МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

Кафедра кібербезпеки

МЕТОДИЧНІ ВКАЗІВКИ

виконання лабораторних та самостійних робіт
з дисципліни
«Комплексні системи контролю та управління доступом»

для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»

Одеса 2020

УДК 004.6

Укладач:

Кухаренко С.В. – кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Рекомендовано Навчально-методичною радою

Національного університету «Одеська юридична академія»,

протокол № 2 від 4 грудня 2020 р.

Рецензенти:

Яценко В.О. – керівник проекту Освітній Фонд KeepSolid;

Логінова Н.І. – доцент, кандидат педагогічних наук, завідувач кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Розглянуто загальні поняття про моделі комп’ютерних систем з дискреційним, мандатним і рольовим управлінням доступом, моделі безпеки інформаційних потоків і ізольованого програмного середовища, а також питання, пов’язані з оцінкою рівня захищеності інформаційно-комунікаційних систем і технологій від несанкціонованого доступу до ресурсів. Описані основні елементи управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів, а також управління доступом до інформаційних ресурсів та процесів в інформаційно-телекомунікаційних системах на основі моделей управління доступом

Призначено для студентів з метою закріплення лекційного матеріалу і підготовки до лабораторних занять та самостійних робіт з дисципліни «Комплексні системи контролю та управління доступом».

Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни «Комплексні системи контролю та управління доступом» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології» / Уклад.: С.В.Кухаренко. – О.: НУ «ОЮА», 2020. – 32 с.

ПЕРЕДМОВА

Дисципліна «Комплексні системи контролю та управління доступом» вивчається студентами академії за напрямом бакалаврської підготовки з галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека» на четвертому курсі навчання.

Метою викладання навчальної дисципліни «Комплексні системи контролю та управління доступом» є оволодіння студентами базовими поняттями щодо діяльності, пов’язаної із захистом інформації; навчання загальним принципам побудови моделей і політик безпеки, основним методам дослідження коректності систем захисту, методології обстеження та проектування систем захисту.

Дисципліна знайомить з моделями комп’ютерних систем з дискреційним, мандатних і рольовим управлінням доступом, моделями безпеки інформаційних потоків і ізольованого програмного середовища, а також розглядаються питання, пов’язані з розвитком формальних моделей безпеки комп’ютерних систем.

Оволодіння курсом «Комплексні системи контролю та управління доступом» передбачає читання лекцій, проведення лабораторних занять, виконання самостійної роботи та складання екзамену. Особлива увага приділяється прищепленню студентам практичних навичок із застосування сучасних інформаційно-комунікаційних технологій у майбутній професійній діяльності.

Згідно з вимогами освітньо-професійної програми після вчення дисципліни «Комплексні системи контролю та управління доступом» здобувачі вищої освіти повинні:

– **володіти** методами моделювання безпеки комп’ютерних систем, в тому числі моделювання управління доступом та інформаційними потоками в комп’ютерних системах;

– **володіти** знаннями про основні моделі управління доступом, методи, принципи і правила побудови систем захисту інформації від несанкціонованого доступу на об’єктах інформаційної діяльності;

– **вміти** розробляти політики безпеки комп’ютерних систем, політики управління доступом та інформаційними потоками, а також моделі загроз і моделі порушника безпеки комп’ютерних систем;

– **вміти** опрацьовувати отримані результати, аналізувати та осмислювати їх, представляти результати роботи і обґрунтовувати запропоновані рішення на сучасному науково-технічному і професійному рівні;

– **вміти** визначати моделі, принципи і правила побудови систем захисту від несанкціонованого доступу об’єктів і інформаційно-комунікаційних систем.

Лабораторна робота №1

КОМПЛЕКСИ ТЕХНІЧНИХ ТА ПРОГРАМНИХ ЗАСОБІВ БЕЗПЕКИ. УПРАВЛІННЯ ДСТУПОМ ДО ФАЙЛОВИХ РЕСУРСІВ

Навчальні питання:

1. Управление доступом пользователей к файлам и папкам.
2. Защита информации от несанкционированного доступа.

Завдання

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).
2. Установите для этой папки разрешения полного доступа для одного из пользователей группы администраторы, и ограниченные разрешения для пользователя с ограниченной учетной записью.
3. Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.
4. Установите общий доступ к папке и подключитесь к ней через сеть с другого компьютера.
5. Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.
6. Экспериментально убедитесь в правилах объединения разрешений NTFS и разрешений общего доступа.
7. Составьте отчет о проведенных экспериментах.
8. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Для назначения разрешений для файла или папки администратор выбирает данный файл или папку и при нажатии правой кнопки мыши использует команду Свойства (Properties) и в появившемся окне переходит на вкладку Безопасность (Security).

