура безопасности» (Security Architecture and Design). Указанный домен описывает базовые архитектурные компоненты (логические, программные, технические) информационной системы и их использование при проектировании систем безопасности информации. Основное внимание в домене уделено следующим темам из области информационной безопасности:

– модели безопасности, используемые при создании систем защиты информации;

– стандарты и критерии, используемые для оценки эффективности систем защиты информации [6,7].

В данной публикации мы основное внимание уделим первой теме.

Понятие модели информационной безопасности

Основное назначение моделей информационной безопасности (ИБ) – обеспечить формализацию политик безопасности. Модель может быть представлена в виде набора правил, которые должны соблюдаться для выполнения установленных положений политики безопасности. Данные правила могут быть представлены как в формальном (с использованием математических и логических выражений), так и в неформальном (на естественном языке) виде. Модели ИБ представляют проектировщикам и разработчикам систем защиты информации возможность проецировать абстрактные положения в политику безопасности, которая будет использоваться при проектировании программного и аппаратного обеспечения. Кроме этого, модели позволяют разработчикам выполнять верификацию систем защиты информации с целью подтверждения корректности реализации политики безопасности.

Введем ряд определений, необходимых для дальнейшего изложения (рис. 1). Под *политикой безопасности* будем понимать совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы. Модель является формальным выражением политики безопасности [7].

Под *объектом доступа* будем понимать единицу информационного ресурса информационной

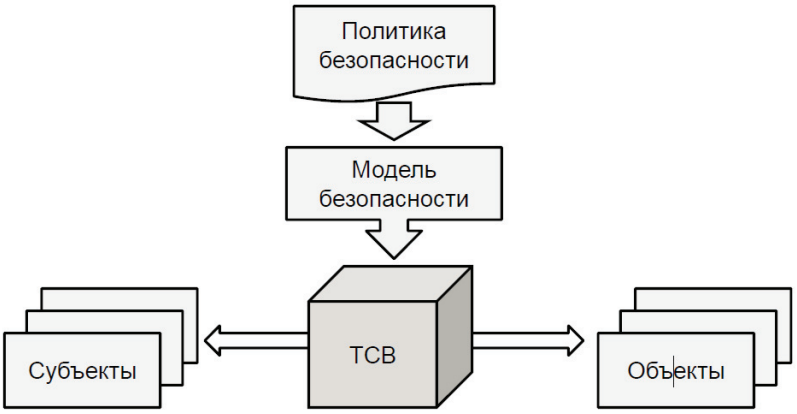

Рис.1. *Связь фундаментальных концепций информационной безопасности*

системы, доступ к которой регламентируется правилами разграничения доступа. Объект доступа является пассивной сущностью, используемой для хранения или получения информации (например, файл, таблица базы данных). *Субъект доступа* - сущность, действие которой регламентируется правилами разграничения доступа. Субъект доступа - активная сущность, которая может инициировать запросы ресурсов и использовать их результаты для выполнения каких-либо вычислительных заданий. Субъекты и объекты доступа могу обладать различными свойствами, которые могут описываться рядом атрибутов (например, классификационная метка, перечень возможностей и т.д.). Под доверенной средой вычислений (Trusted computing base, TCB) будем понимать совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения выполнения политик ИБ. Таким образом, доверенная среда вычислений – подмножество защищаемой информационной системы, обеспечивающее защиту информации и выполнение установленных политик ИБ.

Периметр безопасности (security perimeter) – это воображаемая граница, отделяющая доверенную среду вычислений от остальных частей системы. Все сущности и компоненты, находящиеся внутри периметра безопасности, являются доверенными. Для взаимодействия доверенной среды вычислений и остальной части системы используется доверенный маршрут передачи данных (trusted paths), обеспечивающий необходимую степень уверенности в поддержании установленной политики безопасности (рис. 2).

