МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н.И. ЛОБАЧЕВСКОГО»

РАДИОФИЗИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Научно-исследовательская работа

Работу выполнил студент

Группы \_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_ Шаров В.А.

(подпись)

Номер зачётной книжки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверил: ассистент

\_\_\_\_\_\_\_\_\_\_\_ Рябов А.А.

(подпись)

Н. Новгород, 2018

Содержание

[1. Введение 3](#__RefHeading___Toc1373_557217930)

[2. Основные определения 4](#__RefHeading___Toc1375_557217930)

[3. Механизмы разграничения доступа в различных операционных системах 5](#__RefHeading___Toc1377_557217930)

[3.1. Система управления доступом в ОС семейства Windows 6](#__RefHeading___Toc1379_557217930)

[3.2. Система управления доступом в ОС семейства Linux 9](#__RefHeading___Toc1381_557217930)

[4. Обнаружение несанкционированного доступа 12](#__RefHeading___Toc1383_557217930)

[4.1. Статистический подход к обнаружению НСД 13](#__RefHeading___Toc1385_557217930)

[4.2. Экспертный подход к обнаружению НСД 15](#__RefHeading___Toc1387_557217930)

[5. Поведенческие технологии обнаружения атак 16](#__RefHeading___Toc1389_557217930)

[6. Заключение 18](#__RefHeading___Toc1391_557217930)

[7. Список литературы 19](#__RefHeading___Toc2038_557217930)

### 1. Введение

Современные информационные системы (ИС) являются одним из краеугольных камней, на основе которых строятся бизнес-процессы компаний и предприятий различных форм и назначений. Однако присущая для всех ИС «Ахилесова пята» — *уязвимость* заставляет уделять особое внимание их защите от различных несанкционированных действий.

ИС находится в *состоянии* *безопасности*, если она защищена от нарушений конфиденциальности, целостности и доступности, где:

* **конфиденциальность** (confidentiality) — это состояние ИС, при котором информационные ресурсы доступны только тем пользователям, которым этот доступ разрешён;
* **целостность** (integrity) — это состояние системы, при котором информация, хранящаяся и обрабатываемая этой ИС, а также процедуры обработки информации не могут быть изменены, удалены или дополнены неавторизованным образом.
* **доступность** (availability) — это состояние системы, при котором услуги, оказываемые системой, могут гарантированно и с приемлемой задержкой быть предоставлены пользователям, имеющим на это право.

Различные уязвимости ИС могут эксплуатироваться в результате ошибочных или злонамеренных действий.

В данной работе будут рассмотрены такие проблемы безопасности ИС, как контроль доступа пользователей к ИС и методы обнаружения несанкционированных действий в системе.

### 2. Основные определения

**Объекты** системы представляют физические и логические информационные ресурсы ИС. К физическим ресурсам относятся как отдельные устройства целиком (процессор, внешние устройства и т. д.), так и физические разделяемые ресурсы устройств (например, разделы и секторы диска). Логическими ресурсами являются файлы, вычислительные процессы, сетевые сервисы, приложения и т. п.

**Субъекты** представляют сущности, между которыми разделяются информационные ресурсы. Это могут быть легальные пользователи ИС или группы легальных пользователей, объединённых по различным признакам. Пользователь осуществляет доступ к объектам ИС не непосредственно, а с помощью прикладных процессов, которые запускаются от его имени. Поэтому в качестве субъектов выступают также прикладные вычислительные процессы.

**Операции** выполняются субъектами над объектами. Для каждого типа объектов существует собственный набор операций, которые с ними может выполнять субъект.

**Система** **контроля** **доступа** решает, какие операции разрешены для данного субъекта по отношению к данному объекту. Для автоматизированного контроля доступа необходимо, чтобы для каждой пары субъект-объект были однозначно определены *правила* *доступа*, на основании которых система могла бы разрешить или запретить выполнение каждой из предусмотренных для данного объекта операции.