В зоне Имя (Name) имеется список групп и пользователей, которым уже назначены разрешения для данного файла или папки.

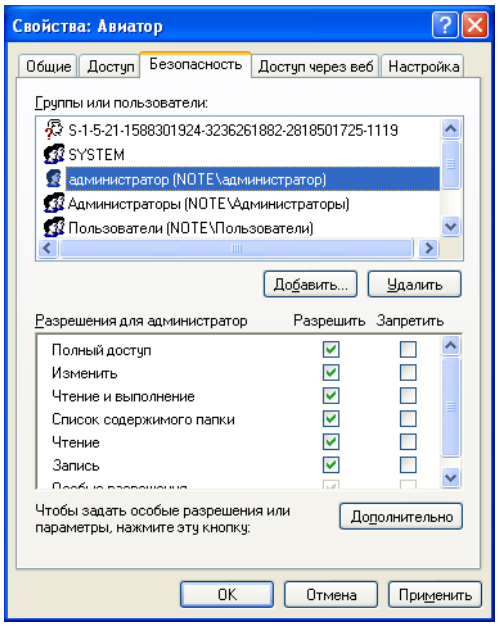


Рисунок 1 Вкладка Безопасность окна свойств папки Авиатор

Для добавления пользователя или группы нажмите кнопку Добавить (Add) или Удалить (Remove). При добавлении появится диалог Выбор: Пользователи, Компьютеры или Группы (SelectUsers,Computers,orGroups). Добавив пользователя или группу мы увидим этот объект в зоне Имя и выделив его, можем задать необходимые разрешения с помощью установки флажков Разрешить (Allow) или Запретить (Deny) в зоне Разрешения (Permissions).

Стандартные разрешения для файлов и папок:

- Полный доступ (Full Control);
- Изменить (Modify);
- Чтение и выполнение (Read&Execute);
- Чтение (Read);
- Запись (Write).

Разрешения для пользователей, получившим доступ к папке или файлу через сеть, регулируются отдельно с помощью так называемых разрешений общего доступа. Эти разрешения распространяются только на папки, к которым предоставлен общий доступ через сеть и действуют только для пользователей, обращающихся к папке через сеть. Возможности пользователя задаются разрешениями, представленными ниже:

- Полный доступ (Full Control);
- Изменить (Change);
- Чтение (Read);

Доступ к средствам настройки разрешений общего доступа выполняется через свойства папки, предоставленной в общий доступ (рисунок 2)

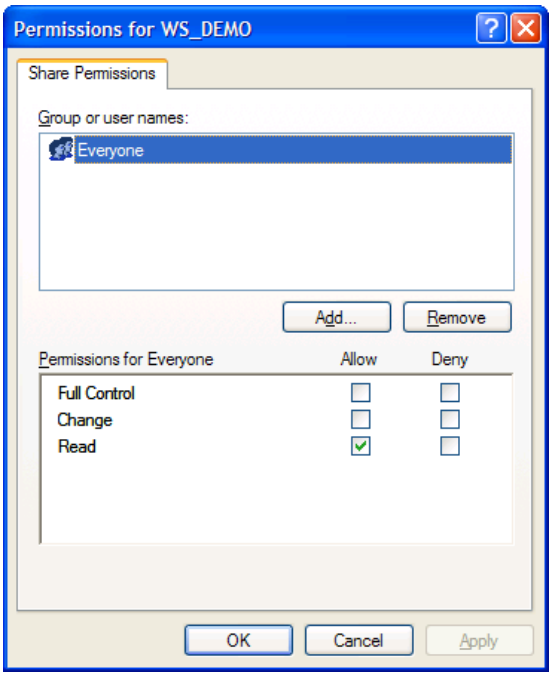


Рисунок 2 Разрешения общего доступа для папки WS_DEMO

Разрешения общего доступа являются средством обеспечения безопасности данных при коллективной работе с документами и поэтому должны устанавливаться очень тщательно и обоснованно. При этом администратору рекомендуется действовать следующим образом.