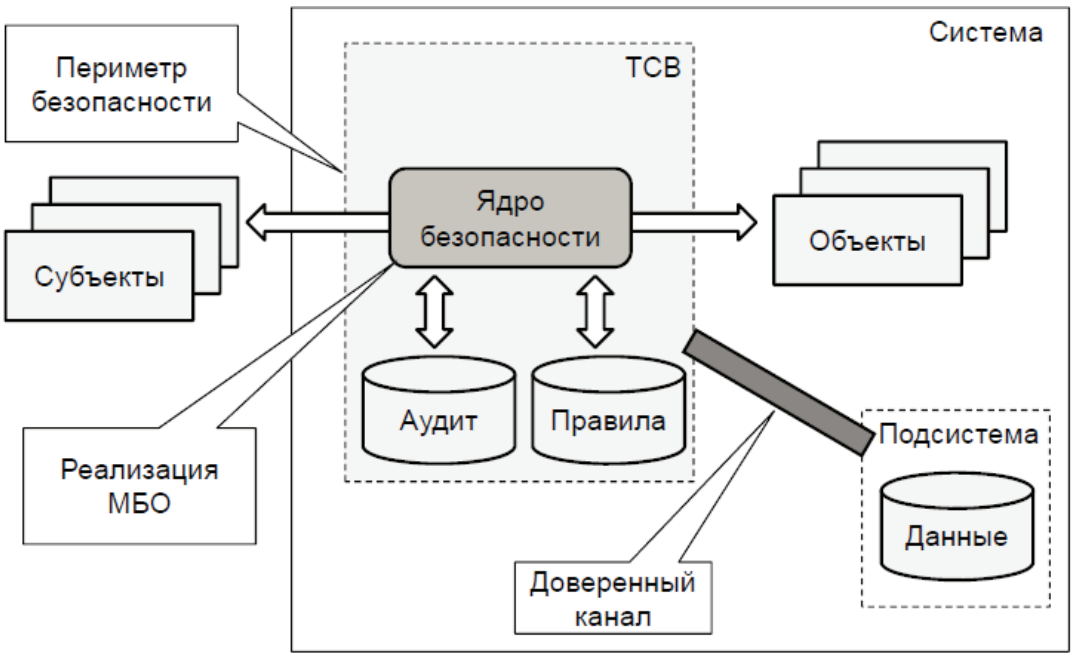

Рис.2. *Связь фундаментальных концепций информационной безопасности*

Когда в системе необходима реализация политик разграничения доступа, в доверенной вычислительной среде целесообразно выделить конечное множество компонент, ответственных за выполнение данных политик. Это множество компонент носит название монитора безопасности обращений (reference monitor, МБО). Концепция монитора безопасности обращений является достаточно естественной формализацией некого механизма, реализующего разграничение доступа в системе. Монитор безопасности обращений представляет собой фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах разграничения доступа. Получив запрос на доступ от субъекта доступа к объекту, монитор безопасности обращений анализирует базу правил, соответствующую установленной в системе политике безопасности, и либо разрешает, либо запрещает доступ. При этом осуществляется регистрация обращений субъектов доступа к объектам доступа в журнале аудита.

Монитор безопасности обращений должен удовлетворять следующим свойствам:

- ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО;
- работа МБО должна быть защищена от постороннего вмешательства;
- представление МБО должно быть достаточно простым для возможности верификации корректности его работы.

Концепция монитора безопасности обращений является абстракцией, но перечисленные свойства справедливы и для программных или аппаратных модулей, реализующих функции монитора обращений в реальных системах (ядро безопасности, security kernel).

Далее рассмотрим наиболее распространенные формальные модели ИБ.

Формальные модели информационной безопасности

К моделям информационной безопасности в рамках домена CISSP «Архитектура безопасности» относят следующие [7]:

- формальные модели управления доступом (модель Белла-ЛаПадулы, модель матрицы доступа, модель Брюэра и Неша и модель «Take-Grant»);
- формальные модели обеспечения целостности (модель Кларка-Вилсона, модель Биба).

Следует отметить, что рассмотренные модели могут быть описаны с использованием более общих моделей, например, конечными автоматами или моделями информационных потоков.

Модель *Белла-ЛаПадулы* была предложена в 1975 году для формализации механизмов мандатного управления доступом в целях обеспечения конфиденциальности (секретности). Мандатный принцип разграничения доступа, в свою очередь, ставил своей целью перенести на информационные системы практику секретного документооборота, принятую в правительственных и военных структурах, когда все документы и допущенные к ним лица ассоциируются с иерархическими уровнями секретности (метки конфиденциальности).

В модели Белла-ЛаПадулы по грифам секретности распределяются субъекты и объекты, действующие в системе, и при этом выполняются следующие правила:

Простое правило безопасности (Simple Security). Субъект не может читать информацию более высокого уровня. Диаграмма информационных потоков, соответствующая реализации данного правила в системе с тремя уровнями секретности, приведена на рис. 3. Для данного правила существует мнемоническое обозначение No Read Up.

