**МИНОБРНАУКИ РОССИИ**

**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**

**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**

**Кафедра ИБ**

**ОТЧЕТ**

**по практической работе №2**

**по дисциплине «Технология разработки ИС в ЗИ»**

**ТЕМА: Разработка матрицы доступа к ресурсам ИС**

|  |  |  |
| --- | --- | --- |
| Студенты гр. 3361 |  | Воловик П. А. |
|  |  | Столетов А. С. |
|  |  | Субботин Д.А |
| Преподаватель |  | Березин А.Н. |

Санкт-Петербург

2018

**Цель работы.**

Получить практические навыки разработки матрицы доступа и заполнения ее в соответствии с существующими требованиями.

Теоретические сведения. Выделяют следующие типы управления доступом (УПД):

1. Дискреционное управление доступом – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.
2. Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности

Дискреционное разграничение доступа, DAC (Discretionary Access Control) характеризуется следующим набором свойств:

1. все субъекты и объекты компьютерной системы должны быть однозначно идентифицированы;
2. для любого объекта компьютерной системы определен пользователь-владелец;
3. владелец объекта обладает правом определения прав доступа к объекту со стороны любых субъектов компьютерной системы;
4. в компьютерной системе существует привилегированный пользователь, обладающий правом полного доступа к любому объекту (или правым становиться владельцем любого объекта).

Достоинства:

1. простая реализация проверка прав доступа субъекта к объекту производится в момент открытия этого объекта;
2. хорошая изученность в наиболее распространенных операционных системах универсального назначения типа Microsoft Windows и Unix применяется именно эта модель разграничения доступа.

Недостатки:

1. статичность разграничения доступа – права доступа к уже открытому субъектом объекту в дальнейшем не изменяются независимо от изменения состояния компьютера;
2. не существует возможности проверки, не приведет ли разрешение доступа к объекту для некоторого субъекта к нарушению безопасности информации в компьютерной системе.

Мандатное разграничение доступа, MAC (Mandatory Access Control) характеризуется следующим набором свойств:

* 1. все субъекты и объекты компьютерной системы должны быть однозначно идентифицированы;
  2. имеется линейно упорядоченный набор меток конфиденциальности и соответствующих им уровней (степеней) допуска;
  3. каждому объекту компьютерной системы присвоена метка конфиденциальности;
  4. каждому субъекту компьютерной системы присваивается степень допуска;
  5. в компьютерной системе существует привилегированный пользователь, имеющий полномочия на удаление любого объекта системы;
  6. понизить метку конфиденциальности объекта может только субъект, имеющий доступ к данному объекту и обладающий специальной привилегией;
  7. право на чтение информации из объекта получает только тот субъект, чья степень допуска не меньше метки конфиденциальности данного объекта (правило «не читать выше»);
  8. право на запись информации в объект получает только тот субъект, чей уровень конфиденциальности не больше метки конфиденциальности данного объекта (правило «не записывать ниже»).

Достоинства:

1. более высокая надежность работы самой компьютерной системы, так как при разграничении доступа к объектам контролируется и состояние самой системы, а не только соблюдение установленных правил;
2. большая простота определения правил разграничения доступа по сравнению с дискреционным разграничением (эти правила более ясны для разработчиков и пользователей компьютерной системы).

Недостатки:

1. сложность программной реализации;
2. снижение эффективности работы компьютерной системы, так как проверка прав доступа субъекта к объекту выполняется не только при открытии
3. объекта, но и перед выполнением любой операции чтения из объекта или записи в объект;
4. создание дополнительных неудобств работе пользователей компьютерной системы, связанных с невозможностью изменения информации в не-конфиденциальном объекте, если тот же самый процесс использует информацию из конфиденциального объекта (его уровень конфиденциальности больше нуля).

