**Лабораторная работа № 3**

**Применение методов и моделей политик информационной безопасности**

**Цель занятия:** получить навыки для оценки состояния организационных методов защиты информации, а также методов, базирующихся на программных решениях защиты данных в организации.

**1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

Одним из действенных организационных методов внедрения результатов АИБ является разработка и выполнение требований политики информационной безопасности (ПИБ).

ПИБ – это совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности

Существует ряд **моделей** политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. К числу их основных видов относятся:

- дискреционная (избирательная) политика безопасности;

- мандатная (полномочная) политика безопасности;

- политика безопасности информационных потоков;

- политика ролевого разграничения доступа;

- политика изолированной программной среды.

**Дискреционная (избирательная) политика** (DAC; Discretionary Access Control) является одной из самых простых и распространенных моделей политик безопасности. Она подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;

- права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Пусть: *О* – множество объектов,

*U* – множество пользователей,

*S* – множество действий пользователей над объектами.

Дискреционная политика определяет отображение  (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект  объявляется собственностью соответствующего пользователя , который может выполнять над ними определенную совокупность действий , в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Для описания свойств избирательного управления доступом применяется модель системы на основе **матрицы доступа** (МД, иногда ее называют **мат­рицей контроля** **доступа**). Такая модель получила название *матричной.*

Матрица доступа представляет собой матрицу, в которой объекту систе­мы соответствует столбец, а субъекту – строка. На пересечении *j* – го стол­бца и *i* – ой стро­ки матрицы располагается элемент *Sij* – множество разрешенных действий *j*-ого пользователя над *i*-ым объектом.

Об­ыч­но выделяют такие типы доступа субъекта к объек­ту как "чте­ние", "запись", "модификация", "исполнение" и др. Множество объектов и типа доступа к ним субъекта может изменяться в соот­ветствии с некоторыми правилами, существующими в данной системе. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата – зависимое условие), часы (время – зависимое условие), в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передавать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение на доступ субъек­та к объек­ту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно, дискреционное управление доступом реализует принцип *"что не разрешено, то запрещено",* предполагающий явное разрешение доступа субъек­та к объек­ту.

*Пример1*

*Пусть имеем множество из 4 пользователей {Администратор, Гость, Пользователь\_1, Пользователь\_2} и множество из 4 объектов {Файл\_1, Файл\_2, CD-RW, Дисковод}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}.*

*Действие «Полные права» разрешает выполнение всех перечисленных 3 действий, Действие «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом.*

*Таблица 1*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Объект / Субъект* | *Файл\_1* | *Файл\_2* | *CD-RW* | *Дисковод* |
| *1(Администратор)* | *Полные права* | *Полные права* | *Полные права* | *Полные права* |
| *2 (Гость)* | *Запрет* | *Чтение* | *Чтение* | *Запрет* |
| *3 (Пользователь\_1)* | *Чтение, передача прав* | *Чтение, запись* | *Полные права* | *Полный запрет* |
| *4 (Пользователь\_2)* | *Чтение, запись* | *Чтение, запись* | *Запрет* | *Запрет* |

*Например, Пользователь\_1 имеет права на чтение и запись в Файл\_2. Передавать же свои права другому пользователю он не может.*

*Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом, пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.*

*Например, если Пользователь\_1 передает право доступа к Файлу\_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла\_1.*

Матрица доступа – наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных автоматизированных систем обработки информации.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД (профили и т.д.). Каждый из этих способов представления МД имеет свои достоинства и свои недостатки, обуславливающие область их применения.

Избирательная (дискреционная) политика безопасности наиболее широко применяется в ко­м­­мерческом секторе, так как она имеет относительно простую систему разграничения прав доступа, ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные ра­с­ходы.

К *недостаткам* дискреционной политики безопасности можно отнести статичность определенных в ней правил разграничения доступа, что не позволяет реализовать ясную и четкую систему защиты информации в ИКС.