Важнейшими элементами управляемого доступа являются:

* **идентификация** — присвоение объектам и субъектам ИС уникальных имён — **идентификаторов**;
* **аутентификация** — процедура доказательства субъектом/объектом того, что он есть то, за что (кого) он себя выдаёт;
* **авторизация** — процедура контроля доступа субъектов к объектам и предоставления каждому из них именно тех прав, которые для них определены правилами доступа.

### 3. Механизмы разграничения доступа в различных операционных системах

После того, как пользователь, успешно пройдя процедуру аутентификации, зашёл в систему, ему предоставляется некоторый набор прав по отношению к защищаемым системой ресурсами.

Наделение легальных пользователей правами доступа к ресурсам называется **авторизацией**, а процедура приведения авторизации в действие называется **управлением** **доступом** (access control).

Большинство реализуемых на практике способов управления доступом может быть отнесено к одной из следующих категорий:

* **дискреционный метод доступа** (Discretionary Access Control, DAC), называемый также избирательным, или произвольным;
* **мандатный метод доступа** (Mandatory Access Control, MAC), называемый также принудительным;
* **ролевой доступ** (Role-based Access Control, RBAC), называемый также недискреционным методом доступа (nondiscretionary access control).

Что касается систем управления доступов в универсальных ОС, то там доминирует модель DAC. Практически все популярные сегодня семейства универсальных ОС — Linux, Mac OS X, MS Windows — опираются на эту модель, как на основную. Поэтому следует упомянуть главные особенности этого метода:

* Права доступа в методе DAC описываются в виде списков ACL (Access Control List), которые дают возможность определения набора разрешённых операций для каждого отдельного пользователя по отношению к каждому отдельному ресурсу, причём и пользователь и ресурсы задаются уникальными идентификаторами.
* В методе DAC право назначать права на доступ к объектам делегируются отдельным пользователям — владельцам объектов. То есть им разрешается действовать «по своему усмотрению» и назначать другим пользователям права на доступ к тем объектам, владельцами которых они являются.

В качестве примеров рассмотрим системы управления доступом таких ОС, как Windows и Linux.

### 3.1. Система управления доступом в ОС семейства Windows

Для системы безопасности ОС семейства Windows характерно наличие большого количества различных встроенных субъектов доступа — как отдельных пользователей, так и групп. Так, в системе всегда имеются пользователи Administrator, System и Guest, а также группы Users, Administrators, Account Operators, Server Operators, Everyone и др. Смысл этих встроенных пользователей и групп состоит в том, что они изначально наделены некоторыми правами, облегчая администратору работу по созданию эффективной системы разграничения доступа. Во многих случаях этих групп оказывается вполне достаточно, и поэтому при добавлении нового пользователя в систему администратору остаётся только решить, к какой группе или группам его отнести.

ОС семейства Windows поддерживает три класса операций доступа, которые отличаются типом субъектов и объектов, участвующих в этих операциях:

* **Разрешения** (permissions) — это множество операций, которые могут быть определены для субъектов всех типов по отношению к объектам любого типа: файлам, каталогам, секциям памяти и т. д.
* **Права** (user rights) определяются для субъектов типа группы на выполнение некоторых системных операций: арихивирование файлов, выключение компьютера и т. п. В этих операциях участвует особый объект доступа — операционная система в целом.
* **Возможности пользователей** (user abilities) определяются для отдельных пользователей на выполнение действий, связанных с формированием их операционной среды. За счёт уменьшения набора возможностей (доступных пользователю по умолчанию) администратор может «заставить» пользователя работать с той операционной средой, которая наилучшим образом соответствует политике безопасности.

В основном именно права, а не разрешения отличают одну встроенную группу пользователей от другой. Права встроенных групп бывают двух типов:

* **Встроенные** — права, являющиеся неотъемлемыми атрибутами встроенных групп. Администратор не может распоряжаться этими правами.
* **Изменяемые** — права, которые можно удалять или добавлять к правам встроенной группы из общего списка изменяемых прав.