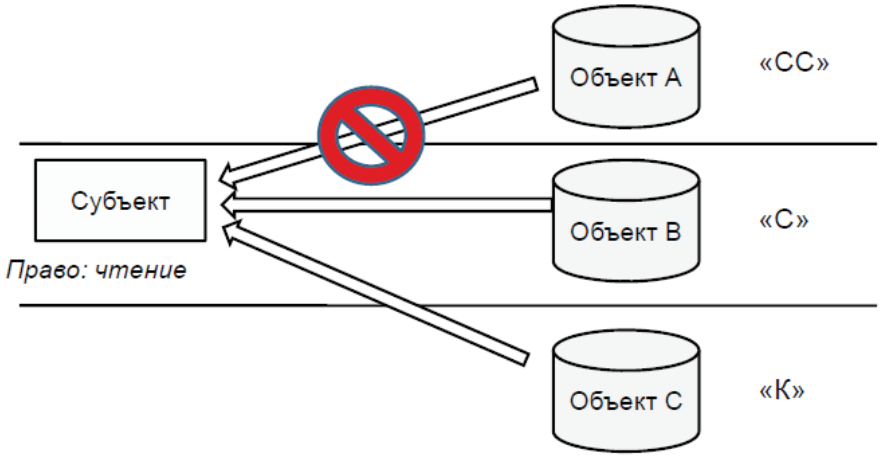

Рис.3. *Диаграмма информационных потоков для свойства «Simple Security»*

-свойство (-property). Субъект не может записывать информацию в более низкий уровень. Диаграмма информационных потоков, соответствующая реализации данного правила в системе с тремя уровнями секретности, приведена на рис. 4. Для данного правила мнемоническое обозначение No Write Down.

и столбца указаны права доступа соответствующего субъекта к данному объекту.

Матрица доступа, как правило, широко используется для реализации политики дискреционного разграничения доступа. Следует отметить, что и другие типы политик контроля доступа (например, мандатная или ролевая) могут быть так-

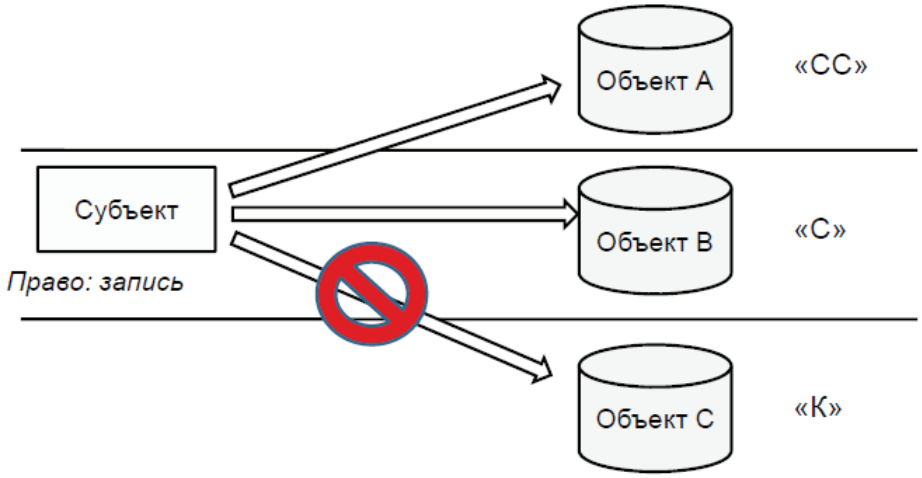

Рис.4. *Диаграмма информационных потоков для свойства «*-property»*

Строгое *-свойство (Strong *-property). Субъект, имеющий права чтения и записи, может выполнять операции только с объектами своего уровня. Диаграмма информационных потоков, соответствующая реализации данного правила в системе с тремя уровнями секретности, приведена на рис. 5.

же формализованы с использованием матрицы доступа. В этом случае строки и столбцы матрицы доступа должны идентифицировать роли или классификационные метки.

Модель целостности Кларка-Вилсона была предложена в 1987 г. как результат анализа практики бумажного документооборота, эффективной