Ролевое разграничение доступа, RBAC (Role-Based Access Control) характеризуется следующим набором свойств:

1. сотрудники выполняют определенные функциональные обязанности не от своего имени, а в рамках некоторой занимаемой ими должности (роли)
2. реализация ролевого разграничения доступа требует разработки набора ролей, определяемых как набор прав доступа к объектам информационной системы (прав на выполнение над ними определенного набора действий)
3. этот набор прав должен соответствовать выполняемой работником трудовой функции

Дополнительные понятия:

1. привилегии (операции) – минимально возможные действия пользователя, требующие разрешения или запрещения этого действия;
2. правила (задачи) – объединение привилегии, подмножества объектов, для которых может быть определена такая привилегия, и признака разрешения или запрещения этой привилегии;
3. роль – набор правил, определяющих, какими привилегиями и по отношению к каким объектам будет обладать пользователь, которому будет назначена эта роль;
4. сессия – подмножество ролей, которые активировал пользователь после своего входа в систему в течение определенного интервала времени.
5. Преимущества проявляются при организации коллективного доступа к ресурсам сложных информационных систем с большим количеством пользователей и объектов.

Недостатки:

1. отсутствие формальных доказательств безопасности компьютерной системы;
2. возможность внесения дублирования и избыточности при предоставлении пользователям прав доступа;
3. сложность конструирования ролей.

В данной лабораторной работе необходимо составить матрицу доступа. Матрица доступа в табличной форме отражает права всех групп пользователей ИСПДн на действия с персональными данными. Действия (операции) с персональными данными, включают сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных).

Есть три основные группы пользователей ИСПДн (группы описаны в Концепции информационной безопасности):

1. Администраторы ИСПДн, осуществляющие настройку и установку технических средств ИСПДн и обеспечивающие ее бесперебойную работу;
2. Разработчики ИСПДн, осуществляющие разработку и поддержку программного обеспечения собственной разработки или стандартных программ, специально доработанных под нужды организации;
3. Операторы ИСПДн, осуществляющие текущую работу с персональными данными.

Каждая группа может быть уточнена (пример уточнения описан в Политике информационной безопасности), например, может быть две группы Операторов ИСПДн. Первая осуществляет лишь сбор и систематизацию персональных данных, вторая – уточнение, использование и распространение. В матрице доступа должно быть описание всех групп, обладающих правами на определенные действия с ПДн. Должен быть уточнен список разрешенных действий каждой из групп.

В нашей работе необходимо рассмотреть не группы, а конкретных пользователей.

Шаблон типовой матрицы доступа представлен в конце практикума в приложении Б.

Постановка задачи.

Выполнить все шаги работы, необходимые для составления матрицы доступа. Доработать шаблон матрицы и зафиксировать свои результаты.

Таблица Б.1 – Матрица доступа

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Субъект доступа**  **Объект** **доступа** | Тип действия | Начальник отдела кадров | Сотрудник отдела кадров | Специалист ИБ | Системный администратор |
| E:\\Data\Личные дела | Чтение | + | + | - | - |
| Копирование | + | - | - | + |
| Запись | + | + | - | - |
| Удаление | + | - | + | - |
| E:\\Data\Бланки и шаблоны | Чтение | + | + | - | - |
| Копирование | + | - | - | + |
| Запись | + | + | - | - |
| Удаление | + | - | + | - |
| E:\\DocumentsAndSettings\CopyOfDocuments\  Копии трудовых книжек | Чтение | + | + | - | - |
| Копирование | + | - | - | + |
| Запись | + | + | - | - |
| Удаление | + | - | + | - |

Продолжение таблицы Б.1 – Матрица доступа

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Субъект доступа**  **Объект** **доступа** | Тип действия | Начальник отдела кадров | Сотрудник отдела кадров | Специалист ИБ | Системный администратор |
| E:\\ DocumentsAndSettings\CopyOfDocuments\  Копии паспортов | Чтение | + | - | - | - |
| Копирование | + | - | - | + |
| Запись | + | - | - | - |
| Удаление | + | - | + | - |
| Принтер | Настройка | - | - | + | + |
| Печать | + | + | + | - |
| ОС, СЗИ | Настройка | - | - | + | - |
| Инсталяция | - | - | - | + |
| Внешние носители информации | Чтение | + | + | + | + |
| Запись | + | - | - | + |
| Удаление | + | + | - | - |

