МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Кафедра безопасности информационных систем

В.В. Бондаренко

Основы теоретической защиты информации

Учебное пособие

Издательство «Самарский университет»
2004

ББК 32.973
УДК 681.322
Б 811

Бондаренко В.В. Основы теоретической защиты информации: Учеб. пособие. Самара: Издательство "Самарский университет", 2004. 40 с.

В данном пособии кратко изложены основные положения формальной теории защиты информации в электронных системах обработки данных, которые проиллюстрированы на примерах. Особое внимание уделяется фундаментальному понятию защиты информации – политике безопасности, а также вопросам гарантирования выполнения в автоматизированной системе ее положений. Рассмотрены документы Министерства обороны США (TCSEC "Оранжевая книга").

Предназначено в качестве лекционного материала для студентов, обучающихся по специальности 075300 – организация и технология защиты информации, при изучении дисциплины "Защита информации в компьютерных системах"

ББК 32.973
УДК 681.322

Рецензент канд. тех.наук, доцент В.В. Камышников

Отв. редактор д-р физ.-мат. наук, проф. В.И. Астафьев

Введение

Основная цель настоящего пособия – изложить методы анализа систем защиты информации, предполагающего иерархическую декомпозицию. Верхний уровень иерархии составляет политика безопасности со своими специфическими методами ее анализа. Следующий уровень – основные системы поддержки политики безопасности (мандатный контроль, аудит и т.д.). Затем следует уровень механизмов защиты (криптографические протоколы, криптографические алгоритмы, системы создания защищенной среды и обновления ресурсов), которые позволяют реализовать системы поддержки политики безопасности. Самый низкий уровень – реализация механизмов защиты (виртуальная память, теговая архитектура, защищенные режимы работы процессора). В дальнейшем будем рассматривать только верхние уровни этой иерархии.

Проблематика защиты информации разделяется на несколько направлений: формулирование и изучение свойств теоретических моделей безопасности, анализ моделей безопасного взаимодействия (различные системы криптографической защиты), теория создания качественных программных продуктов.

Важно отметить, что существующая методология проектирования защищенной системы представляет собой итеративный процесс устранения найденных слабостей, некорректностей, неисправностей. Часто ряд злоумышленных действий не блокируется принципиально – противодействие данным угрозам выводится в область организационно-технических мер. При этом математическая модель политики безопасности рассматривает систему защиты в некотором стационарном состоянии, когда действуют защитные механизмы, а описание разрешенных и неразрешенных действий не меняется.

Основной особенностью информационной безопасности является практическая направленность. Другой особенностью ИБ является многоаспектность: обеспечение безопасности ведется по широкому кругу направлений (от установки ИБП до средств шифрования).

Основные понятия и определения

Понятие "информация" трактуется очень широко – от философского до бытового. В.И. Шаповалов дает следующее определение: "Информация об объекте есть изменение параметра наблюдателя, вызванное взаимодействием наблюдателя с объектом". Количественное измерение информации К. Шеннона гласит, что "информация определяется только вероятностными свойствами сообщений. Все другие их свойства, например полезность для тех или других действий, принадлежность тому или иному автору и др., игнорируются".

Определение. ***Информация*** есть сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, воспринимаемые человеком или специальным устройством и используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами.

Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов) на носителях различных типов. Будем рассматривать только те формы представления информации, которые используются при ее автоматизированной обработке.

Определение. ***Автоматизированная система обработки информации (АСОИ)*** – организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов.

- технических средств обработки и передачи данных (средства вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего ПО;
- информации (массивов, наборов, БД) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Определение. ***Информационная безопасность автоматизированной системы (ИБ АС)*** – состояние рассматриваемой АС, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создают информационных угроз для элементов самой системы и внешней среды.

Вспомогательные структуры (модели), используемые в защите информации

Чтобы провести исследование и получить практический результат, в объект исследования часто вносят некоторую структуру, которая имеет искусственный характер, но облегчает исследование. Иногда говорят еще, что строится модель объекта. Рассмотрим несколько структур, которые вносятся в неопределяемый объект под названием "информация".

Язык, объект, субъекты

Используем некоторые понятия математической логики. Пусть A – конечный алфавит, $\mathcal{A}$ – множество слов конечной длины в алфавите A. Из $\mathcal{A}$ при помощи некоторых правил выделено подмножество $\mathcal{L}$ правильных слов, которое называется языком. Пусть $\mathcal{L}_1$ – язык описания одной инфор-

мации, $\mathcal{L}_2$ – другой. Тогда можно говорить о языке $\mathcal{L}$, объединяющем $\mathcal{L}_1$ и $\mathcal{L}_2$, описывающем ту и другую информацию, а $\mathcal{L}_1$ и $\mathcal{L}_2$ – подъязыки $\mathcal{L}$.

Пусть любая информация представлена в виде слова в некотором языке $\mathcal{L}$. Можно полагать, что состояние любого устройства в вычислительной системе достаточно полно описано словом в некотором языке. Тогда можно отождествлять слова и состояния устройств и механизмов вычислительной системы или произвольной электронной системы обработки данных (ЭСОД). Эти предположения позволяют весь анализ вести в терминах некоторого языка.

Определение. ***Объектом относительно языка*** $\mathcal{L}$ (или просто ***объектом***) называется произвольное конечное множество языка $\mathcal{L}$.

Пример

Произвольный файл в компьютере – объект.

Пример

Пусть текст в файле разбит на строки так, что любая строка также является словом языка $\mathcal{L}$. Следовательно, один объект может являться частью другого объекта.

Пример

Принтер компьютера - объект.

Выделим особо описания преобразований данных.

Преобразование информации отображает слово, описывающее исходные данные, в другое слово. Описание преобразования также является словом. Каждое преобразование информации может:

- храниться - хранение описания преобразования в некотором объекте;
- действовать – описание программы взаимодействует с другими ресурсами ВС (память, процессор).

Определение. Ресурсы системы, выделяемые для действия преобразования, называются ***доменом***.

Для осуществления преобразования кроме домена необходимо передать этому преобразованию особый статус в системе, при котором ресурсы системы осуществляют преобразование. Этот статус называется ***управление***.

Определение. Преобразование, которому передано управление, называется ***процессом***.

Определение. Объект, описывающий преобразование, которому выделен домен и передано управление, называется ***субъектом***:

субъект = (домен , процесс).

Для реализации преобразования субъект использует информацию, содержащуюся в объекте o, т.е. осуществляет ***доступ*** к o.

Пример

Доступ субъекта s к объекту o на чтение r данных об объекте o.

Пример

Доступ субъекта s к объекту o на запись w данных в объект o. В данном случае возможно стирание предыдущей информации.

Пример

Доступ субъекта s к объекту o на активизацию процесса *exe*, записанного в объекте o как данные. При этом формируется домен и передается управление программе.

Обозначим множество возможных доступов в системе через $\mathcal{R}$, множество объектов через $\mathcal{O}$, множество субъектов через $\mathcal{S}$. Каждый субъект является объектом относительно некоторого языка, который может в активной фазе сам менять свое состояние. Следовательно, $\mathcal{S} \subset \mathcal{O}$.

Состояние системы характеризуется некоторым конечным множеством объектов. В любой момент времени на множестве субъектов введем бинарное отношение активизации @.

Пусть субъекты s_1, s_2 находятся в отношении активизации $s_1 @ s_2$. Это означает, что субъект s_1, обладая управлением и ресурсами, может передать часть ресурсов и управление субъекту s_2, т.е. происходит процесс активизации. Следовательно, на множестве объектов, для которых определено понятие активизации, введенным бинарным отношением определяется некоторый граф. Вершины графа, в которые никогда не входит ни одной дуги, это субъекты – пользователи. Субъекты, в которые никогда не входят дуги и из которых не выходят дуги, из нашего рассмотрения исключаются.

Аксиома ("Оранжевая книга").

Все вопросы безопасности информации описываются доступами субъектов к объектам.

В связи с этим будем рассматривать множество объектов и последовательности доступов.

Пусть время дискретно. $\mathcal{O}_t$ – множество объектов в момент времени t, $\mathcal{S}_t$ – множество субъектов в момент времени t. На множестве $\mathcal{O}_t$ определим ориентированный граф доступов G_t. Дуга $s \xrightarrow{\rho} o$ принадлежит графу G_t, $\rho \subset \mathcal{R}$, тогда и только тогда, когда в момент времени t субъект s имеет множество доступов ρ к объекту o.

С точки зрения защиты информации нас интересует множество графов доступов $\{\mathsf{G}_t\}_{t=1}^{T}$ и множество возможных графов доступа $\mathcal{G} = \{\mathsf{G}\}$.

$\mathcal{G}$ есть фазовое пространство системы. Траектория в фазовом пространстве $\mathcal{G}$ есть функционирование вычислительной системы.