**Мандатная (полномочная) политика** безопасности (Mandatory Access Control; MAC) имеет в своей основе идею полномочного управления доступом *с использованием меток безопасности*, которая подразумевает, что:

1. все субъекты и объекты системы должны быть однозначно идентифи­ци­рованны;
2. каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;
3. каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Другими словами, в данной модели каждому субъекту приписывается *уровень допуска* (форма допуска), а каждому объекту – *уровень конфиденциальности* (гриф секретности).

Мандатную модель можно определить следующей группой аксиом:

1. Имеется множество атрибутов безопасности. В качестве таких атрибутов достаточно часто используется следующее множество: {«Совершенно секретно», «Секретно», «Для служебного пользования», «Открытые данные»}.
2. Каждому объекту компьютерной системы присваивается определенный атрибут безопасности, который соответствует его ценности.
3. Каждому субъекту присваивается определенный атрибут безопасности, который определяет уровень его допуска. Он равен максимальному из атрибутов безопасности объектов, к которому субъект будет иметь доступ.

Если субъект *Ui*∈*U* имеет атрибут *Ai*, то он будет иметь доступ ко всем объектам, у которых уровень секретности (атрибут безопасности) будет меньше, либо равен *Ai*.

При реализации мандатной модели политики безопасности, как правило, существует два вектора:

- вектор , задающий *уровни конфиденциальности* для всех объектов компьютерной системы (*n* – количество объектов);

- вектор , задающий *уровни допуска* для всех субъектов в компьютерной системе (*m* – число субъектов).

Модуль защиты при осуществлении доступа субъекта к объекту сравнивает уровень допуска субъекта с уровнем конфиденциальности объекта и по результатам сравнения разрешает либо запрещает данный доступ. Доступ разрешается, если уровень допуска субъекта больше либо равен уровня конфиденциальности объекта. В ином случае, доступ запрещается. То есть фактически информация может передаваться только "наверх": субъект может читать содержимое объекта, если его текущий уровень допуска не ниже метки конфиденциальности объекта, и записывать в него, - если не выше

В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реа­ли­зовать иерархически не нисходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка конфиденциальности. Поэтому наиболее защищенными ока­­­­­­­зы­ваются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулиро­вание доступа субъектов системы к объектам с различным уровнем допуска и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с ниж­них уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности). Имеет более высокую степень надежности по сравнению с дискреционной политикой безопасности.

К *недостаткам* мандатной политики безопасности относится то, что она довольно сложна и требует значительных ресурсов компьютерной системы.

**Политика безопасности информационных потоков** основана на разделении всех возможных информационных потоков между объектами системы на два непересекающихся множества: множества благоприятных информационных потоков и множества неблагоприятных информационных потоков. Задачей такой политики является обеспечение невозможности возникновения в ИКС неблагоприятных информационных потоков. Реализация политики безопасности информационных потоков часто затруднена. Используется в сочетании с политикой другого вида.

**Политика ролевого разграничения доступа** представляет собой развитие политики дискреционного разграничения доступа. При этом права доступа субъектов системы на объекты группируются по определенным правилам, с учетом специфики их применения, образуя роли. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования ИКС правила разграничения доступа. Может быть объединено с мандатным разграничением доступа.

**Политика изолированной программной среды** реализуется с целью определения порядка безопасного взаимодействия субъектов системы, обеспечивающего невозможность воздействия на систему защиты ИКС и модификации ее параметров или конфигурации и, следовательно, невозможность изменения политики разграничения доступа. Реализуется путем изоляции субъектов системы друг от друга и путем контроля порождения новых субъектов. Таким образом, в системе могут быть активными только субъекты из заранее предопределенного списка.

**2 ЗАДАНИЯ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ**

**Задание 1.**

1. Выбрать из таблицы 1 организацию (взять по номеру в журнале группы) и составить для нее примерную функциональную модель IDEF0 процесса обеспечения ИБ, отражающую точку зрения специалиста по ИБ.