- Для каждого ресурса общего доступа определить, каким группам пользователей необходим доступ к нему и какой требуется уровень доступа;
- Для упрощения администрирования назначайте разрешения группам, а не отдельным пользователям;

- Устанавливайте максимально строгие разрешения, которые, однако, должны позволять пользователям совершать необходимые действия;
- Организуйте ресурсы общего доступа таким образом, чтобы папки с одинаковым уровнем требований безопасности находились в одной папке. Затем установите общий доступ только к ней, все вложенные папки наследуют настройки безопасности;
- Для папок общего доступа применяйте интуитивно понятные пользователям имена, корректно отображаемые всеми клиентскими операционными системами, используемыми на предприятии.
- Если в общих папках предполагается хранить программы-приложения, то целесообразно поместить их в одну папку – единое место хранения и обновлении я приложений;

Несколько общих папок, доступных членам группы Администраторы, так называемые скрытые Административные общие папки, создаются операционной системой автоматически. Имена этих папок заканчиваются знаком $. Это корневые каталоги каждого тома на жестком диске (C$,D$ и т.д.), папка Admin$ для доступа к системному каталогу, папка Print$ для доступа к файлам драйверов принтеров. Кроме того, скрытую папку с общим доступом можно создать с целью доступа к ней только тех пользователей, которые будут знать имя скрытой папки.

Получить доступ к общим папкам других компьютеров можно используя компоненты Сетевое окружение, Мой компьютер, Мастер добавления в сетевое окружении и команду выполнить (Run).

Соединение с общей папкой через Сетевое окружение выполняется двойным щелчком по ресурсу, к которому необходимо получить доступ. Если общий ресурс отсутствует в списке доступных, выберите значок Добавить новый элемент в сетевое окружение и укажите адрес подключаемого ресурса.

Соединение с общей папкой через компонент Мой компьютер выполняется через меню Сервис этого компонента в пункте Подключить сетевой диск при указании пути к общему ресурсу. Если необходимо пользоваться этим соединением постоянно, нужно чтобы флажок Восстанавливать при входе в

систему был установлен. Соединение будет доступно в разделе Сетевые диске окна Мой компьютер.

Для соединения с общей папкой с помощью команды Выполнить щелкните Пуск, затем Выполнить и введите путь к папке в формате UNC(\\имя_ компьютера\имя_общей папки).

Разрешения можно не только устанавливать, но запрещать. Запрет имеет больший приоритет, чем разрешение. Запрет разрешений как метод контроля ресурсов Microsoft применять не рекомендует, и он используется, в основном, для дополнительной настройки разрешений конкретным пользователям, в отличие от разрешений для других пользователей группы.

Рассмотренные разрешения называются стандартными и позволяют решить большинство задач, связанных с регулированием уровня доступа групп к ресурсам.

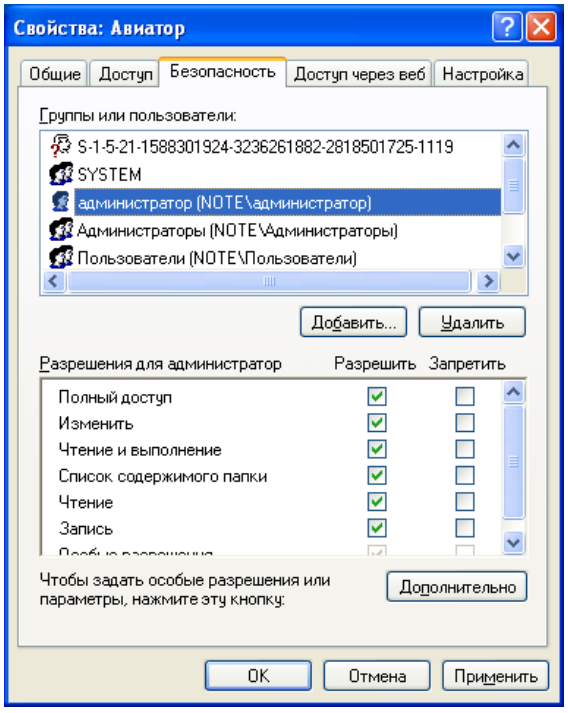


Рисунок 3 Установка разрешений для группы Все

Кнопка Дополнительно служит для задания специальных разрешений. Каждое стандартное разрешение состоит из нескольких специальных, например стандартное разрешение Запись состоит из шести специальных разрешений: создание файлов/запись данных, Создание папок/дозапись данных, запись атрибутов, Запись дополнительных атрибутов, чтение разрешений, синхронизация.