от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_ от Исполнителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Таблица Б.2 – Разрешенные операции для субъектов

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Имя субъекта:** | Начальник отдела кадров | | **Имя субъекта:** | Сотрудник отдела кадров | | **Имя субъекта:** | Специалист ИБ | |
| **Объект доступа:** | Принтер  Машинные носители информации E:\\Data\Личные дела  E:\\Data\Бланки и шаблоны  E:\\DocumentsAndSettings\CopyOfDocuments\Копии трудовых книжек  E:\\ DocumentsAndSettings\  CopyOfDocuments\  Копии паспортов | | **Объект доступа:** | Принтер  Машинные носители информации  E:\\Data\Личные дела  E:\\Data\Бланки и шаблоны  E:\\DocumentsAndSettings\CopyOfDocuments\Копии трудовых книжек | | **Объект доступа:** | Принтер  Машинные носители информации  Программные средства  ОС, СЗИ | |
| **Разрешения:** | **Разрешить** | **Запретить** | **Разрешения:** | **Разрешить** | **Запретить** | **Разрешения:** | **Разрешить** | **Запретить** |
| - сбор | **+** |  | - сбор | **+** |  | - сбор |  | **+** |
| - систематизация | **+** |  | - систематизация | **+** |  | - систематизация |  | **+** |
| - накопление | **+** |  | - накопление | **+** |  | - накопление |  | **+** |
| - хранение | **+** |  | - хранение | **+** |  | - хранение | **+** |  |
| - уточнение | **+** |  | - уточнение | **+** |  | - уточнение |  | **+** |
| - использование | **+** |  | - использование | **+** |  | - использование |  | **+** |
| - блокирование | **+** |  | - блокирование |  | **+** | - блокирование | **+** |  |
| - уничтожение | **+** |  | - уничтожение |  | **+** | - уничтожение | **+** |  |
| **Имя субъекта:** | Системный администратор | | **Имя субъекта:** |  | | **Имя субъекта:** |  | |
| **Объект доступа:** | Принтер  Машинные носители информации  Программные средства  ОС, СЗИ | | **Объект доступа:** |  | | **Объект доступа:** |  | |
| **Разрешения:** | **Разрешить** | **Запретить** | **Разрешения:** | **Разрешить** | **Запретить** | **Разрешения:** | **Разрешить** | **Запретить** |
| - сбор |  | **+** | - сбор |  |  | - сбор |  |  |
| - систематизация |  | **+** | - систематизация |  |  | - систематизация |  |  |
| - накопление |  | **+** | - накопление |  |  | - накопление |  |  |
| - хранение | **+** |  | - хранение |  |  | - хранение |  |  |
| - уточнение |  | **+** | - уточнение |  |  | - уточнение |  |  |
| - использование |  | **+** | - использование |  |  | - использование |  |  |
| - блокирование |  | **+** | - блокирование |  |  | - блокирование |  |  |
| - уничтожение |  | **+** | - уничтожение |  |  | - уничтожение |  |  |

**Вывод**

В ходе данной работы была разработана матрица доступа по существующим требованиям к ИСПДн в соответствии с 8 пунктом статьи 19 ФЗ-152: «Обеспечение безопасности персональных данных достигается, в частности: установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационной системе персональных данных».

Матрица доступа должна отражать полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПДн – чтение, запись, копирование, удаление. Документ утверждается руководителем.

В процессе выполнения задания были получены сведения о типах разграничения доступа и их особенностях. В данной работе была применена дискреционная модель разграничения прав доступа к ресурсам ИС. Были установлены правила получения информации в исследуемой системе, следовательно, работу можно считать выполненной.

**Список литературы**

1. В. Н. Сабынин, А. Н. Березин, И. В. Ковалева,Технология разработки информационных систем в защищенном исполнении: лабораторный практикум. СПбГЭТУ «ЛЭТИ», 2016
2. Методический документ ФСТЭК «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн»
3. Федеральный закон «О персональных данных» ФЗ-152