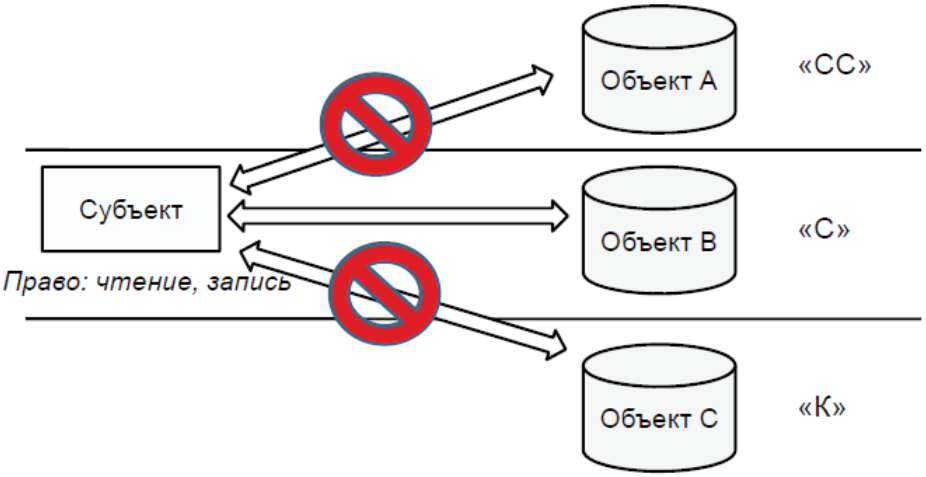

Рис.5. *Диаграмма информационных потоков для свойства «Strong *-property»*

Матрица доступа может быть представлена в виде таблицы, описывающей права доступа субъектов к объектам (рис. 6). Строки матрицы доступа соответствуют субъектам, существующим в системе, а столбцы – объектам. На пересечении строки

с точки зрения обеспечения целостности информации. Модель является описательной и не содержит каких бы то ни было строгих математических конструкций – скорее её целесообразно рассматривать как совокупность практических реко-

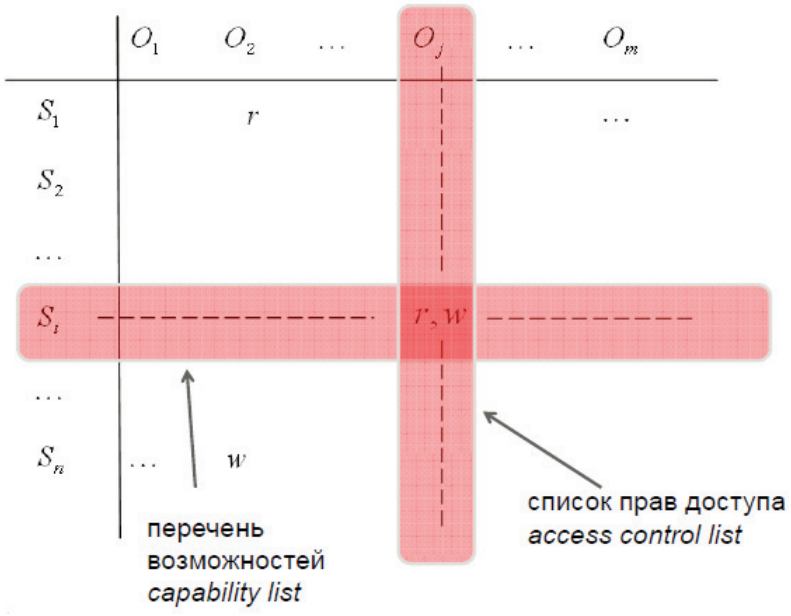

Рис.6. *Модель матрицы доступа*

мендаций по построению системы обеспечения целостности в информационной системе (рис. 7).

Введём следующие обозначения: CDI (Constrained Data Items) – данные, целостность которых контролируется; UDI (Unconstrained Data Items) – данные, целостность которых не контролируется. Правила модели Кларка-Вилсона представлены далее по тексту.

1. В системе должны иметься механизм контроля целостности (КЦ), способный подтвердить целостность любых данных типа CDI. Примером может служить механизм подсчёта контрольных сумм.

2. Применение любой процедуры преобразования к любому CDI должно сохранять целостность этого CDI.

3. Только процедуры преобразования могут вносить изменения в данные типа CDI.

4. Субъекты могут инициировать только определённые процедуры преобразования над определёнными данными типа CDI.

5. Должна быть обеспечена политика разделения обязанностей субъектов – т.е. субъекты не должны изменять данные типа CDI без вовлечения в операцию других субъектов системы.

6. Специальные процедуры преобразования могут превращать данные типа UDI в данные типа CDI.

7. Каждое применение процедуры преобразования должно регистрироваться в журнале регистрации событий (CDI log). При этом: данный CDI должен быть доступен только для добавления ин-