Задача защиты информации формулируется следующим образом. В фазовом пространстве $\mathcal{G}$ определены возможные траектории $\mathcal{G}'$. В $\mathcal{G}'$ выделено подмножество неблагоприятных траекторий $\mathcal{N}$. Необходимо, чтобы любая реальная траектория вычислительного процесса в $\mathcal{G}$ не попала в $\mathcal{N}$. Это можно сделать только ограничением на доступ в каждый момент времени. Но дело в том, что службе защиты доступно только локальное воздействие. В этом и заключается основная сложность: имея возможность использовать набор локальных ограничений на доступ в каждый момент времени, необходимо решить глобальную проблему недопущения выхода любой возможной траектории во множество $\mathcal{N}$.

Следует отметить, что $\mathcal{N}$ не обязательно определяет ограничения на доступ конкретных субъектов к конкретным объектам. Проиллюстрируем это на примере.

Пример

Пусть в системе имеются пользователи u_1 и u_2, процесс s чтения на экран файла, файлы $o_1, o_2, \ldots, o_m$. В каждый момент работает только один пользователь. По окончании его работы система отключается, и другой пользователь включает систему заново. В системе имеются следующие графы доступа:

$$u_j \xrightarrow{R} s \xrightarrow{r} o_i,\ i = \overline{1,m},\ j = 1,2, \qquad (1)$$

которые образуют множество графов $\mathcal{G}$. Траектории фазового пространства есть последовательность графов вида (1). Неблагоприятными для некоторого $i = \overline{1,m}$ будем считать состояния:

$$u_1 \xrightarrow{R} s \xrightarrow{r} o_i,$$

$$u_2 \xrightarrow{R} s \xrightarrow{r} o_i,$$

т.е. неблагоприятно, когда оба пользователя могут прочитать один объект. Механизм защиты должен строить ограничения на очередной доступ исходя из множества объектов, с которыми уже ознакомился другой пользователь. Следовательно, можно доказать, что в указанном смысле обеспечивается безопасность информации.

Пример

Пусть неблагоприятна любая траектория, содержащая граф вида

$$u_1 \xrightarrow{R} s \xrightarrow{r} o_1.$$

В этом случае доказывается, что система защищена ограничением доступа на чтение пользователя u_1 к объекту o_1.

Иерархические модели

В настоящее время основным инструментом решения задач анализа, проектирования, создания и поддержки в рабочем состоянии сложных систем является иерархический метод. В основе метода лежит разбиение системы на ряд уровней, которые связаны одинаправленной функциональной зависимостью.

В целях понимания одного и того же в декомпозициях различной природы сложных систем можно договориться об универсальных принципах иерархического метода. Предположим, что сложная система A адекватно описана на языке $\mathcal{L}$. Пусть проведена декомпозиция (разложение) языка $\mathcal{L}$ на семейство языков $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$. Если язык $\mathcal{L}_i$, $i = \overline{2,n}$, синтаксически зависит только от словоформ языка $\mathcal{L}_{i-1}$, то они образуют два соседних уровня. Тогда система A может быть описана набором слов $B_1, B_2, \ldots, B_n$ в языках $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$. При этом описание B_i синтаксически может зависеть только от набора B_{i-1}. В этом случае говорят об иерархической декомпозиции системы A к уровням декомпозиции $B_1, B_2, \ldots, B_n$, где уровень B_i непосредственно зависит от B_{i-1}. Рассмотрим примеры иерархического построения сложных систем.

Пример

Пусть вся информация в системе разбита на два класса: секретно и совершенно секретно (цифровые обозначения 0 и 1 соответственно). Пусть все пользователи разбиты в своих возможностях допуска к информации на два класса, которые также будем обозначать 0 и 1. Обозначим через $\bar{x}$ класс запрашиваемой информации X, $\bar{y}$ – класс пользователя Y. Сформулируем правило допуска к информации X при запросе пользователя Y: допуск к информации разрешен тогда и только тогда, когда $\bar{x} = \bar{y}$, или в виде формулы некоторого языка $\mathcal{L}_2$:

$$if \quad \bar{x} = \bar{y} \quad then \quad \text{"Допуск } Y \text{ к } X\text{"}$$

Для вычисления этого выражения необходимо осуществить следующие операции в терминах языка $\mathcal{L}_1$:

$$\bar{x} := U_1(X),$$
$$\bar{y} := U_2(Y),$$
$$z := \bar{x} \oplus y,$$
$$U(X, Y, z).$$

Здесь $U_1(X)$ – оператор определения по имени объекта X номера класса доступа $\bar{x}$; $U_2(Y)$ – оператор определения по имени пользователя Y но-

мера класса допуска y; $U(X,Y,z)$ – оператор, реализующий доступ Y к X, если $z=0$, и блокирующий систему, если $z=1$. По построению уровень B_2 зависит от B_1, а вся система представлена иерархической двухуровневой декомпозицией с языками $\mathcal{L}_1$ и $\mathcal{L}_2$, $\mathcal{L}=(\mathcal{L}_1,\mathcal{L}_2)$.

Пример

Иерархическая декомпозиция вычислительной системы в виде трех уровней:

Аппаратная часть – Операционная система – Программы пользователя

Информационный поток

Структуры информационных потоков являются основой анализа каналов утечки и обеспечения секретности информации. Эти структуры опираются на теорию информации и математическую теорию связи. Рассмотрим примеры потоков.

Пример

Субъект s осуществляет доступ на чтение r к объекту o. В этом случае идет речь об информационном потоке от o к s, объект o – источник, субъект s – получатель информации.

Пример

Субъект s осуществляет доступ на запись w к объекту o. Здесь имеется информационный поток от s к o, объект o – получатель, субъект s – источник информации.

Из простых потоков можно строить сложные. Например, информационный поток от субъекта s_2 к субъекту s_1 по схеме:

$$s_1 \xrightarrow{r} o \xleftarrow{w} s_2.$$

Здесь s_2 – источник, а s_1 – получатель информации, и можно говорить о передаче информации, позволяющей реализовать поток.

Определение. Каналы, использующие общие ресурсы памяти, называются ***каналами по памяти***.

С точки зрения защиты информации, каналы и информационные потоки бывают законными и незаконными. Незаконные информационные потоки создают утечку информации и могут нарушать секретность данных.

Будем считать, что всю информацию о вычислительной системе можно описать конечным множеством объектов. Каждый объект – конечное множество слов в некотором языке $\mathcal{L}$. В каждом объекте выделено состоя-

ние, а совокупность состояний объектов называется состоянием системы. Функция системы – последовательное преобразование информации в системе под действием команд. В результате из состояния v под действием команды α система переходит в состояние v' и обозначается как

$$v \to_{\alpha} v'.$$

Приведем еще несколько примеров информационных потоков в вычислительных системах.

Пример

Операция присвоения значения переменных:

$$Y := X.$$

После выполнения операции присвоения по полученной в состоянии v' величине Y однозначно восстанавливается X. В данном случае имеем симметричный информационный канал.

Пример

$$Y := X;$$
$$Z := Y.$$

Выполнение этих команд вызывает косвенный поток информации $X \to Z$ такой же величины, как прямой поток $X \to Y$.

Пример

$$Z := X + Y.$$

Пример

$$Z := X \oplus Y.$$

Здесь Z не несет информации о X и Y

Ценность информации

Чтобы защитить информацию, надо затратить определенные силы и средства. Для этого надо знать, какие потери мы могли бы понести. Очевидно, что в денежном выражении затраты на защиту не должны превышать возможные потери. Для решения этих задач в информацию вводятся вспомогательные структуры – ценность информации.

Аддитивная модель

Пусть информация представлена в виде конечного множества элементов Необходимо оценить суммарную стоимость информации в денежных единицах исходя из оценок компонент. Оценки компонент строятся на основе экспертных оценок. При этом возникает вопрос адекватности и объективности количественных оценок компонент даже при квалифицированной экспертизе из-за неоднородности компонент в целом. Поэтому делают

единую иерархическую относительную шкалу. Она определяет линейный порядок, который позволяет сравнивать отдельные компоненты по ценности относительно друг друга. Единая шкала означает равенство цены всех компонент, имеющих одну и ту же порядковую оценку.

Пример

Пусть $o_1, o_2, \ldots, o_n$ – объекты, $1 < 2 < \ldots < 5$ – шкала, (2; 1; 3; ...;4) – вектор относительных ценностей по оценкам экспертов. Если $c_1 = 100$ руб., то $c_3 = 150$ руб. Сумма $\sum_{i=1}^{n} c_i$ дает стоимость всей информации. Если априорно известна цена информации, то относительные оценки в порядковой шкале позволяют вычислить цены компонент.