Специальные разрешения можно использовать для более тонкой настройки в нестандартных ситуациях.

В окне специальных разрешений имеются закладки Аудит, Владелец и Эффективные (действующие) разрешения.

Аудит - это процесс, позволяющий фиксировать события, происходящие в системе и имеющие отношения к безопасности. На данной вкладке производится выбор пользователя или группы, для которых данная папка (или файл) будет объектом аудита.

Закладка Владелец обеспечивает такое свойство безопасности, как право владения объектом файловой системы. Администратор всегда может стать владельцем любого объекта файловой системы, любой пользователь является владельцем созданных им объектов и, если локальные или доменные политики безопасности разрешат, пользователь может назначать себя владельцем других файлов и папок.

Список управления доступом (ACL) хранится на диске NTFS для каждого файла или папки. В нем перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения.

Разрешения, назначенные родительской папке, по умолчанию наследуются всеми подпапками и файлами, содержащимися в папках. Однако есть возможность предотвратить наследование для любой вложенной папки и в этом случае эта папка сама становится родительской для вложенных в нее папок.

Если папка предоставлена для общего доступа, то на нее распространяются разрешения двух видов:

- разрешения файловой системы, установленные для пользователей данного компьютера;
- разрешения общего доступа, объявленные для пользователей, получивших доступ через сеть.

Обычно для папок общего доступа задают разрешения полного доступа, а ограничения вводят установкой разрешений NTFS.

В этом случае действует объединение разрешений NTFS и разрешений для общей папки, при котором наиболее строгое разрешение имеет приоритет над другими.

Контрольні запитання

1. Какое из следующих разрешений NTFS для папок позволяет вам удалять папку?
   - Чтение
   - Чтение и выполнение
   - Изменение
   - Администрирование
2. Какое разрешение NTFS для файлов следует установить для файла, если вы позволяете пользователям удалять файл, но не позволяете становиться владельцами файла?
3. Какие объекты по умолчанию наследуют разрешения, установленные для родительской папки?
4. Кто может устанавливать разрешения для отдельных пользователей и групп? (выберите все правильные ответы)
   - Члены группы Администраторы
   - Члены группы Опытные пользователи
   - Пользователи, обладающие разрешением Полный доступ
   - Владельцы файлов и папок
5. Какой из следующих вкладок диалогового окна свойств файла или папки следует воспользоваться для установки или изменений разрешений NTFS:
   - Дополнительно
   - Разрешения
   - Безопасность
   - Общие
6. Если вы хотите, чтобы пользователь или группа не имела доступа к определенной папке или файлу, следует ли запретить разрешения для этой папки или файла?

Лабораторна робота №2

МЕТОДИ ТА МОДЕЛІ ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Навчальні питання:

1. Управління силами і засобами системи інженерно-технічного захисту інформації.
2. Організація захисту інформації від витоку технічними каналами

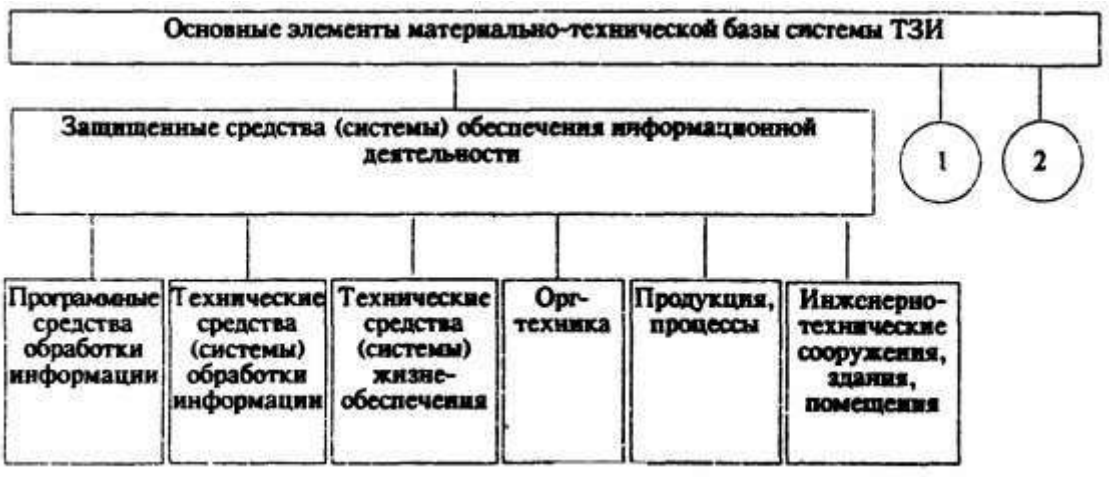
Завдання

Вигадати інформаційну систему (наприклад, армійська рація+приймальник або більшу) та візуалізувати найпростішу план-схему, яка міститиме технічні та криптографічні засоби, пояснити свій вибір. Умовні позначки вибираються самостійно, легенда повинна додаватись.