Таблица 1 – Перечень предметных областей

|  |  |  |  |
| --- | --- | --- | --- |
| №  вар. | **Предметная область** | №  вар. | **Предметная область** |
| 1 | Фирма, занимающаяся рекламной деятельностью | 16 | Фирма, занимающаяся разработкой программного обеспечения |
| 2 | Фирма, реализующая грузовые перевозки | 17 | Фирма по внедрению новых информационных технологий |
| 3 | Туристическая фирма | 18 | Салон красоты |
| 4 | Фирма, организующая услуги по ремонту квартир и офисов | 19 | Фирма, занимающаяся созданием алиби для частных лиц |
| 5 | Фитнес-центр | 20 | Кредитная организация |
| 6 | Брачное агентство | 21 | Салон кухонной мебели |
| 7 | Станция тех. обслуживания легковых автомобилей | 22 | Фирма, занимающаяся подбором и продажей легковых автомобилей |
| 8 | Фирма, занимающаяся реализацией коммерческой недвижимости | 23 | Фирма, занимающаяся консалтинговой деятельностью в области развития бизнеса |
| 9 | Фирма, занимающаяся разработкой дизайна квартир | 24 | Фирма, занимающаяся реализацией не элитного жилья |
| 10 | Фирма, занимающаяся реализацией элитного жилья | 25 | Фирма, организующая экстремальный туризм |
| 11 | Агентство по трудоустройству | 26 | Магазин по продаже компьютеров |
| 12 | Фирма, предоставляющая охранные услуги | 27 | Магазин по продаже бытовой техники |
| 13 | Фирма по оценке недвижимости | 28 | Салон продажи мотоциклов |
| 14 | Фирма, предоставляющая услуги по защите информации | 29 | Фирма, занимающаяся разработкой проектов жилых загородных домов |
| 15 | Фирма, занимающаяся подготовкой и проведением праздничных мероприятий и досуга | 30 | Фирма, организующая охоту для состоятельных клиентов |

1. Разработать документ, отражающий ПИБ для заданной организации учитывающий содержание построенной функциональной модели. При выполнении этого пункта рекомендуется пользоваться шаблоном документов по ИБ «Политика информационной безопасности» (там их два – можно взять любой), адаптируя их под свою организацию. Шаблоны доступны на сайте «Шаблоны типовых документов по информационной безопасности» (пролистать по алфавиту до буквы «П») по адресу: <http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B> Следует иметь ввиду, что в документе «Политика информационной безопасности» могут быть несколько разделов – проверить, на сколько разработанная в 1 п. модель соответствует названиям разделов. При целесообразности, на ваше усмотрение, скорректируйте модель из 1п. или обоснуйте, почему этот раздел можно исключить для рассматриваемой организации.
2. Составить должностную инструкцию начальника отдела информационной безопасности для своей организации, адаптировав соответствующий шаблон с сайта «Шаблоны типовых документов по информационной безопасности».

**Задание 2.**

На основании данных о количестве пользователей и объектов компьютерной системы (приложение А), соответственно Вашему варианту, разработать матрицу доступа пользователей к объектам компьютерной системы

* 1. Разработать блок-схему программы создающей матрицу доступа пользователей к объектам компьютерной системы. Разработатьпрограммный модуль (в любой среде программирования), создающий матрицу доступа пользователей к объектам компьютерной системы. Модуль должен:
  2. - обеспечивать выбор идентификаторов пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам).
     1. - заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно варианту. При заполнении матрицы доступа необходимо учесть, что один из пользователей должен являться администратором системы (например, пользователь Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные. Права остальных пользователей для доступа к объектам компьютерной системы могут быть заполнены случайным образом вручную или с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учесть, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.
  3. - при запуске модуля должен запрашиваться идентификатор пользователя (должна проводиться идентификация пользователя). При успешной идентификации пользователя должен осуществляться вход в систему. При неуспешной – выводиться соответствующее сообщение: «Пользователь с данным именем не зарегистрирован в системе».
  4. - при входе в систему после успешной идентификации пользователя, на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, в виде следующей экранной формы:

*User: Boris*

*Идентификация прошла успешно, добро пожаловать в систему*

*Перечень Ваших прав:*

*Объект1: Чтение*

*Объект2: Запрет*

*Объект3: Чтение, Запись, Удаление*

*Объект4: Полные права*

*Жду ваших указаний >*

После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant), должна модифицироваться матрица доступов. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