Анализ риска

Пусть в рамках аддитивной модели проведен учет стоимости информации в системе. Оценка возможных потерь строится на основе полученных стоимостей компонент исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий. Потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

Пример

Пусть $o_1, o_2, \ldots, o_n$ – объекты, $c_1, c_2, \ldots, c_n$ – их ценности, ущерб одному объекту не снижает цены других и вероятность нанесения ущерба объекту o_i равна p_i. Тогда функция потерь ущерба для объекта o_i равна:

$$W_i = \begin{cases} c_i, \text{объекту нанесен ущерб,} \\ 0, \text{иначе.} \end{cases}$$

Оценка потерь от реализации угроз объекту o_i равна:

$$EW_i = p_i c_i .$$

Потери в системе равны:

$$W = W_1 + W_2 + \ldots + W_n .$$

Ожидаемые потери (средний риск):

$$EW = \sum_{i=1}^{n} p_i c_i .$$

Порядковая шкала ценностей

Оценка личной, политической или военной информации не всегда разумна в денежном исчислении. Но и в этих случаях по-прежнему используют подход, связанный со сравнением ценности отдельных информационных элементов между собой.

Пример

Все объекты (документы) государственного учреждения разбиваются по грифам секретности, которые образуют порядковую шкалу:

несекретно<для служебного пользования<секретно<совершенно секретно.

В США:

$$\text{unclassified} < \text{confidential} < \text{secret} < \text{top secret}.$$

Более высокий класс имеет более высокую ценность, и поэтому требования по его защите от НСД более высокие.

Модель решетки ценностей

Модель решетки является обобщением порядковой шкалы.

Пусть SC – конечное частично упорядоченное множество относительно бинарного отношения $\preceq$ Это означает, что для каждых A, B, C выполняются свойства:

1) $A \preceq A$ – рефлексивность;

2) $A \preceq B, B \preceq C \Rightarrow A \preceq C$ – транзитивность;

3) $A \preceq B, B \preceq A \Rightarrow A = B$ - антисимметричность.

Определение. Для $A, B \in \text{SC}$ элемент $C = A \oplus B \in \text{SC}$ называется ***наименьшей верхней границей*** (верхней гранью), если

1) $A \preceq C, B \preceq C$;

2) $A \preceq D, B \preceq D \Rightarrow C \preceq D \ \forall D \in \text{SC}$.

Элемент $A \oplus B$ может не существовать.

Определение. Для $A, B \in \text{SC}$ элемент $E = A \otimes B \in \text{SC}$ называется ***наибольшей нижней границей*** (нижней гранью), если

1) $E \preceq A, E \preceq B$;

2) $D \preceq A, D \preceq B \Rightarrow D \preceq E \ \forall D \in \text{SC}$.

Эта граница также может не существовать.

Вопрос. Что можно сказать об единственности этих граней?

Определение. (SC, $\preceq$) называется ***решеткой***, если для любых A, $B \in \text{SC}$ существуют $A \oplus B \in \text{SC}$ и $A \otimes B \in \text{SC}$.

Лемма

Для любого набора $S = \{A_1, A_2, \ldots, A_n\}$ *элементов из решетки* SC *существуют единственные элементы:*

$\oplus S = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ – *наименьшая верхняя грань,*

$\otimes S = A_1 \otimes A_2 \otimes \ldots \otimes A_n$ – *наибольшая нижняя грань.*

Доказательство проведите самостоятельно.

Для всех элементов SC в конечных решетках существуют верхний элемент High = ⊕ SC и нижний элемент Low = ⊗ SC.

Определение. ***Конечная линейная решетка*** – это линейно упорядоченное множество.

Поэтому можно всегда считать, что $SC = \{0,1,2,\ldots,n\}$.

Для большинства встречающихся в теории защиты информации решеток существует представление решетки в виде графа. Рассмотрим корневое дерево на вершинах из конечного множества $X = \{X_1, X_2, \ldots, X_n\}$ с корнем X_1. Пусть на единственном пути, соединяющем вершину X_i с корнем, есть вершина X_j. Положим по определению: $X_i \le X_j$. Таким образом, на дереве определен частичный порядок.

Вопрос. Решетка ли это?

Решетка подмножеств X

Для любых множеств $A, B \subseteq X$ положим:

$$A \le B \overset{def}{=} A \subseteq B.$$

Вопрос. Выполняются ли условия частичного порядка?

Вопрос. Чем являются $A \oplus B$, $A \otimes B$?

Вопрос. Решетка ли это?

MLS (Multilevel Security) решетка

MLS решетка лежит в основе государственных стандартов оценки информации. Решетка строится как прямое произведение линейной решетки L и решетки SC подмножеств множества X, т.е. (α, β), (α', β') – элементы произведения, $\beta, \beta' \in L$, $\alpha, \alpha' \in SC$. Тогда

$$(\alpha, \beta) \le (\alpha', \beta') \Leftrightarrow \alpha \subset \alpha', \beta \le \beta'.$$

Верхние и нижние границы определяются так:

$$(\alpha, \beta) \oplus (\alpha', \beta') \Leftrightarrow (\alpha \cup \alpha', \max\{\beta, \beta'\}),$$
$$(\alpha, \beta) \otimes (\alpha', \beta') \Leftrightarrow (\alpha \cap \alpha', \min\{\beta, \beta'\}).$$

Вся информация (объекты системы) отображается в точки решетки $\{(\alpha;\beta)\}$. Обычно линейная решетка указывает гриф секретности, а точки множества X называются ***категориями***.

Свойства решетки в оценке информации существенно используются при классификации новых объектов, полученных в результате вычислений.

Пусть дана решетка ценностей SC, множество текущих объектов $\mathcal{O}$, отображение $c:\mathcal{O}\to \mathrm{SC}$. Программа использует информацию объектов $o_1,o_2,\ldots,o_n$, которые классифицированы точками решетки: $c(o_1),c(o_2),\ldots,c(o_n)$. В результате работы программы появился объект o, который необходимо классифицировать. Это можно сделать, положив:

$$c(o)=c(o_1)\oplus c(o_2)\oplus\ldots\oplus c(o_n).$$

Такой подход к классификации наиболее распространен в государственных структурах.

Пример

В сборник научных статей включают две статьи с грифом "секретно" и "совершенно секретно". По тематике первая статья – "кадры", вторая статья – "криптография". В итоге сборник приобретает гриф "совершенно секретно", его тематика определяется совокупностью тематик статей ("кадры", "криптография").

Вопрос. Приведите аналогичные примеры.

Угрозы информации

Если информация представляет ценность, то необходимо понять, в каком смысле эту ценность нужно оберегать. Когда ценность информации теряется при ее раскрытии, то имеется опасность нарушения ее секретности. При потере ценности информации из-за ее изменения или уничтожения говорят об опасности для целостности информации. Если ценность информации заключается в ее оперативном использовании, то имеется опасность нарушения доступности информации. В случае же, когда ценность информации теряется при сбоях в системе, то есть опасность потери устойчивости к ошибкам. Рассматривают четыре опасности, которые надо предотвратить путем защиты: секретность, целостность, доступность, устойчивость к ошибкам.

Определение. ***Угроза*** – потенциально возможное событие, действие/воздействие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Определение. ***Угроза ИБ АС*** – возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к искажению, унич-

тожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

В настоящее время перечень угроз ИБ АС насчитывает сотни пунктов. Наиболее характерные и часто реализуемые следующие:

- несанкционированное копирование носителей информации;
- неосторожные действия, приводящие к разглашению секретной информации или делающие ее доступной;
- игнорирование организационных установленных правил при определении ранга системы.

Задание возможных угроз ИБ проводится с целью определения полного перечня требований к разрабатываемой системе защиты. Перечень угроз, оценки вероятностей их реализаций, модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты АС. Кроме выявления возможных угроз должен быть проведен их анализ на основе классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз ИБ АС обусловлена невозможностью формализации задачи описания полного множества угроз из-за того, что накапливаемая, хранимая и обрабатываемая в АС информация подвержена случайным влияниям чрезвычайно большого числа факторов. Поэтому для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз.

Классификация всех возможных угроз ИБ АС может быть проведена по ряду базовых признаков.

1. По природе возникновения.
   1.1. Естественные угрозы – вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.
   1.2. Искусственные угрозы – угрозы ИБ АС, вызванные деятельностью человека.
2. По степени преднамеренности проявления.
   2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.
   2.2. Угрозы преднамеренного действия.
3. По непосредственному источнику угроз.
   3.1. Угрозы, непосредственным источником которых является природная среда.

3.2. Угрозы, непосредственным источником которых является человек.
3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.
3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства.

4. По положению источника угроз.
4.1. Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС.
4.2. Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС.
4.3. Угрозы, источник которых имеет доступ к периферийным устройствам АС (терминалам).
4.4. Угрозы, источник которых расположен в АС.

5. По степени зависимости от активности АС.
5.1. Угрозы, которые могут проявляться независимо от активности АС.
5.2. Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных.