Для ОС семейства Windows характерна высокая степень детализации операций доступа. Так для доступа к файлам и каталогам предусмотрено два типа разрешений:

* **индивидуальные** **разрешения** относятся к элементарным операциям;
* **стандартные** **разрешения** являются объединением индивидуальных разрешений.

|  |  |
| --- | --- |
| **Разрешение** | **Для** **файла** |
| Read (R) | Чтение данных, атрибутов, имени владельца и разрешений файла |
| Write (W) | Чтение имени владельца и разрешений файла, изменение атрибутов файла, изменение и добавление данных файла |
| Execute (X) | Чтение атрибутов файла, имени владельца и разрешений. Выполнение файла, если он хранит код программы |
| Delete (D) | Удаление файла |
| Change Permission (P) | Изменение разрешений файла |
| Take Ownership (O) | Вступление во владение файлом |

*Табл. 1. Индивидуальные разрешения для каталогов и файлов*

|  |  |
| --- | --- |
| **Стандартное** **разрешение** | **Индивидуальные** **разрешения** |
| No Access | Ни одного |
| Read | RX |
| Change | RWXD |
| Full Control | Все |

*Табл. 2. Стандартные и индивидуальные разрешения для файлов*

Результатом успешной аутентификации пользователя в ОС Windows является создание для него системой **токена** **доступа** (access token). Токен доступа привязывается ко всем процессам, которые данный пользователь создаёт в течение сеанса работы, и включает в себя идентификатор пользователя и идентификаторы всех групп, в которые он входит, список прав пользователя на выполнение системых операций и др.

Проверка прав доступа к объектам выполняется *централизованно* с помощью модуля ОС — **монитора** **безопасности** (Security Reference Monitor). Монитор безопасности сравнивает идентификаторы пользователя и групп пользователей из токена доступа процесса с соответствующими идентификаторами, хранящимися в элементах ACL объекта. Проверка прав доступа выполняется при первом обращении процесса к объекту, а не при каждом использовании объекта.

### 3.2. Система управления доступом в ОС семейства Linux

В отличие от ОС Windows, система разграничения доступа ОС Linux, не может зафиксировать права каждого из пользователей на каждый файловый объект. По отношению к каждому из файлов пространство пользователей делится на три неравные по численности категории: *одного* владельца файла, членов его *основной* группы и всех остальных зарегистрированных пользователей.

При регистрации система присваивает каждому пользователю уникальный числовой идентификатор **UID** (User ID). Пользователь с **UID** = 0 по умолчанию имеет учетное имя **root** и является для системы администратором (суперпользователем). Права суперпользователя традиционно являются объектом противоправных посягательств. Система не позволяет регистрировать более одного суперпользователя.

Пользователей в целях удобства администрирования можно объединять в группы, которым также присваиваются символьные имена и уникальные числовые идентификаторы **GID** (Group ID). При этом **GID** = 0 присваивается группе администратора.

Всего в операционной системе Linux предусмотрено шесть типов файлов:

1. Обычный файл (regular file);
2. Каталог (directory);
3. Именованный канал (named pipe);
4. Символическая ссылка (soft link);
5. Специальный файл устройства (device file);
6. Сокет (socket).

Всего существует три первичных и относительно независимых вида доступа (mode) к файлам:

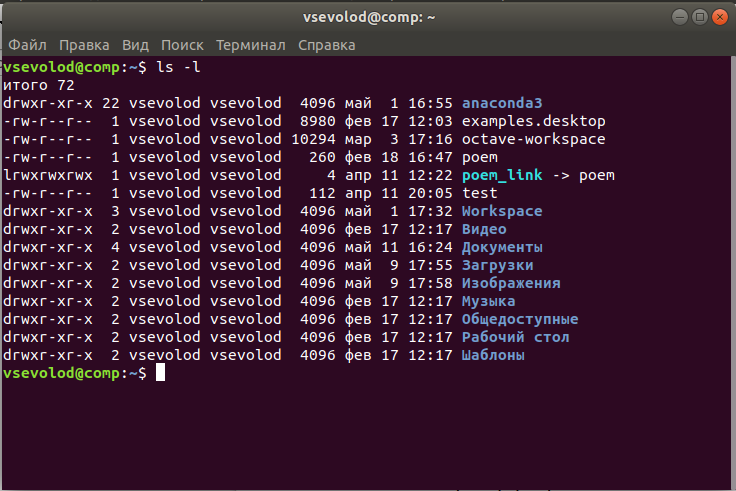
* чтение (**r** — **r**ead);
* запись (**w** — **w**rite);
* исполнение (**x** — e**x**ecute).