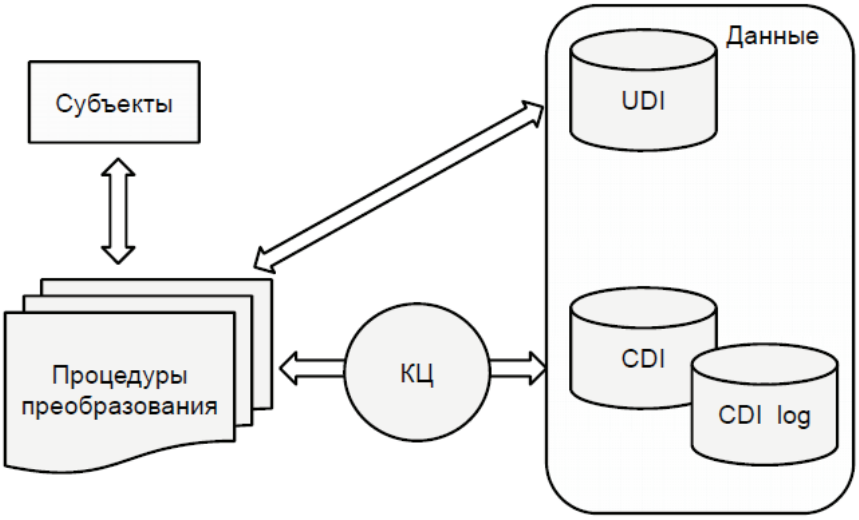

Рис.7. *Представление модели Кларка-Вилсона*

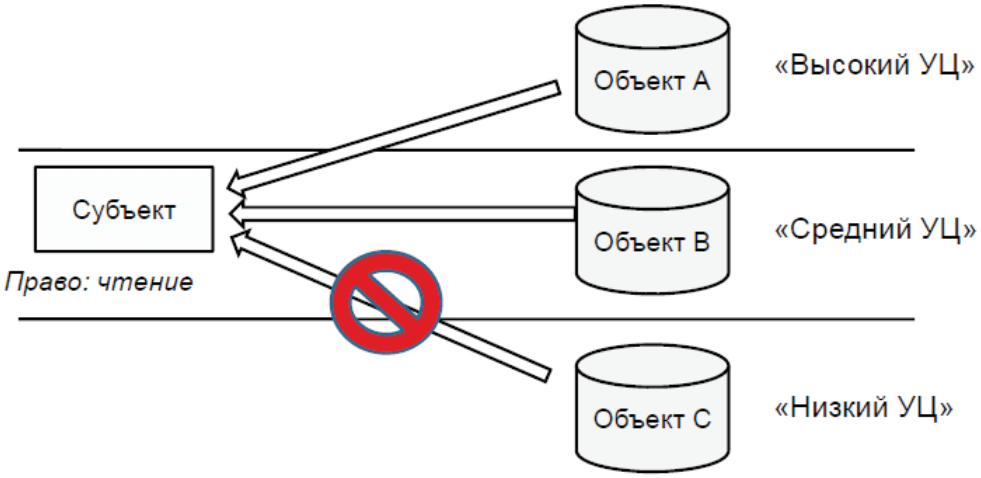

Рис.8. *Диаграмма информационных потоков для свойства «Simple Integrity»*

формации; в данный CDI необходимо записывать информацию, достаточную для восстановления полной картины функционирования системы.

8. Система должна распознавать субъекты, пытающиеся инициировать выполнение процедур преобразования.

низкого уровня целостности. Диаграмма информационных потоков, соответствующая реализации данного правила в системе с тремя уровнями целостности, приведена на рис. 8. Для данного правила существует мнемоническое обозначение No Read Down.

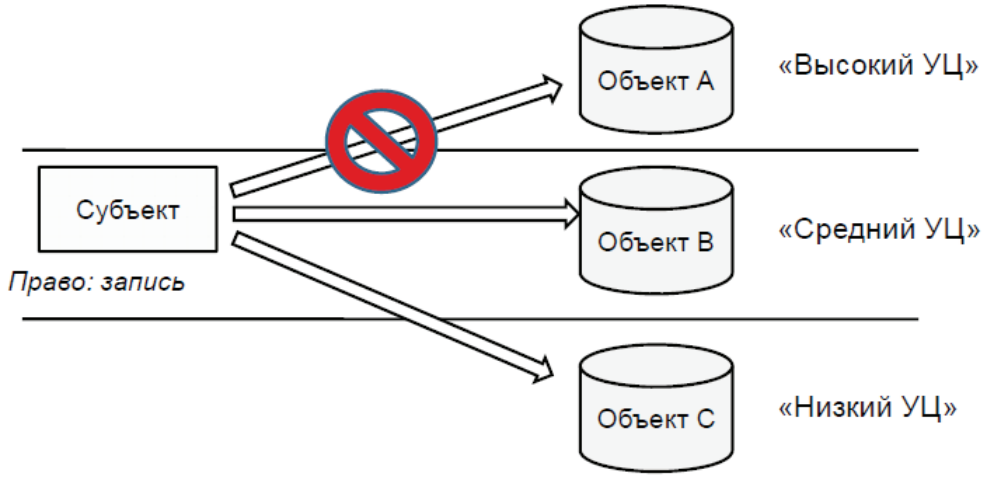

Рис.9. *Диаграмма информационных потоков для свойства «*-integrity»*

9. Система должна разрешать производить изменения в списках авторизации только специальным субъектам (например, администраторам безопасности).