6. По степени воздействия на АС.
6.1. Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС.
6.2. Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС.

7. По этапам доступа пользователей или программ к ресурсам АС.
7.1. Угрозы, которые могут проявляться на этапе доступа к ресурсам АС.
7.2. Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС.

8. По способу доступа к ресурсам АС.
8.1. Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС.
8.2. Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС.

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.
9.1. Угрозы доступа к информации на ВЗУ.
9.2. Угрозы доступа к информации в ОЗУ.
9.3. Угрозы доступа к информации, циркулирующей в линиях связи.
9.4. Угрозы доступа к информации, отображаемой на дисплее или печатаемой на принтере.

Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются конфиденциальность, целостность и доступность информации.

Таким образом, принято считать, что ИБ АС обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности, целостности и доступности. Соответственно, для АС рассматривают три основных вида угроз: угроза нарушения секретности, угроза нарушения целостности, угроза отказа в обслуживании.

Данные виды угроз являются первичными или непосредственными, т.к. реализация вышеперечисленных угроз приведет к непосредственному воздействию на защищаемую информацию. Если система, в которой циркулирует информация, прозрачна (не существует систем защиты или других препятствий), то также возможно для атакующего непосредственное воздействие на информацию. На сегодняшний день функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется в чистом виде. На пути к ней имеется система защиты, поэтому атакующая сторона должна преодолеть эту систему. Однако не существует абсолютно стойкой системы защиты. Вопрос лишь во времени и средствах, требующихся на ее преодоление. В связи с этим примем следующую модель:

Защита информационной системы считается преодоленной, если в ходе ее исследования определены все уязвимости системы

Так как преодоление защиты также представляет угрозу, то добавим четвертый вид угроз: угрозу раскрытия параметров АС, которую можно рассматривать как опосредованную. Последствия ее реализации не причиняют ущерб обрабатываемой информации, но дают возможность реализоваться первичным угрозам. Введение угрозы раскрытия позволяет с научно-методической точки зрения описывать отличия защищенных ИС от открытых. Для последних угроза разведки параметров системы считается реализованной.

Для обоснования угрозы раскрытия рассмотрим модель. Пусть существует информационная система W. Для функционирования система W использует собственную модель M_W. Одним из параметров модели является объем информационных ресурсов – объем базы знаний ИС. Рассматриваемой системе W противодействует аналогичная система T (противник), функционирующая на основе собственной модели M_T. Между системами происходит информационное противоборство – влияние на информационные ресурсы противоборствующих сторон. При информацион-

ном противоборстве системы еще строят модели противоборствующих сторон: $M_{T(W)}$ и $M_{W(T)}$ для W и T соответственно.

При информационном взаимодействии отсутствует непосредственный контакт двух систем. Вся информация передается по информационному каналу, являющемуся составляющей модели информационного взаимодействия. Таким образом, получена симметричная модель.

Сопоставим вышеперечисленные виды угроз с моделью информационного противоборства двух систем. Угроза нарушения конфиденциальности: возможность добавлять информационные ресурсы противоборствующей системы к собственным ресурсам. Угроза нарушения целостности: возможность противоборствующей системы внедрять собственные информационные ресурсы, используя для этого передачу по информационному каналу. Угроза отказа служб: возможность одной из систем разорвать информационный канал. Угроза разведки параметров системы: возможность системы организовать информационный канал с целью нарушения конфиденциальности и целостности.

Таким образом, существование угрозы разведки параметров системы получает свое подтверждение с формальной точки зрения на основании модели информационного противоборства двух информационных систем.

Угрозы секретности

В руководстве по использованию американского стандарта защиты информации говорится, что существует только два пути нарушения секретности:

1) утрата контроля над системой защиты;

2) каналы утечки информации.

Утрата управления системой защиты может быть реализована оперативными мерами. В этом случае на первое место выступают административные и кадровые методы защиты. Утрата контроля за защитой может возникнуть в критической ситуации, созданной стихийно или искусственно. Поэтому отсутствие устойчивости к ошибкам – одна из главных опасностей для системы защиты. Утрата контроля может возникнуть за счет взламывания защиты самой системы защиты. Противопоставить этому можно только создание защищенного домена для системы защиты.

Основной класс каналов утечки в ЭСОД – это ***каналы по памяти*** – каналы, которые образуются за счет использования доступа к общим объектам системы. Канал утечки по памяти можно изобразить следующим образом:

$$u_1 \xrightarrow{r,exe} S \xrightarrow{r} O \xleftarrow{w} u_2.$$

Пользователь u_1 активизирует процесс, который может получить доступ на чтение к общему с пользователем u_2 ресурсу o. При этом u_2 может писать в o, а u_1 может читать от s.

Следующий основной класс каналов утечки это ***каналы по времени*** – каналы, передающие противнику информацию о процессе, промодулированном ценной закрытой информацией. Канал утечки по времени можно изобразить следующим образом:

$$u_1 \xrightarrow{r,exe} s \xrightarrow{r} s_m \xleftarrow{w} s_c \xleftarrow{exe} u_2,$$

где u_1 – злоумышленник, u_2 – пользователь, s_c – субъект, информация о котором представляет интерес, s_m – субъект, процесс которого модулируется информацией процесса s_c, s – процесс от имени u_1, позволяющий наблюдать процесс s_m. Функционирование канала утечки определяется той долей ценной информации о процессе s_c, которая передается путем модуляция процессу s_m.

Угрозы целостности

Нарушение целостности информации – это незаконное уничтожение или модификация информации.

Защита целостности информации относится к категории организационных мер. Основным источником угроз целостности являются пожары и стихийные бедствия, случайные и преднамеренные критические ситуации в системе, вирусы, «троянские кони». В данном случае говорят о канале воздействия на целостность или канале разрушающего воздействия. Они аналогичны каналам утечки, если заменить доступ r доступом w.

В качестве примера приведем схему канала несанкционированной модификации, использующего механизм «***троянского коня***».

$$u_1 \xrightarrow{w} T \subset S \xleftarrow{exe} u_2$$
$$\downarrow w$$
$$O$$

Здесь u_1 – злоумышленник, u_2 – пользователь, o – объект с ценной информацией, S – процесс (программа), являющийся общим ресурсом для u_1 и u_2. Злоумышленник u_1, пользуясь правом доступа w, модифицировал общий ресурс S, встроив в него скрытую программу T, модифицирующую информацию в o при запуске ее пользователем u_2. Исследованием подобных схем занимается теория распространения вирусов.

Основой защиты целостности являются:

- регулярное копирование ценной информации;
- помехозащищенное кодирование информации (введение избыточности в информацию);
- создание системной избыточности.

Использование таких механизмов позволяет также решать задачи устойчивости к ошибкам и задачи защиты от нарушений доступности.

Политика безопасности

Понятие политики безопасности

Понятие "защищенности" принципиально не отличается от других свойств технической системы и является для системы внешним, априорно заданным. Особенностью понятия "защищенность" является его тесная связь с понятиями "злоумышленник" (обозначение внешней причины для вывода системы из состояния "защищенности") и "угроза" (обезличенная причина вывода системы из защищенного состояния действиями злоумышленника).

При рассмотрении понятия "злоумышленник" выделяется объект его воздействия – часть системы, на которую направлены его действия ("объект атаки"). Можно выделить три компонента, связанные с нарушением безопасности системы:

1) "злоумышленник" – внешний по отношению к системе источник нарушения свойства "безопасность";
2) "объект атаки" – часть, принадлежащая системе, на которую злоумышленник производит воздействие;
3) "канал воздействия" – среда переноса злоумышленником действия.

Интегральной характеристикой защищаемой системы является политика безопасности (ПБ) – качественное (качественно-количественное) выражение свойств защищенности в терминах, представляющих систему. Описание ПБ может включать или учитывать свойства злоумышленника и объекта атаки. Часто рассматриваются политики безопасности, связанные с понятием "доступ" Доступ – категория субъектно-объектной модели, описывающая процесс выполнения операций субъектов над объектами.

Политика безопасности включает:

4) множество возможных операций над объектами;
5) для каждой пары "субъект, объект" (s_i, o_j) множество разрешенных операций, являющееся подмножеством множества возможных операций.

Операции связаны с целевой функцией защищаемой системы, т.е. с назначением системы и решаемыми задачами.

Аксиомы защищенных АС

Аксиома 1

В защищенной АС всегда присутствует активный компонент (субъект), выполняющий контроль операций субъектов над объектами.

Этот компонент фактически отвечает за реализацию ПБ.

Аксиома 2

Для выполнения в защищенной АС операций над объектами необходима дополнительная информация и наличие содержащего ее объекта о разрешенных и запрещенных операциях субъектов с объектами.

Аксиома 3

Все вопросы безопасности информации в АС описываются доступами субъектов к объектам.