Можно заметить, что права доступа в ОС Linux по своему назначению соответствуют разрешениям в ОС Windows.

Все зарегистрированные пользователи в системе по отношению к каждому из файлов делятся на три неравных по численности категории:

1. Владелец файла (как правило им является создатель файла);
2. Члены основной (первичной) группы владельца;
3. Все остальные зарегистрированные пользователи системы.

Информации о правах доступа к объектам файловой системы можно узнать с помощью команды **ls -l** (list — список). Первый столбец в выводимой таблице как раз и указывает на тип файла и права доступа к нему:

**

*Рис. 1. Работа команды ls -l*

Первый символ первого столбца указывает на тип файла. Остальные символы можно разделить на тройки, каждая из которых будет указывать на права доступа для каждой категории пользователей. Эти права записываются в бинарном виде и представляют собой восьмеричную цифру. Отсутствующее право доступа обозначается дефисом, а в двоичном виде – нулем. Наличие права отображается латинским символом или единицей. Например:

**r - -** = 100 = 4;

**r w -** = 110 = 6;

**r w x** = 111 = 7 и т. д.

Права на доступ к уже существующему файлу или каталогу можно изменять. Администратор может изменить права доступа к любому файлу, пользователь – только к своим файлам. Производится это с помощью утилиты **chmod** (change mode – изменить режим). Ее наиболее распространённая форма:

**chmod XXX <file\_name>**,

где **XXX —** 3 восьмеричные цифры, означающие права владельца, его основной группы и остальных пользователей соответственно. Такой способ называется *абсолютным* изменением, поскольку при нём сразу же устанавливаются все биты прав доступа. В табл. 3. перечислены наиболее распространённые варианты:

|  |  |  |
| --- | --- | --- |
| **Режим** | **Значение** | **Применение** |
| 644 | Пользователь: чтение/запись; группа, другие: чтение | Файлы |
| 600 | Пользователь: чтение/запись; группа, другие: нет | Файлы |
| 755 | Пользователь: чтение/запись/исполнение; группа, другие: чтение/исполнение | Каталоги, команды |
| 700 | Пользователь: чтение/запись/исполнение; группа, другие: нет | Каталоги, команды |
| 711 | Пользователь: чтение/запись/исполнение; группа, другие: исполнение | Каталоги |

*Табл. 3. Абсолютные режимы прав доступа*

С каждым процессом в системе связан идентификатор пользователя

**UID**, от имени которого процесс запущен. Алгоритм, реализованный системной функцией, сперва сравнивает **UID** процесса и **UID** файла, и, обнаружив совпадение, выдаёт процессу права владельца на этот файл. Если совпадения не было, то проверяется наличие пользователя в основной группе владельца с помощью **GID**, и в случае успеха, процессу выдаются права основной группы владельца на файл. В противном случае — выдаются права остальных пользователей.

В ОС Linux также предусмотрена передача прав владения файлами, однако эту функцию может использовать только администратор. Эта операция производится с помощью утилиты **chown** (change owner – сменить владельца) командой

**chown <user\_name> <file\_name>**

### **4. Обнаружение несанкционированного доступа**

**Несанкционированный доступ к информации (НСД)** — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Последствиями НСД могут быть:

1. Нарушение функций:

* Временные нарушения, приводящие к путанице в графиках работы, расписаний и т. п.;
* Недоступность системы для пользователей;
* Повреждение аппаратуры;
* Повреждение программного обеспечения;

1. Потеря значимых ресурсов;
2. Потеря монопольного использования;
3. Нарушение прав (авторских, патентных и т. п.);
4. Утечка информации:

* Утечка персональных данных;
* Утечка коммерческой тайны и ноу-хау;
* Утечка служебной переписки;
* Утечка государственной тайны и т. д.