Безусловными достоинствами модели Кларка-Вилсона являются её простота и лёгкость совместного использования с другими моделями безопасности.

Модель Биба была разработана в 1977 году как модификация модели Белла-ЛаПадулы, ориентированная на обеспечение целостности данных.

Базовые правила Модели Биба формулируются следующим образом.

Простое правило целостности (Simple Integrity, SI). Субъект не может читать информацию с более

-свойство (-integrity). Субъект не может записывать информацию в более высокий уровень целостности. Диаграмма информационных потоков, соответствующая реализации данного правила в системе с тремя уровнями целостности, приведена на рис. 9. Для данного правила мнемоническое обозначение No Write Up.

Свойство вызова (Invocation property). Субъект не может запрашивать сервис у другого субъекта, находящегося на более высоком уровне целостности.

Отдельного комментария заслуживает вопрос, что именно понимается в модели Биба под уровнями целостности. Действительно, в большинстве приложений целостность данных рассматривает-

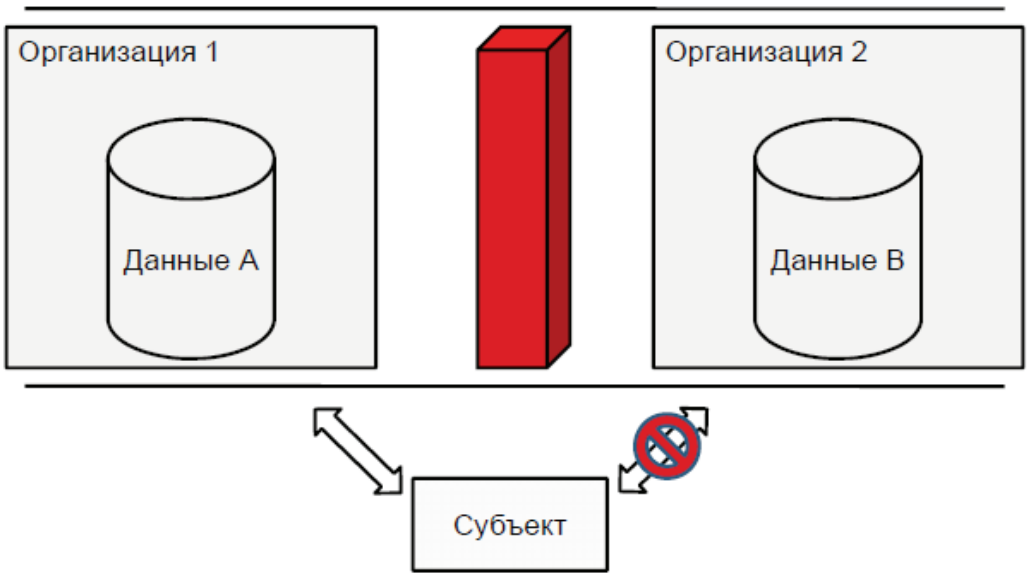

Рис.10. *Модель Брюэра и Неша*

ся как некое свойство, которое либо сохраняется, либо не сохраняется – и введение иерархических уровней целостности может представляться излишним. В действительности уровни целостности в модели Биба стоит рассматривать как уровни достоверности, а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот.

Модель «Take-Grant» является моделью, описывающей распространение прав доступа. Данная модель представляется в виде графа, который демонстрирует, каким образом права доступа могут передаваться между субъектами и объектами доступа. Преобразование графа возможно с использованием следующих правил:

- правило «Take» - позволяет субъекту брать право доступа у другого объекта;
- правило «Grant» - позволяет субъекту давать право доступа другому объекту;
- правило «Create» -позволяет субъекту создать новое право доступа;
- правило «Remove» -позволяет субъекту удалить право доступа.

Модель Брюэра и Неша, также называемая моделью «Китайская стена», разработана в 1989 году и позволяет избежать конфликта интересов при обращении к данным. Модель позволяет динамически изменять права доступа пользователя к данным в зависимости от его предыдущих действий. Модель применяется к единой базе данных и создает в ней домены безопасности, чувствительные с точки зрений конфликта интересов. Например, пользователь, работающий в компании «А» и имеющий доступ к данным компании «Б» (например, по роду своей деятельности), не должен одновременно иметь доступа к данным компании «В», конкурирующей с компанией «Б». Основная область применения модели – финансово-аналитические организации.

Отдельное внимание в домене уделено архитектурным нарушениям, которые приводят снижению уровня информационной безопасности. Указанное во многом связывают с понятием «скрытого канала».