ПБ выражает нестационарное состояние защищенности. Защищенная система может изменяться, дополняться новыми компонентами. Следовательно, ПБ должна быть поддержана во времени, и в процессе изучения свойства защищаемой системы должны быть определены процедуры управления безопасностью. Нестационарность защищаемой АС, вопросы реализации политики безопасности в конкретных конструкциях защищаемой системы предопределяют необходимость рассмотрения задачи гарантирования заданной политики безопасности.

Итак, при рассмотрении политики безопасности необходимо решить 4 класса взаимосвязанных задач:

1) формулирование и изучение ПБ;
2) реализация ПБ;
3) гарантирование заданной ПБ;
4) управление безопасностью.

Кроме этого, важно помнить, что система защиты не самоцель и должна нести подчиненную функцию по сравнению с главной целью вычислительного процесса. Часто достигается снижение одной опасности за счет возрастания другой.

Результат решения задачи выбора правил распределения и хранения информации, а также обращения с информацией есть выбор ПБ. ПБ никогда не удовлетворит все стороны, участвующие во взаимодействии с защищаемой информацией.

Выбор ПБ – окончательное решение проблемы: что хорошо и что плохо. После принятия такого решения можно строить защиту, т.е. систему поддержки выполнения правил ПБ. Таким образом, построенная система защиты информации хорошая, если она надежно поддерживает выпол-

нение правил ПБ и наоборот. Такое решение проблем защищенности информации и построения системы защиты позволяет привлечь в теорию защиты точные математические методы, т.е. доказать, что данная система в заданных условиях поддерживает ПБ. В этом суть доказательного подхода к ЗИ, позволяющего говорить о "гарантированно защищенной системе". Смысл "гарантированной защиты" в том, что при соблюдении исходных условий заведомо выполняются все правила ПБ. Термин "гарантированная защита" впервые встречается в "Оранжевой книге" – стандарте МО США на требования к защищенным системам.

Определение. ***Политика безопасности*** – набор правил, норм и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Смысл ПБ – набор правил управления доступом.

Следует отметить отличие ПБ от НСД. Во-первых, ПБ определяет как разрешенные, так и неразрешенные доступы. Во-вторых, ПБ по своему определению конструктивна, может быть основой определения некоторого автомата для своей реализации.

Пример

ПБ учреждения. Цель защиты – обеспечение секретности информации. Политика безопасности: каждый пользователь использует только свои данные, без обмена с другими пользователями. Решение: каждый пользователь имеет свой персональный компьютер в персональной охраняемой комнате, куда не допускаются, кроме него, посторонние лица. Это тривиальная разграничительная (дискреционная) политика безопасности.

ПБ определяется неоднозначно, всегда связана с практической реализацией системы и механизмов защиты. Корректность в данных конкретных условиях должна быть доказана.

Построение ПБ соответствует следующим шагам:

1) в информацию вносится структура ценностей и проводится анализ риска;
2) определяются правила любого процесса пользования данным видом доступа к элементам информации, имеющим данную оценку ценностей.

Дискреционная политика (Discretionary Policy)

Дискреционная политика (или ее еще называют разграничительной политикой) – одна из самых распространенных в мире. В системах по умолчанию имеется в виду именно эта политика.

Пусть $\mathcal{O}$– множество объектов, S – множество субъектов, $S \subset \mathcal{O}$. $\mathcal{U}$ – множество пользователей, $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$. Введем отображение own:

$$\text{own}: \mathcal{O} \to \mathcal{U}.$$

Каждый объект объявляется собственностью соответствующего пользователя. Пользователь, являясь собственником объекта, имеет все права к нему, а иногда и право передачи прав другому пользователю.

Собственник объекта определяет права доступа других субъектов к объекту, т.е. политику безопасности в отношении данного объекта. Права, определяющие доступы субъекта s_i к объекту o_j, $i = 1,2,\ldots$, $j = 1,2,\ldots$, записываются в виде матрицы доступа с элементами подмножества множества доступов $\mathcal{R}$,.

Существует несколько способов задания матрицы доступов.

1. **Лист возможностей**. Для всех ^{S_i} создается файл всех объектов, к которым имеет доступ данный объект.
2. **Лист контроля доступа**. Для всех объектов создается список всех субъектов, имеющих право доступа к этому объекту.

	O_1	O_2	…	O_n	S_1	…	S_m
S_1	own r	w					
⋮							
S_m							

К сожалению, многих проблем защиты дискреционная политика решить не может. Например, разграничительная политика не выдерживает атак при помощи "троянского коня". Это значит, что система защиты, реализующая дискреционную политику, плохо защищает от проникновения в систему вирусов и других средств скрытого разрушающего воздействия. Матрица доступа для атаки типа "троянский конь" имеет следующий вид.

	O_1	O_2
u_1	own r, w	w
u_2		own r, w

Здесь u_1 – пользователь, u_2 – злоумышленник, o_1 – ценный объект, o_2 – программа с троянцем.

Следующая проблема дискреционной политики – автоматическое определение прав, а также проблема контроля распространения прав доступа.

Многоуровневая политика безопасности (политика MLS)

В повседневном секретном делопроизводстве госсектор России придерживается политики MLS.

Основами политики MLS являются решетка ценностей SC и понятие информационного потока. Пусть X, Y – произвольные объекты,

$$X \to_a Y -$$

информационный поток, где X – источник, Y – получатель информации. Кроме этого, пусть задано отображение c:

$$c : \mathcal{O} \to SC .$$

Если $c(Y) \geq c(X)$, то Y более ценно, чем X.

Определение. Политика MLS считает информационный поток $X \to_a Y$ ***разрешенным*** тогда и только тогда, когда $c(Y) \geq c(X)$ в решетке SC.

Политика MLS имеет дело с множеством информационных потоков в системе и делит их на разрешенные и неразрешенные простым условием. Однако информационных потоков в системе огромное количество, поэтому приведенное определение неконструктивно. Получим конструктивное определение на языке доступов.

Рассмотрим класс систем с двумя видами доступа: r и w. Другие виды доступа либо не определяют информационный поток, либо выражаются через r и w. Пусть процесс s в ходе решения своей задачи последовательно обращается к объектам $o_1, o_2, \ldots, o_n$. Некоторые из o_i могут возникнуть в ходе решения задачи. Пусть

$$s \xrightarrow{r} o_{i_1},\ s \xrightarrow{r} o_{i_2},\ \ldots,\ s \xrightarrow{r} o_{i_k},\ s \xrightarrow{w} o_{j_1},\ \ldots,\ s \xrightarrow{w} o_{j_{n-k}}.$$

При выполнении условий

$$c(s) \geq c(o_{i_t}),\ t = \overline{1,k}$$

соответствующие потоки информации будут идти в разрешенном политикой MLS направлении. При выполнении условий

$$c(s) \leq c(o_{j_t}),\ t = \overline{1,n-k}$$

потоки, определенные доступом w, будут также идти в разрешенном направлении. Таким образом, в результате выполнения задачи процессом s связанные с ним информационные потоки удовлетворяют политике MLS.

Такого качественного анализа достаточно для классификации процессов и принятия решения о соблюдении политики MLS. Если политика нарушается, то соответствующий доступ не разрешается.

Обратите внимание на то, что s может создать такой объект o, что $c(s) > c(o)$, но не может писать туда информацию. При передаче управления поток от s или к s прерывается, хотя другие процессы могут записывать или считывать информацию в/из s как из объекта.

Таким образом, получили управление потоками через контроль доступов.

Определение. В системе с двумя доступами r и w политика MLS определяется следующими правилами доступа:

$$X \xrightarrow{r} Y \Leftrightarrow c(X) \geq c(Y),$$

$$X \xrightarrow{w} Y \Leftrightarrow c(X) \leq c(Y).$$

Структура решетки помогает организации поддержки политики MLS. Пусть имеется последовательная цепочка информационных потоков:

$$o_1 \rightarrow_a o_2 \rightarrow_b o_3 \rightarrow_c \ldots \rightarrow_z o_k.$$

Если каждый из потоков разрешен, то разрешен сквозной поток $o_1 \rightarrow_a \ldots \rightarrow_z o_k$. Предлагается читателю доказать это утверждение в качестве упражнения.

В современных системах защиты политика MLS реализуется через мандатный контроль (мандатную политику). Мандатный контроль реализуется подсистемой защиты на самом низком аппаратном уровне. Это позволяет эффективно строить защищенную среду для механизма мандатного контроля.

Мандатный контроль реализуется следующим образом. Каждый объект o имеет метку с информацией о классе $c(o)$. Каждый субъект имеет аналогичную метку $c(s)$. Мандатный контроль сравнивает метки и удовлетворяет запрос субъекта s к объекту o на чтение, если $c(s) \geq c(o)$, и на запись, если $c(s) \leq c(o)$. Тогда мандатный контроль реализует политику MLS.