*Жду ваших указаний > read*

*Над каким объектом производится операция? 1*

*Операция прошла успешно*

*Жду ваших указаний > write*

*Над каким объектом производится операция? 2*

*Отказ в выполнении операции. У Вас нет прав для ее осуществления*

*Жду ваших указаний > grant*

*Право на какой объект передается? 3*

*Отказ в выполнении операции. У Вас нет прав для ее осуществления*

*Жду ваших указаний > grant*

*Право на какой объект передается? 4*

*Какое право передается? read*

*Какому пользователю передается право? Ivan*

*Операция прошла успешно*

*Жду ваших указаний > quit*

*Работа пользователя Boris завершена. До свидания.*

*User:*

Приложение А

Таблица А1

|  |  |  |
| --- | --- | --- |
| Вариант | Количество субъектов доступа (пользователей) | Количество объектов доступа |
| 1 | 3 | 3 |
| 2 | 4 | 4 |
| 3 | 5 | 4 |
| 4 | 6 | 5 |
| 5 | 7 | 6 |
| 6 | 8 | 3 |
| 7 | 9 | 4 |
| 8 | 10 | 4 |
| 9 | 3 | 5 |
| 10 | 4 | 6 |
| 11 | 5 | 3 |
| 12 | 6 | 4 |
| 13 | 7 | 4 |
| 14 | 8 | 5 |
| 15 | 9 | 6 |
| 16 | 10 | 3 |
| 17 | 3 | 4 |
| 18 | 4 | 4 |
| 19 | 5 | 5 |
| 20 | 6 | 6 |
| 21 | 7 | 3 |
| 22 | 8 | 4 |
| 23 | 9 | 4 |
| 24 | 10 | 5 |
| 25 | 3 | 6 |
| 26 | 4 | 3 |
| 27 | 5 | 4 |
| 28 | 6 | 4 |
| 29 | 6 | 5 |
| 30 | 8 | 6 |

**Лабораторная работа № 4**

**Задание 1. Изучение возможностей и приемов работы с программой Crystal Security (**[**http://www.crystalsecurity.eu/**](http://www.crystalsecurity.eu/) **)**

Программы Crystal Security. - это облачная система, которая обнаруживает и удаляет вредоносные программы с вашего компьютера. Его технология обеспечивает быстрое обнаружение вредоносных программ и позволяет вам узнать об изменениях на вашем компьютере в режиме реального времени.

Облако Crystal Security собирает данные из миллионов участвующих систем пользователей по всему миру, чтобы защитить вас от самых последних вирусов и вредоносных атак. Облачное обнаружение вредоносных программ, простой в использовании, удобный интерфейс, автоматические / ручные обновления, отсутствие инсталляции, поддержка нескольких языков и многие другие функции.

В процессе выполнения задания запустить сервис на виртуальной машине и осуществить обнаружение вредоносных программ (если виртуальной машины нет, то ограничится ознакомлением с возможностями программы).

**Задание 2. Восстановлению файлов с помощью FileScavenger.**

File Scavenger – универсальная утилита восстановления, которая работает со всеми известными типами файлов. Поддерживает файловые системы, совместимые с Windows: NTFS, FAT16 и FAT32. Работает на всех современных версиях ОС Windows, от XP до Windows 10.

Бесплатно можно скачать демонстрационную версию программы, у которой одно, но чрезвычайно важное ограничение – невозможность восстановить свыше 64 Кб. То есть у файла будет восстановлен только этот объем, остальные данные не сохранятся. Этого хватит, чтобы вернуть полностью небольшой документ Word (около 10 страниц) без таблиц или графиков. Чтобы восстановить весь объем, нужно скачать программу и купить лицензию.

**В процессе выполнения**  задания стереть несколько файлов на флешке и попытаться их восстановить с поимощью данной программы.

**Порядок восстановления**

File Scavenger отличается простым интерфейсом. Главное окно поделено на два раздела – Scan и Save. Чтобы разобраться, как пользоваться ими, подробная инструкция не нужна, однако небольшое руководство не помешает.