Для избежания таких неприятных последствий в первую очередь необходимо вовремя распознать факт НСД.

Рассмотрим основные подходы, используемые при обнаружении атак – **статистический** и **экспертный**.

### 4.1. Статистический подход к обнаружению НСД

При **статистическом** **анализе** вывод о том, что произошла атака, строится на основе дисперсии (отклонения от среднего значения) профиля нормального поведения. Средние величины вычисляются для каждого типа нормального поведения (например, количество входов в систему, количество отказов в доступе, время суток и т. д.). О возможных атаках сообщается, когда наблюдаемые значения выпадают из нормального диапазона, т. е. превышают заданный порог.

Параметры, которые включаются в шаблон поведения субъекта системы, могут быть отнесены к следующим группам:

* Числовые параметры (загрузка центрального процессора, число файлов, к которым осуществлялся доступ, и т. п.);
* Категориальные параметры (имена файлов, команды пользователя, и т. д.);
* Параметры активности (число обращений к файлам или соединений за единицу времени и др.).

При этом важно правильно выбрать контролируемые параметры, т. к. малое их число или неправильно выбранные параметры могут привести к тому, что модель описания поведения системы будет неполной, и многие атаки останутся за пределами её рассмотрения. С другой стороны, слишком большое количество контролируемых параметров приводит к снижению производительности за счёт требований к потребляемым ресурсам.

|  |  |
| --- | --- |
| **Достоинства** | **Недостатки** |
| Обнаружение неизвестных атак | Злоумышленник может обмануть систему при постепенном изменении режима работы с течением времени и “приручения” системы к новому поведению |
| Обнаружение более сложных атак | Высокая вероятность получения ложных сообщений об атаках |
| Возможность адаптации системы к изменению поведения пользователя | Не очень корректная обработка изменения в деятельности пользователя |
|  | Неспособность обнаружения атак со стороны субъектов, для которых нельзя составить шаблон типичного поведения |
|  | Неспособность обнаружения атак со стороны субъектов, которые с самого начала выполняют несанкционированные действия. Таким образом, их шаблоны обычного поведения будут включать только атаки |
|  | Необходима предварительная настройка (задание пороговых значений для каждого параметра для каждого пользователя) |
|  | Нечувствительность к порядку следования событий |

*Табл. 4. Достоинства и недостатки статистического метода обнаружения несанкционированного доступа*

### 4.2. Экспертный подход к обнаружению НСД

Второй, экспертный, подход к обнаружению атак основывается на построении **экспертной** **системы** – системы, которая в контексте обнаружения атак принимает решение о принадлежности того или иного события к классу атак на основании имеющихся правил, описывающих сценарии атак. Эти правила основаны на опыте специалистов и хранятся в специальном хранилище, называемом **базой** **знаний**. Механизм обнаружения идентифицирует потенциальные атаки в случае, если действия пользователя совпадают с установленными правилами. Наличие исчерпывающих баз данных таких правил является наиболее важным аспектом для экспертных систем обнаружения атак. В большинстве случаев правила экспертной системы опираются на так называемые сигнатуры, которые ищутся в контролируемом пространстве.

**Сигнатуры** – это шаблоны, сопоставленные известным атакам или злоупотреблениям в системах. Большинство коммерческих продуктов обнаружения атак проводят анализ сигнатур в сравнении с базой данных известных атак, поставляемой продавцом. Также могут быть добавлены дополнительные сигнатуры, установленные клиентом.

|  |  |
| --- | --- |
| **Достоинства** | **Недостатки** |
| Простота реализации | Неспособность к обнаружению неизвестных атак |
| Скорость функционирования | Небольшие изменения в атаке приводят к невозможности её обнаружения |
| Отсутствие ложных тревог | Зависимость от квалификации специалистов, заполняющих базу знаний |

*Табл. 5. Достоинства и недостатки экспертных систем обнаружения атак*

В большинстве случаев сочетаются оба подхода при обнаружении атак.