Следует отметить, что политика MLS устойчива к атакам типа "троянский конь". Предлагается читателю рассмотреть данную ситуацию самостоятельно.

Политика MLS создана для сохранения секретности информации. Вопросы целостности при помощи этой политики не решаются.

Политика целостности Биба (Biba)

Цель политики безопасности Биба – защита от нарушений целостности информации. При этом предполагается, что опасности для нарушения секретности не существует.

Пусть в информацию внесена решетка ценностей SC. Любой информационный поток $X \to_a Y$ может воздействовать на целостность Y и совершенно не воздействовать на целостность источника X. Если в Y более ценная информация, чем в X, то такой поток при нарушении целостности Y принесет более ощутимый ущерб, чем поток в обратном направлении от более ценного Y к менее ценному X.

Определение. В политике Биба информационный поток $X \to_a Y$ разрешен тогда и только тогда, когда $c(Y) \le c(X)$.

Определение. Для систем с доступом r и w политика Биба разрешает доступ в следующих случаях (рекомендуется обосновать данную эквивалентную формулировку):

$$X \xrightarrow{r} Y \Leftrightarrow c(X) \le c(Y),$$

$$X \xrightarrow{w} Y \Leftrightarrow c(X) \ge c(Y).$$

Для реализации политики Биба подходит мандатный контроль.

Доказательный подход к системам защиты

Пусть задана политика безопасности $\mathcal{P}$ Система защиты хорошая, если она поддерживает $\mathcal{P}$, и плохая в противном случае. Попытаемся ответить на вопрос: как определить надежность поддержки политики безопасности?

Обратимся к иерархической схеме. Пусть политика $\mathcal{P}$ выражена на языке $\mathcal{L}_1$, формулы которого определяются через услуги $U_1, U_2, \ldots, U_k$. Все субъекты $\mathcal{S}$ системы разбиты на два множества $\mathcal{S}_1$ и $\mathcal{S}_2$, $\mathcal{S}_1 \bigcup \mathcal{S}_2 = \mathcal{S}$, $\mathcal{S}_1 \bigcap \mathcal{S}_2 = \varnothing$. Все объекты, к которым может быть осуществлен доступ, разделены на два множества $\mathcal{O}_1$ и $\mathcal{O}_2$, $\mathcal{O}_1 \bigcup \mathcal{O}_2 = \mathcal{O}$, $\mathcal{O}_1 \bigcap \mathcal{O}_2 = \varnothing$. Политика безопасности $\mathcal{P}$ формулируется следующим образом: субъект s имеет доступ $\rho \in \mathcal{R}$ к объекту o тогда и только тогда, когда $s \in \mathcal{S}_i$, $o \in \mathcal{O}_i$, $i = 1,2$. Вычислим функции принадлежности:

$$I_x(A) = \begin{cases} 1, x \in A, \\ 0, x \notin A, \end{cases}$$

$$I_s(\mathcal{S}_1),\ I_s(\mathcal{S}_2),\ I_o(\mathcal{O}_1),\ I_o(\mathcal{O}_2).$$

Следующее логическое выражение соответствует политике безопасности:

$$F = \left(I_s(S_1) \wedge I_o(O_1)\right) \vee \left(I_s(S_2) \wedge I_o(O_2)\right).$$

Язык $\mathcal{L}_1$ опирается на услуги:

– вычисление $I_x(A)$;

– вычисление логического выражения F;

– вычисление: если $F = 1$, то доступ $s \xrightarrow{\rho} o$ разрешен, если $F = 0$, то доступ $s \xrightarrow{\rho} o$ запрещен.

Для поддержки услуг языку $\mathcal{L}_1$ требуется свой язык $\mathcal{L}_2$ и т.д.

Пусть услуги, описанные на языке $\mathcal{L}_2$, можно гарантировать. Тогда надежность выполнения политики $\mathcal{P}$ определяется полнотой ее описания в терминах услуг $U_1, U_2, \ldots, U_k$. Если $\mathcal{P}$ – формальная модель, т.е. язык $\mathcal{L}_1$ формально определяет правила политики $\mathcal{P}$, то можно доказать или опровергнуть утверждение о том, что множество предоставленных услуг полностью и однозначно определяет политику $\mathcal{P}$. Тогда более сложная задача сводится к более простой и к доказательству факта, что этих услуг достаточно для выполнения политики. Этот подход представляет метод анализа систем защиты, позволяющий выявлять слабости в проектируемых (существующих) системах.

К сожалению, проводить подобный анализ в каждой системе дорого, методика проведения анализа государственных систем – конфиденциальная информация. В связи с этим условия теорем, доказывающих поддержку политики безопасности, формулируют без доказательства в виде стандарта. Такой подход был впервые применен в США в 1983 году – открыто опубликованный проект стандарта по защите информации – "Оранжевая книга".

Пример гарантированно защищенной системы обработки информации

Определим модель Σ системы, оперирующей ценной информацией. Пусть время дискретно: $t \in N = \{1,2,\ldots\}$. Информация в Σ представлена в форме слов языка $\mathcal{L}$ над некоторым конечным алфавитом A. Вся информация о Σ в данный момент может быть представлена в виде состояний конечного множества объектов. Состояние Σ – набор состояний ее объектов. Объекты могут создаваться и уничтожаться. В связи с этим получается множество объектов системы Σ в момент t, обозначаемое $\mathcal{O}_t$, $|\mathcal{O}_t| < \infty$.

Для каждого t выделим в $\mathcal{O}_t$ подмножество субъектов S_t. Для любого субъекта $s \in S_t$ есть описание преобразования информации в системе Σ. Для реализации этого преобразования в Σ нужно выделить ресурсы (домен) и организовать определенное взаимодействие ресурсов, приводящее к преобразованию информации – процесс.

Каждый субъект может находиться в двух состояниях:

– в форме описания – неактивизированном;

– в форме (домен, процесс) – активизированном.

Активизировать субъект может только другой активизированный субъект. Для момента времени t на множестве S_t можно определить орграф Γ_t, где субъекты $s_1, s_2 \in S_t$ соединены дугой $s_1 \to s_2$ тогда и только тогда, когда в случае активизации субъекта s_1 возможна активизация субъекта s_2. Если в вершину s не входит ни одной дуги, то эта вершина определяет ***пользователя***.

Пусть в системе два пользователя u_1 и u_2. Они считаются активизированными по определению и могут активизировать другие субъекты. Условимся, что запись вида:

$$s_1 \xrightarrow{a} s_2,\ s_1, s_2 \in S_t$$

означает активизацию процессом s_1 субъекта s_2.

Предположение 1

Если субъект s активизирован в момент t, то существует единственный активизированный субъект $s' \in S_t$, который активизировал s. В момент $t = 0$ активизированы только пользователи.

Лемма 1

Если в данный момент t активизирован субъект s, то существует единственный пользователь u, от имени которого активизирован субъект s.

Другими словами, существует цепочка:

$$u \xrightarrow{a} s_1 \xrightarrow{a} s_2 \xrightarrow{a} \ldots \xrightarrow{a} s_k \xrightarrow{a} s,$$

Доказательство. Согласно предположению 1, существует единственный субъект s_k, активизировавший s. Если $s_k = u_1$ или $s_k = u_2$, то лемма доказана. Если $s_k \neq u_i$, $i = 1,2$, то существует единственный субъект s_{k-1}, активизировавший s_k. В силу конечности времени работы системы Σ и то-

го, что в момент $t = 0$ активизированы только пользователи, получаем в начале цепочки одного из них. На этом цепочка, согласно определению пользователя, обрывается. ♦

Предположение 1 требует единственности идентификации субъектов. Поэтому пусть каждый объект в системе имеет уникальное имя.

Кроме активизации существуют другие виды доступа. Пусть $\mathcal{R}$ – множество всех видов доступа, $|\mathcal{R}| < \infty$. Будем записывать множество доступов ρ, $\rho \subseteq \mathcal{R}$, активизированного субъекта s к объекту o следующим образом:

$$s \xrightarrow{\rho} o.$$

Рассмотрим промежуток времени $[t, t + k]$. Соответствующую ему цепочку

$$s \xrightarrow{a} s_1 \xrightarrow{a} s_2 \xrightarrow{a} \ldots \xrightarrow{a} s_k \xrightarrow{\rho} o$$

будем обозначать через

$$s \xrightarrow{\rho} {}^{*} o.$$

При этом нас не интересует, какую задачу решает система Σ. Мы моделируем функционирование системы последовательностью доступов.

Предположение 2

Функционирование системы Σ описывается последовательностью доступов множеств субъектов к множествам объектов в каждый момент времени $t \in N$.

В граф Γ_t добавим дуги $s \to o$, означающие возможность любого доступа субъекта s к объекту o в момент времени t в случае активизации s.