Скрытый канал передачи данных

Рассмотри уязвимости проектирования и угрозы, которые могут быть реализованы с целью нарушения информационной безопасности, и контрмеры, которые могут использоваться для противостояния угрозам.

Под *скрытым каналом передачи информации* понимают любой канал связи, изначально для передачи информации не предназначенный. Для нас будут представлять интерес скрытые каналы, реализуемые за счёт особенностей формальных моделей управления доступом. Пусть имеется модель мандатного управления доступом и её реализация. Тогда любая потенциальная связь между двумя субъектами разных уровней конфиденциальности называется скрытым каналом передачи информации (рис. 11), если эта связь не разрешена в модели безопасности.

Выделяют следующие типы скрытых каналов:

- скрытые каналы по памяти, в которых информация передаётся через доступ отправителя на запись и получателя на чтение к одним и тем же ресурсам или объектам;

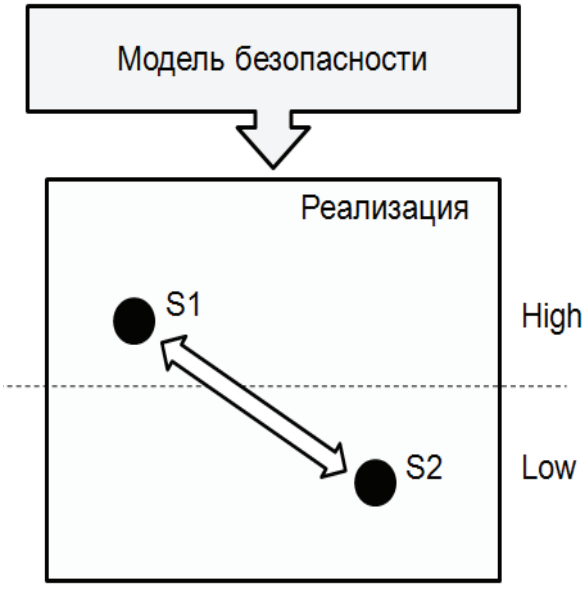

Рис.11. *Скрытый канал передачи информации*

- скрытые каналы по времени, которые характеризуются доступом отправителя и получателя к одному и тому же процессу или изменяемому во времени атрибуту.

Приведём примеры скрытых каналов передачи информации. Рассмотрим систему, в которой имеются два уровня секретности: High и Low. Передача информации с уровня Low на уровень High разрешена, а в обратном направлении – запрещена. Цель нарушителя состоит в том, чтобы организовать скрытый канал для передачи информации от программно-аппаратного агента, функционирующего в среде High, к другому программно-аппаратному агенту, функционирующему в среде Low.

Пример скрытого канала по памяти приведён на рис. 12. Субъект, функционирующий в среде High, может выполнять настройки параметров безопасности элементов файловой системы, и настройки доступны для наблюдения в среде Low. В этом случае злоумышленник может закодировать передаваемую информацию в значениях параметров безопасности тех или иных элементов файловой системы.

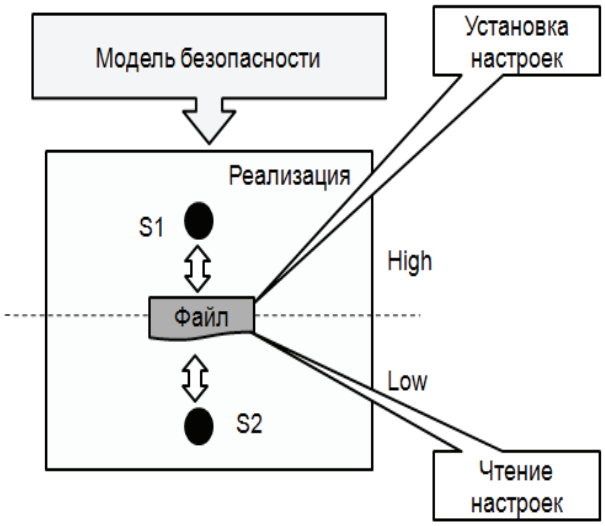

Рис.12. *Пример скрытого канала по памяти*

Пример скрытого канала по времени приведён на рис. 13. В данном случае между уровнями High и Low нет общих ресурсов, за исключением системной библиотеки, доступ к которой возможен только на чтение. Для организации скрытого канала передачи информации субъект S1 может модулировать определённым образом интервалы занятости библиотеки, а субъект S2– сканировать время занятости библиотеки, осуществляя запросы к ней с заданной периодичностью.