Методичні рекомендації

Системи технічного захисту інформації, зазвичай, базуються на поєднанні апаратних та криптографічних комплексів, які включають в себе моделювання сигналів, їх шифрування, подальшу деформацію тощо. Будь-яка система ТЗІ починається з розробки плану-схеми такої системи, що дає можливість виконати реалізації швидке, якісніше та уникаючи помилок.

Приклад системи технічного захисту інформації:



Список джерел, необхідних для виконання завдання:

1. https://www.delphiplus.org/inzhenerno-tekhnicheskaya-zashchita-informatsii/upravlenie-silami-i-sredstvami-sistemy-inzhenerno-tekhnicheskoi-zashchity-informatsii.html
2. http://www.bnti.ru/showart.asp?aid=751&lvl=04.03. (Организация защиты информации от утечки по техническим каналам)

Контрольні запитання

1. Яка інформація відноситься до інформації, що захищається?
2. Що входить в створення системи технічного захисту інформації?
3. Класифікація об’єктів, що захищаються?
4. Перерахуйте потенційні технічні канали витоку інформації.
5. Перерахуйте потенційні технічні канали витоку мовної інформації.
6. Що необхідно забезпечити для ефективного управління силами і засобами системи інженерно-технічного захисту-інформації?
7. Які основні завдання автоматизації управлінських рішень?

Лабораторна робота №3
МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ

Навчальні питання:

1. Модель «Китайська стіна».

Завдання

Реалізувати систему надання доступу «Китайська стіна» програмно або візуалізовано у вигляді схеми на реальному прикладі довільного інформаційного середовища. Пояснити роботу такої реалізованої моделі.

Методичні рекомендації

У 1989 р Бювером і Нешем була розроблена модель «Китайська стіна», створювана як протилежність моделі Белла-ЛаПадули. Основна область застосування моделі - фінансові аналітичні організації, для яких важливо уникнути конфлікту інтересів.

Список джерел, необхідних для виконання завдання:

1. https://studbooks.net/2178536/informatika/model_kitayskoy_steny

Лабораторна робота №4
МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ

Навчальні питання:

1. Можливості Windows і Linux по обмеженню доступу до об’єктів операційної системи.
2. Основні інструменти управління доступом

Завдання

1. Опанувати управління доступом користувачів до локальної файлової системи Windows через діалогове вікно властивостей файлових об’єктів (натиснути правою кнопкою миші на об’єкті, що підлягає захисту (файлі або папці) и вибрати «Свойства» Перейти на вкладку «Безопасность»).

2. Для управління доступом користувачів до файлової системи необхідно:

а) натиснути «Пуск» > «Выполнить»;

б) набрати команду cmd и натиснути «ОК»;

в) використати команду CACLS.

3. Вивчити управління доступом до реєстру Windows за допомогою Regedit.

4. Вивчити управління доступом до загальних (мережевих) ресурсів Windows за допомогою fsmgmt.msc.

5. Для управління доступом до загальних (мережевих) ресурсів через командний рядок необхідно використати: NET FILE, NET SHARE, NET SESSION

Методичні рекомендації

Управління доступом полягає в наданні користувачам, групам і комп’ютерів певних дозволів на доступ до об’єктів операційної системи.

Дозвіл являє собою правило, пов’язане з об’єктом ОС, яке визначає, яким користувачам і якого типу доступ до об’єкта дозволений.

Для кожного об’єкта або ресурсу ОС, підтримується контрольний список доступу (Access Control List - ACL). Він визначає перелік користувачів, яким дозволений доступ до даного об’єкта, а також тих, кому заборонений.

Кожен список контролю доступу (ACL) являє собою набір елементів контролю доступу (Access Control Entries, або ACE).

Для редагування і управління доступом до реєстру призначена стандартна утиліта Regedit. Управління доступом здійснюється аналогічно управлінню доступом до файлової системи, з тією відмінністю, що ACL встановлюються не для папок і файлів, а для розділів і ключів реєстру.