Введем в рассмотрение множество $\mathcal{D}_t(s)$:

$$\mathcal{D}_t(s) = \{o : s \to_* o \quad \text{в момент } t\},$$

где $s \to_* o$ означает возможность доступа к объекту o от имени s. Для любого момента времени t определены множества $\mathcal{D}_t(u_1)$ и $\mathcal{D}_t(u_2)$. Рассмотрим множество:

$$\mathcal{D} = \mathcal{D}_t(u_1) \cap \mathcal{D}_t(u_2),$$

фиксированное для всех моментов времени. Тогда

$$\mathcal{O}_t = \mathcal{D}_t(u_1) \cup \mathcal{D}_t(u_2)$$

$$\mathcal{O}_0 = \{u_1, u_2\} \cup \mathcal{D}.$$

Определение. Множество объектов $\mathcal{D}$ называется ***общими ресурсами системы***.

Средствами из $\mathcal{D}$ можно создавать и удалять объекты, возможно, не принадлежащие $\mathcal{D}$. И это тоже будет доступ.

Из объектов системы Σ построена подсистема, которая реализует доступы. Любое обращение s за доступом ρ к объекту o в эту подсистему начинается с запроса:

$$s \xrightarrow{\rho?} o.$$

Пусть субъект s порождает объект o. По лемме 1 следует, что существует единственный пользователь u, от имени которого активизирован субъект, создавший объект. $\mathcal{O}_t(u)$ – множество объектов из $\mathcal{O}_t$, которые породил u. Следовательно, $u \in \mathcal{O}_t(u)$.

Лемма 2

Для каждого момента времени $t \in N$, объекта $o \in \mathcal{O}_t$, $o \notin \mathcal{D}$, существует единственный пользователь u такой, что $o \in \mathcal{O}_t(u)$.

Доказательство. Так как $\mathcal{O}_0 = \{u_1, u_2\} \bigcup \mathcal{D}$, $o \in \mathcal{O}_t$, $o \notin \mathcal{D}$, то объект o порожден в момент времени τ, $0 < \tau \leq t$. Тогда в $\mathcal{O}_\tau$ существует активизированный субъект s, создавший o. Следовательно, существует единственный пользователь u, породивший o. ♦

Рассмотрим вопрос безопасности в системе. Если $r, w \in \mathcal{R}$, то ограничимся опасностью утечки информации через каналы по памяти, возникающие при доступах к объектам. Таким каналом может быть следующая последовательность доступов при $\tau < t$:

$u_i \xrightarrow{w} o$ в момент времени τ, $u_j \xrightarrow{r} o$ в момент времени t, $i \neq j$.

При определенных условиях может оказаться опасным доступ от имени пользователя:

$u_i \xrightarrow{w} * o$ в момент времени τ, $u_j \xrightarrow{r} * o$ в момент времени t, $i \neq j$.

Если будем считать неблагоприятными доступы $\rho_1, \rho_2 \in \mathcal{R}$ вида

$$u_i \xrightarrow{\rho_1} * o,\ u_j \xrightarrow{\rho_2} * o,\ i \neq j, \qquad (2)$$

то исчерпаем возможные каналы по памяти.

Предположение 3

Если $o \in \mathcal{D}$, то доступы вида (2) при любых ρ_1, ρ_2 не могут создать канал утечки.

Это означает, что нельзя отразить ценную информацию в объектах общего доступа.

Тогда в (2) ограничиваемся объектами, не лежащими в $\mathcal{D}$. Таким образом, в системе считаются неблагоприятными доступы вида:

$$\exists t, \exists \rho \subseteq \mathcal{R}, \rho \neq \varnothing, \exists u_i, \exists o \in \mathcal{O}_t,$$

$$u_i \xrightarrow{\rho} * o,\ o \in \mathcal{O}_t(u_j),\ i \neq j. \qquad (3)$$

Другими словами, это доступ от имени пользователя к объекту, созданному другим пользователем. Такие доступы называется ***утечкой информации***.

Предположение 4

Если $s \in \mathcal{D}$ активизирован от имени пользователя u_2 ($u_1 \xrightarrow{a} * s$), в момент времени t субъекту s предоставлен доступ к объекту o, то

либо $o \in \mathcal{D}$;

либо $o \in \mathcal{O}_t(u_i)$;

либо система прекращает работу.

Определим политику безопасности.

Если происходит запрос на доступ $s \xrightarrow{\rho?} o$, то при $s, o \in \mathcal{O}_t(u)$ доступ $s \xrightarrow{\rho} o$ разрешается, а при $s \in \mathcal{O}_t(u_i)$, $o \in \mathcal{O}_t(u_j)$, $i \neq j$ доступ $s \xrightarrow{\rho} o$ невозможен.

Теорема 1

Пусть в построенной системе выполняются предположения 1–4. Если все доступы осуществляются в соответствии с политикой безопасности, то утечка вида (3) невозможна.

Доказательство. Предположим противное:

$$\exists t, \exists \rho \subset \mathcal{R}, \rho \neq \varnothing, \exists u_i, \exists o \in \mathcal{O}_t, u_i \xrightarrow{\rho} * o,\ o \in \mathcal{O}_t(u_j),\ i \neq j.$$

Пусть $s_1, \ldots, s_n$ – активизированные субъекты, имеющие доступы $\beta_i \supseteq \rho$, $i = \overline{1,n}$ к объекту o в момент времени t. По лемме 2 множество этих субъектов разбивается на три непересекающихся множества:

$$A = \{s_k : s_k \in \mathcal{D}\};$$

$$B = \{s_k : s_k \in \mathcal{O}_t(u_i)\};$$
$$C = \{s_k : s_k \in \mathcal{O}_t(u_j),\ i \neq j\}.$$

По лемме 1 для любого s_k существует единственный пользователь, от имени которого активизирован субъект s_k. Если $s_k \in A$, то по предположению 4 и условию теоремы 1 доступ $s_k \xrightarrow{\beta_k} o$ разрешен. Следовательно, s_k активизирован от имени u_j, а это противоречит предположению. Если $s_k \in B$, то доступ $s_k \xrightarrow{\beta_k} o$ невозможен согласно политике безопасности. ♦

Определим множество условий, реализованных в системе Σ, таких, что можно доказать теорему о достаточности выполнения этих условий для реализации правил политики безопасности.

Условие 1. Идентификация и аутентификация.

Если для любых t, $\rho \subseteq \mathcal{R}$, $s, o \in \mathcal{O}_t$ происходит запрос на доступ $u_i \xrightarrow{\rho?} o$, то вычислены функции принадлежности s и o к множествам $\mathcal{O}_t(u_1)$, $\mathcal{O}_t(u_2)$, $\mathcal{D}$.

Условие 2. Разрешительная подсистема.

Если $s \in \mathcal{O}_t(u_i)$, $o \in \mathcal{O}_t(u_j)$, происходит запрос на доступ $s \xrightarrow{\rho?} o$, то при $i = j$ доступ $s \xrightarrow{\rho} o$ разрешается, а при $i \neq j$ доступ $s \xrightarrow{\rho} o$ запрещается.

Условие 3. Отсутствие обходных путей политики безопасности.

Если субъект s, активизированный к моменту времени t, получил в момент времени t доступ $s \xrightarrow{\rho} o$, то в момент времени t произошел запрос на доступ $s \xrightarrow{\rho?} o$ при любых t, $\rho \subseteq \mathcal{R}$.

Теорема 2

Если в построенной системе Σ выполняются предположения 1–4 и условия 1–3, то выполняется политика безопасности.

Показательство теоремы следует из следующих утверждений:

1) если для произвольного доступа $\rho \subset \mathcal{R}$ происходит запрос на доступ $s \xrightarrow{\rho?} o$, $s \in \mathcal{O}_t(u_i)$, $o \in \mathcal{O}_t(u_i)$, то доступ разрешен;
2) если же $s \in \mathcal{O}_t(u_i)$, $o \in \mathcal{O}_t(u_j)$, $i \neq j$, то такой доступ в момент времени t невозможен.

Докажем первое утверждение. Если происходит запрос на доступ $s \xrightarrow{\rho?} o$, то по условию 1 вычислены функции принадлежности и определено, что $s \in \mathcal{O}_t(u_i)$, $o \in \mathcal{O}_t(u_j)$. Если $i = j$, то выполнено условие 2 и доступ разрешен.