### **5. Поведенческие технологии обнаружения атак**

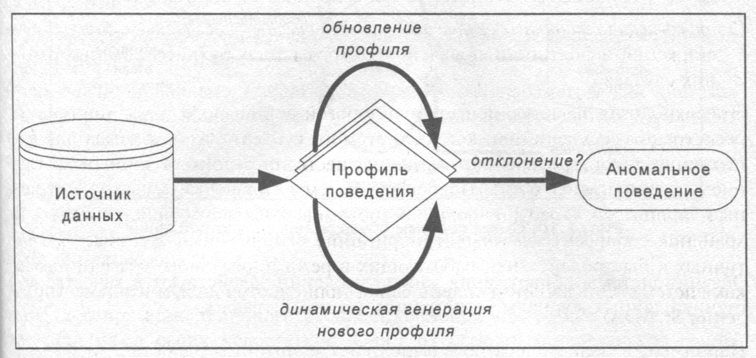
Обнаружение атак требует выполнения одного из двух условий: или понимания ожидаемого поведения контролируемого объекта системы или знания всех возможных атак и их модификаций. В первом случае используется технология **обнаружения** **аномального** **поведения** (anomaly detection), а во втором технология **обнаружения** **злоупотреблений** (misuse detection).

Технология обнаружения аномалий, так же называемая **поведенческой** **технологией** **обнаружения** **атак**, основана на том, что аномальное поведение субъекта (системы, программы, пользователя), т. е., как правило, атака или какое-нибудь враждебное действие часто проявляется как отклонение от нормального поведения. Однако аномальное поведение не всегда является атакой. С учетом этого факта можно заметить, что возможны две крайности:

* Обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак (false positive).
* Пропуск атаки, которая не подпадает под определение аномального поведения (false negative). Этот случай гораздо более опасен, чем ложное причисление аномального поведения к классу атак.

При настройке и эксплуатации систем такой категории решаются две задачи:

* Построение профиля субъекта.
* Определение граничных значений характеристик поведения субъекта для снижения вероятности появления одной из крайностей.



*Рис. 2. Схема системы обнаружения аномального поведения*

Как правило, при обнаружении аномального поведения используется метод статистического анализа обнаружения атак. Однако, поведенческий метод может быть также реализован при помощи экспертных систем. При этом база знаний такой системы описывает штатное поведение информационной системы.

### 6. Заключение

Были рассмотрены такие проблемы безопасности ИС, как контроль доступа и обнаружение несанкционированного доступа.

При рассмотрении проблемы контроля доступа были исследованы системы управления доступом таких операционных систем, как Windows и Linux. Выяснилось, что эти системы имеют общие черты: например, использование метода DAC при контроле доступа, а также схожую систему разбиения субъектов на пользователей и группы пользователей. Также были выявлены некоторые различия: например, невозможность зафиксировать права отдельных пользователей в ОС Linux в отличие от ОС Windows; система управления доступом в ОС Windows в целом является более гибкой из-за разнообразия прав на выполнение системных действий.

При исследовании вопроса обнаружения несанкционированного доступа были рассмотрены статистический и экспертный подходы обнаружения атак. Выяснилось, что статистический подход наиболее эффективен при обнаружении неизвестных типов атак, а экспертный — при обнаружении уже известных. Для обеспечения высокой степени защищённости ИС сочетаются оба подхода.

Выяснилось, что для обнаружения атаки требуется либо понимание ожидаемого поведения ИС, либо знание всевозможных атак и их модификаций. В первом случае используются так называемые поведенческие технологии обнаружения. Они могут быть реализованы как с помощью статистического, так и с помощью экспертного подхода.

### 7. Список литературы

1. Олифер В., Олифер Н. — Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — Спб.: Питер, 2017. — 992 с.
2. Бакланов В.В. — Защитные механизмы операционной системы Linux: учебное пособие. — Екатеринбург: УрФУ, 2011. — 354 с.
3. Уорд Б. — Внутреннее устройство Linux. — Спб: Питер, 2018. — 384 с.
4. Лукацкий А.В. — Обнаружение атак. 2-е изд. — Спб.: БХВ-Петербург, 2003. — 563 с.