Управління доступом до загальних (мережевих) ресурсів

Файли і папки, що зберігаються на локальному комп’ютері, в мережі або в Інтернеті, можна передавати в загальний доступ. Файли і папки, що знаходяться в загальному доступі, менш захищені, ніж при відсутності загального доступу до них. Користувачі, що мають доступ до комп’ютера по мережі, в залежності від встановлених дозволів, можуть переглядати, копіювати, змінювати, створювати або видаляти файли, що містяться в загальнодоступному місці.

Управління доступом до реєстру

Реєстр Windows являє собою реляційну базу даних, в якій акумулюється вся необхідна для нормального функціонування комп'ютера інформація про налаштування операційної системи, а також про використаний спільно з Windows програмний продукт і пристрій. Все що зберігаються в реєстрі дані представлені в стандартизованої формі і чітко структуровані відповідно до запропонованої розробниками Windows ієрархії.

HKEY_CLASSES_ROOT

Гілка HKEY_CLASSES_ROOT, зазвичай позначається в технічній документації абревіатурою HKCR, включає в себе ряд підрозділів, в яких містяться відомості про розширення всіх зареєстрованих в системі типів файлів і дані про COM-серверах, зареєстрованих на комп'ютері. Фактично, цю галузь з функціональної точки зору можна вважати аналогом ключа HKEY_LOCAL_MACHINE \ Software, оскільки тут зібрані всі необхідні операційній системі дані про файлових асоціаціях.

HKEY_CURRENT_USER

В гілці HKEY_CURRENT_USER, що позначається в документації абревіатурою HKCU, міститься інформація про користувача, що веде на комп'ютері поточний сеанс роботи, який обслуговується реєстром. В її підрозділах знаходиться інформація про змінні оточення, групах програм даного користувача, настройках Робочого столу, кольорах екрану, мережевих з’єднаннях, принтерах і додаткових настройках додатків. Ця інформація береться з підрозділу Security ID (SID) гілки HKEY_USERS для поточного користувача. Фактично, в цій галузі зібрані всі відомості, що відносяться до профілю користувача, що працює з Windows на даний час.

HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE (HKLM) — это ветвь, в которой содержится информация, относящаяся к операционной системе и оборудованию, например, тип шины компьютера, общий объем доступной памяти, список загруженных в данный момент времени драйверов устройств, а также сведения о загрузке Windows. Данная ветвь включает наибольшее количество информации в системном реестре Windows и нередко используется для тонкой настройки аппаратной конфигурации компьютера. Следует понимать, что хранящиеся в этой ветви данные справедливы для всех профилей, зарегистрированных в системе пользователей.

HKEY_USERS

Ветвь HKEY_USERS (HKU) содержит подразделы с информацией обо всех профилях пользователей данного компьютера. Один из ее подразделов всегда соотносится с подразделом HKEY_CURRENT_USER (через параметр Security ID

(SID) пользователя). Другой подраздел, HKEY_USERS\DEFAULT, содержит информацию о настройках системы в момент времени, предшествующий началу сеанса текущего пользователя.

HKEY_CURRENT_CONFIG

Ветвь HKEY_CURRENT_CONFIG (HKCC) содержит подразделы с информацией обо всех профилях оборудования, используемого в данном сеансе работы. Профили оборудования позволяют выбрать драйверы поддерживаемых устройств для заданного сеанса работы. Эта информация берется из подразделов HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.

Некорректное изменение хранящейся в реестре информации вполне способно нарушить работоспособность Windows. *Достаточно допустить ошибку в записи значения какого-либо ключа или параметра, и пользователь больше не сможет загрузить компьютер. Именно по этой причине разработчики Windows заметно ограничили доступ к реестру, и редактировать параметры реестра, касающиеся безопасности, могут только пользователи* Windows, *имеющие в системе учетную запись Администратора.*

Контрольні запитання

1. Як здійснюється управління доступом до загальних (мережевих) ресурсів?
2. Як здійснюється управління доступом до реєстру
3. У чому полягає управління доступом?

Лабораторна робота №5

СИСТЕМА НАДАННЯ ДОСТУПУ НА ОСНОВІ ДИСКРЕТНОЇ МАТРИЦІ РОЗПОДІЛЕННЯ ДОСТУПУ

Навчальні питання:

1. Дискретна матриця (таблиця) надання доступів.