Докажем второе утверждение. Если происходит запрос на доступ $s \xrightarrow{\rho?} o$, $s \in \mathcal{O}_t(u_i)$, $o \in \mathcal{O}_t(u_j)$, $i \neq j$, то по условию 2 доступ $s \xrightarrow{\rho} o$ невозможен. Если доступ $s \xrightarrow{\rho} o$ происходит в обход запроса $s \xrightarrow{\rho?} o$ и субъект s активизирован, то получаем противоречие условию 3. Если субъект s не активизирован, то наличие доступа $s \xrightarrow{\rho} o$ противоречит условию доступа. ♦

Критерии оценки безопасности компьютерных систем Министерства обороны США ("Оранжевая книга")

"Критерии оценки безопасности компьютерных систем" (Trusted Computer System Evaluation Criteria – TCSEC, "Orange Book" – "Оранжевая книга") были разработаны и опубликованы Министерством обороны США в 1983 году, а приняты в качестве стандарта в 1985 году. В данном документе было впервые формально определено понятие «политика безопасности». Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

Общая структура

"Оранжевая книга" (ОК) предназначается для следующих целей.

1. Предоставить стандарт на средства безопасности, удовлетворяющие требованиям гарантированной защищенности для использования при обработке конфиденциальной информации.
2. Предоставить метрику для оценки защищенности ЭСОД. Предлагается два вида оценки: без учета среды, в которой работает техника, и в конкретной среде (аттестация).

3. Обеспечить базу для исследования требований к выбору защищенных систем.

Во всех документах, связанных с ОК, принято одно понимание обеспечения безопасности информации, которое принимается в качестве аксиомы.

Аксиома

ЭСОД называется безопасной, если она обеспечивает контроль за доступом к информации так, что только надлежащим образом уполномоченные лица или процессы, который функционируют от их имени, имеют право читать, писать, создавать или уничтожать информацию.

Безопасность = контроль за доступом.

Введем ряд определений.

Определение. ***Политика безопасности*** – набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации.

Определение. ***Идентификация*** – распознаваниє имени объекта. Идентифицируемый объект есть однозначно распознаваемый.

Определение. ***Аутентификация*** – подтверждение того, что предъявленное имя соответствует объекту.

Определение. ***TCB*** (Trusted Computing Base) – совокупность механизмов защиты в вычислительной системе, которые отвечают за поддержку ПБ.

Определение. ***Аудит*** (отслеживание) – регистрация событий, позволяющая восстановить и доказать факт их происшествия.

В ОК предложены три категории требований безопасности: политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности, вытекающих из Аксиомы. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, два последних – на качество средств защиты. Сформулируем эти требования.

I. Политика безопасности.
   1. Политика обеспечения безопасности – необходимо иметь явную и хорошо определенную политику обеспечения безопасности.
   2. Маркировка – метки, управляющие доступом, должны быть установлены и связаны с объектами.

II. Подотчетность.
   3. Идентификация – субъекты индивидуально должны быть идентифицированы.

4. Подотчетность – аудиторская информация должна селективно храниться и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

III Гарантии.

5. Гарантии – вычислительная система в своем составе обязана иметь аппаратно-программные механизмы, допускающие независимую оценку для получения достаточного уровня гарантий того, что система обеспечивает выполнение изложенных выше требований с 1 по 4.
6. Постоянная защита – гарантированно защищенные механизмы, реализующие указанные базовые требования должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

Классы защищенности компьютерных систем

ОК предусматривает 4 группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Каждая группа включает один или несколько классов. Группы D и A содержат по одному классу (классы D и A соответственно), группа C – классы C1 и C2, а группа B три класса – B1, B2, B3, характеризующиеся различными наборами требований защищенности. Уровень защищенности возрастает от группы D к группе A, а внутри группы – с увеличением номера класса. Усиление требований осуществляется с постепенным смещением акцентов от положений, определяющих наличие в системе каких-то определенных механизмов защиты, к положениям, обеспечивающим высокий уровень гарантий того, что система функционирует в соответствии с требованиями политики безопасности. Например, по реализованным механизмам защиты классы B3 и A1 идентичны (см. таблицу).

Таблица

Базовые требования ОК	Классы защищенности					
	C1	C2	B1	B2	B3	A1
Политика безопасности						
Дискреционная ПБ	+	+	+	=	=	=
Мандатная ПБ	–	–	+	+	=	=
Метки секретности	–	–	+	+	=	=
Целостность меток	–	–	+	=	=	=
Рабочие метки	–	–	–	+	=	=
Повторение меток	–	–	+	–	=	=
Освобождение ресурсов при повторном использовании объектов	–	+	=	+	=	=
Изолирование модулей	–	+	=	=	=	=

Пометка устройств ввода/вывода	–	–	+	=	=	=
Пометка читаемого вывода	–	–	+	=	=	=
Подотчетность						
Идентификация и аутентификация	+	+	=	–	=	=
Аудит	–	+	+	+	+	=
Защищенный канал	–	–	–	+	=	=
Гарантии						
Проектная спецификация и верификация	–	–	+	+	+	+
Системная архитектура	+	=	=	+	+	=
Целостность системы	+	=	=	=	=	=
Тестирование системы безопасности	+	+	+	+	+	=
Доверенное восстановление после сбоев	–	–	–	–	+	=
Управление конфигурацией системы	–	–	–	+	+	+
Доверенное дооснащение системы	–	–	–	+	+	=
Доверенное распространение	–	–	–	–	+	=
Анализ скрытых каналов	–	–	–	+	+	+
Документация						
Руководство пользователя	+	=	=	=	=	=
Руководство по конфигурированию системы защиты	+	+	+	+	+	=
Документация по тестированию	+	=	=	=	=	+
Проектная документация	+	=	+	+	=	+
Обозначения: – нет требований к данному классу; + новые или дополнительные требования; = требования совпадают с требованиями предыдущего класса						

Класс D. Минимальная защита.

Класс C1. Защита, основанная на разграничении доступа (DAC).

Класс C2. Защита, основанная на управляемом контроле доступом.

Класс B1. Мандатная защита, основанная на присваивании меток объектам и субъектам, находящимся под контролем TCB.

Класс B2. Структурированная защита.

Класс B3. Домены безопасности.

Класс A1. Верифицированный проект.

Выбор класса защиты

Выбор требуемого класса безопасности систем определяется следующими основными факторами, характеризующими условия работы системы:

1) безопасность режима функционирования системы;
2) основой для выбора класса защиты является индекс риска, определяющий минимальный требуемый класс.

Различают пять режимов функционирования системы:

а) режим, в котором система обрабатывает ценную информацию одного класса в окружении, которое обеспечивает безопасность для работы с этим классом;

б) режим особой секретности самой системы. Все пользователи и элементы системы имеют один класс и могут получать доступ к любой информации. В рамках данного режима обрабатывается информация высших грифов секретности;

в) многоуровневый режим. Система обрабатывает информацию двух и более уровней секретности, и не все пользователи имеют допуск ко всем уровням обрабатываемой информации;

г) контролирующий режим. Это многоуровневый режим обработки информации, при котором нет полной гарантии защищенности ТСВ;

д) режим изолированной безопасности. Данный режим позволяет изолированно обрабатывать информацию различных классов или классифицированную и неклассифицированную.

Отобразим классы секретности в числа, например, U–0, C–1, S–2, TS–3. Определим $R_{\min}$ – минимальный уровень допуска пользователя в системе, $R_{\max}$ – максимальный класс ценности информации, присутствующий в системе. Индекс риска можно определить следующим образом:

$$RI = R_{\max} - R_{\min}.$$

В случае, когда $R_{\min} \geq R_{\max}$, полагают: $RI = 1$, если есть категории, к которым кто-либо из пользователей не имеет доступа, и $RI = 0$ в противном случае.

Если система функционирует в окружении, которое можно назвать «безопасным периметром», то требования к минимальным классам защиты можно сделать значительно ниже.

Свое дальнейшее развитие стандарт TCSEC получил в работах [6–11], которые доступны в электронной библиотеке кафедры БИС и на сайте http://www.ssu.samara.ru/~is.

Библиографический список

1. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Изд-во агентства «Яхтсмен». 1996. – 192 с.
3. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему? / Под ред. П.Д. Зегжды и В.В. Платонова – СПб.: Мир и семья, 1997. 312 с.
4. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. Технология создания безопасных систем/ Под ред. П.Д. Зегжды и В.В. Платонова – СПб.: Мир и семья, 1998. 256 с.
5. Trusted Computer System Evaluation Criteria. US Department of Defense. CSC-STD-001-83, Aug. 1983.
6. Trusted Network Interpretation. National Computer Security Center. NCSC-TG-005 Version 1, July 1987.
7. Trusted Database Management System Interpretation. National Computer Security Center. NCSC-TG-021 Version 1, April 1991.
8. A Guide to Understanding Discretionary Access Control in Trusted Systems. National Computer Security Center. NCSC-TG-003 Version 1, September 1987.
9. Password management guideline. US Department of Defense. CSC-STD-002-85, April 1985.
10. Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments. US Department of Defense. CSC-STD-003-85, June. 1985
11. A Guide to Understanding Configuration Management in Trusted Systems. National Computer Security Center. NCSC-TG-006-88, March 1988.

Оглавление