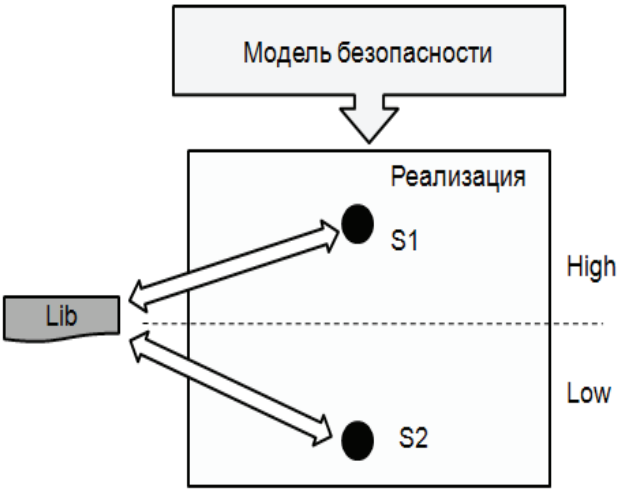

Рис.13. *Пример скрытого канала по времени*

Подходы к решению задачи выявления скрытых каналов передачи информации в настоящее время активно изучаются и совершенствуются. На сегодняшний день наиболее распространен метод разделяемых ресурсов Кемерера. Данный метод состоит в следующем: для каждого разделяемого ресурса в системе строится матрица, строки которой соответствуют всевозможным атрибутам разделяемого ресурса, а столбцы – операциям, выполняемым в системе; значения в ячейках матрицы соответствуют воздействиям, осуществляемым при выполнении тех или иных операций в отношении атрибутов разделяемых ресурсов.

При выполнении *атаки типа «время проверки / время использования»* (TOC/TOU – time-of-check/time-of-use) атакующий пытается изменить некоторое условие выполнения операции после того, как выполняемая программа проверила это условие. Это тип атак использует в своих целях зависимость от времени событий, происходящих в

многозадачной операционной системе. Для примера рассмотрим последовательность операций, выполняемых операционной системой при контроле доступа к файлам:

- субъект доступа (с меткой «конфиденциально») запрашивает доступ на чтение к файлу с конфиденциальной информацией;
- операционная система проверяет метки субъекта и объекта доступа;
- операционная система принимает решение о разрешении чтения файла;

Если между шагом 2 и шагом 3 атакующему удастся подменить файл с конфиденциальной информацией на файл с секретной информацией, то возможно нарушение установленной политики безопасности.

Для защиты от данного типа атак, как правило, используется блокировка к элементом, которые будут использоваться *при выполнении задач «проверки».*

Заключение

В настоящей статье рассмотрены ключевые модели домена «Архитектура безопасности», разобравшись в которых можно серьезно повысить свои шансы на успешную сдачу экзамена CISSP [8-11], поскольку заметная часть вопросов экзамена сформулирована с учетом базовых понятий, рассмотренных в данной статье.

Литература:

1. Дорофеев А. В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3. Дорофеев А. В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С. 66-73.
4. Дорофеев А. В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С. 69-73.
5. Дорофеев А. В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4(7).
6. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов; под ред. А. С. Маркова. - М.: Радио и связь, 2012. 192 с.
7. Цирлов В. Л. Основы информационной безопасности: краткий курс. Ростов н/Д: Феникс, 2008. 253 с.
8. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012. 600 p.
9. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
10. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012. 1216 p.
11. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012. 968 p.

References:

1. Dorofeev A. V. Status CISSP: kak poluchit' i ne poteryat'? Voprosy kiberbezopasnosti, 2013, No 1(1), pp.65-68.
2. Dorofeev A. V., Markov A. S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii, Voprosy kiberbezopasnosti, 2014, No 1 (2), pp. 67-73.
3. Dorofeev A. V. Menedzhment informatsionnoy bezopasnosti: upravlenie riskami, Voprosy kiberbezopasnosti, 2014, No 2(3), pp. 66-73.
4. Dorofeev A. V. Menedzhment informatsionnoy bezopasnosti: perekhod na ISO 27001:2013, Voprosy kiberbezopasnosti, 2014, No 3(4), pp. 69-73.
5. Dorofeev A. V. Podgotovka k CISSP: telekommunikatsii i setevaya bezopasnost', Voprosy kiberbezopasnosti, 2014, No 4(7).
6. Metody otsenki nesootvetstviya sredstv zashchity informatsii / A. S. Markov, V.L.Tsirlov, A. V. Barabanov; by ed. A. S. Markov. Moscow, Radio i svyaz', 2012, 192 p.
7. Tsirlov V. L. Osnovy informatsionnoy bezopasnosti: kratkiy kurs. Rostov n/D: Feniks, 2008, 253 p.
8. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012, 600 p.
9. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012, 936 p.
10. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012, 1216 p.
11. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012, 968 p.