Завдання

Написати найпростішу дискретну матрицю (таблицю) надання доступів у будь-якій довільній системі, наприклад: адміністратор -> офіційний користувач з логіном та паролем доступу в систему.

Методичні рекомендації

Доступність інформації - стан інформації (ресурсів автоматизованої інформаційної системи), при якому суб’єкти, що мають права доступу, можуть реалізовувати їх безперешкодно. До прав доступу відносяться: право на читання, зміна, зберігання, копіювання, знищення інформації, а також права на зміну, використання, знищення ресурсів. Системи надання доступів в середовищах ТЗІ надаються за декількома принципами та можуть бути розширені дослідниками до будь-яких розмірів. Однією з таких систем є система надання доступів на основі дискретної матриці розподілення доступів.

Контрольні запитання

1. Що таке розмежування доступу?
2. Як здійснюється розмежування доступу?
3. Дайте визначення матриця повноважень це...
4. Що таке правила розмежування доступу?
5. Що таке розмежування за рівнями таємності?

Лабораторна робота №6
УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ (ROLE BASED ACCESS CONTROL)

Навчальні питання:

1. Система надання доступу «RBAC».

Завдання

Реалізувати найпростішу систему надання доступу «RBAC» програмно або візуалізовано у вигляді схеми на реальному прикладі довільного інформаційного середовища. Пояснити роботу такої реалізованої моделі.

Методичні рекомендації

Управління доступом на основі ролей (англ. Role Based Access Control, RBAC) - розвиток політики виборчого управління доступом, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі. Формування ролей покликане визначити чіткі і зрозумілі для користувачів комп'ютерної системи правила розмежування доступу. Рольове розмежування доступу дозволяє реалізувати гнучкі, динамічні в процесі функціонування комп'ютерної системи правила розмежування доступу. Таке розмежування доступу є складовою багатьох сучасних комп'ютерних систем. Як правило, даний підхід застосовується в системах захисту СУБД, а окремі елементи реалізуються в мережевих операційних системах. Рольовий підхід часто використовується в системах, для користувачів, у яких чітко визначено коло посадових повноважень і обов'язків.

Список джерел, необхідних для виконання завдання:

1. https://cleverics.ru/digital/2015/06/upravlenie-dostupom-na-osnove-rolej-preimushhestva-praktika-osobennosti/
2. https://www.securitylab.ru/contest/395442.php

Контрольні запитання

1. Стандарти рольового підходу до управління доступом.
2. Дайте визначення базової моделі RBAC.
3. Можливості та застосування RBAC.
4. Підходи до контролю доступу.

Лабораторна робота №7
ПРОЦЕДУРИ ВИЗНАЧЕННЯ ТА НАДАННЯ ПРАВ ДОСТУПУ ДО РЕСУРСІВ І УПРАВЛІННЯ ЦИМ ДОСТУПОМ

Навчальні питання:

1. Поняття ідентифікації, аутентифікації та аудиту.
2. Види облікових записів користувачів комп'ютерної системи.
3. Порядок аутентифікації й авторизації у комп'ютерних системах
4. Робота з утилітами перехоплення й розшифровки парольних хешей програмою Cain&Abel.

Завдання

1. Запустіть програму. Ознайомтесь з можливостями основних пунктів меню: Конфігурації (Configure), Сервіс (Tools).
2. Створіть на вашій робочій станції кілька локальних користувачів з паролями різної довжини й складності. При створенні користувачів не встановлюйте флаг «User must change password at next logon». Також створіть загальний каталог, з ім'ям «Test», і надайте створеним вами користувачам права на нього.
3. Відкрийте пункт меню Конфігурації (Configure), на вкладці «Sniffer», виберіть ваш мережний адаптер і натисніть OK. Потім натисніть на кнопку Start Sniffer і перейдіть на вкладку Sniffer, у ній на вкладку Passwords, для того щоб переглянути інформацію про перехоплені паролі.

4. Попросіть сусіда підключитися до вашого комп’ютера за мережею від імені створених вами користувачів, для цього можна скористатися меню директорії «Сервіс» (Service), «Підключити мережний диск» (Map Network Drive) із параметром «Підключити, використовуючи ім’я» (Connect using a 129 different user name). Переконайтеся, що в контейнері SMB є перехоплені парольні хеші.
5. Переглянете кількість завантажених хеш. Для цього в контекстному меню Send all to Cracker виберіть перехоплені парольні хеші, із вкладки Cracker, потім виберіть меню (Dictionary Attack NTLM + Challenge) для перегляду інформації про кількість завантажених хеш.
6. Здійсніть перебір паролів методом, залежно від вашого варіанта.
7. Протестуйте пароль, за допомогою команди «Тестувати пароль» (Test Password), контекстного меню.
8. Після закінчення лабораторної роботи видаліть створених вами користувачів і мережних дисків.

Методичні рекомендації

Ідентифікація - це присвоєння якому-небудь об’єкту або суб’єкту унікального образу, імені або числа. Встановлення дійсності (аутентифікація) полягає в перевірці, чи є об’єкт (суб’єкт), що перевіряється, справді тим, за кого себе видає.

Аутентифікація - це процедура доказу користувачем того, що він є тим, за кого себе видає, зокрема, доказ того, що саме йому належить введений ним ідентифікатор.

Аудит (audit) - це процес фіксації в системному журналі подій, зв'язаних з доступом до системних ресурсів, що захищаються.

Існує два типи облікових записів користувачів, доступних на комп’ютері: обліковий запис адміністратора комп’ютера і обліковий запис з обмеженими правами. Обліковий запис гостя доступний для користувачів, що не мають власних облікових записів на комп’ютері. Обліковий запис адміністратора комп’ютера

призначений для тих, хто може вносити зміни на рівні системи, встановлювати програми і мати доступ до усіх файлів на комп'ютері. Користувач з обліковим записом адміністратора комп’ютера має повний доступ до інших облікових записів користувачів на комп’ютері.

Для централізованого рішення задач аутентифікації й авторизації у комп’ютерних системах (мережах) призначена мережна служба Kerberos. Вона може працювати в середовищі багатьох популярних ОС, вбудована як основний компонент безпеки.

Утиліта Cain&Abel - це відновлення паролів. Відновити можна паролі входу в систему, загальні паролі, паролі екранної заставки, паролі доступу до мережі й будь-які інші, кэшируємі в системі, у зовнішньому PWL-файлі або в системному реєстрі. Cain&Abel має потужні засоби дешифрування.

Контрольні запитання

1. Як називають процес повідомлення суб'єктом свого імені або номера, з метою отримання певних прав доступу на виконання деяких (дозволених йому) дій в системах з обмеженим доступом?
2. Як називають процедуру перевірки відповідності суб’єкта і того, за кого він намагається себе видати, за допомогою якоїсь унікальною інформації?
3. Як називається процедура визначення та надання прав доступу до ресурсів і управління цим доступом?
4. Як називається умовне позначення знаків, призначених для підтвердження особи або повноважень, використовується для захисту інформації від несанкціонованого доступу, зберігається в секреті?
5. Які з видів аутентифікації (смарт-картка, токен, PIN код, відбиток пальця) відносяться до апаратної аутентифікації?
6. Назвіть правильний порядок здійснення санкціонованого доступу до ресурсів інформаційної системи.

Лабораторна робота №8
РОЗМЕЖУВАННЯ ДОСТУПУ СУБ'ЄКТІВ ДО ОБ'ЄКТІВ З МАНДАТНИМ ДОСТУПОМ

Навчальні питання:

1. Мандатний контроль доступу.

Завдання

Реалізувати програмне забезпечення з можливістю надання суб'єктам та об'єктам довільної системи мандатного доступу та їх контролю, з урахуванням роботи двох основних правил системи Белла-Лападули.

Методичні рекомендації

Мандатний контроль доступу (англ. Mandatory access control, MAC) - розмежування доступу суб'єктів до об'єктів, засноване на присвоєннях мітки конфіденційності для інформації, що міститься в об'єктах, і видачу офіційних дозволів (допуску) суб'єктам на звернення до інформації такого рівня конфіденційності. Також, іноді, перекладається як «примусовий контроль доступу». Це спосіб, що поєднує захист і обмеження прав, що застосовується по відношенню до комп'ютерних процесів, даних і системних пристроїв і призначений для запобігання їх небажаного використання.

Список джерел, необхідних для виконання завдання:

1. https://habr.com/ru/company/avanpost/blog/482060/
2. http://masters.donntu.org/2006/fvti/zhidkih/ind/kyrs/chapter/chapter4/menu3.html
3. https://studme.org/179763/informatika/model_bella_lapadula

Контрольні запитання

1. Особливості мандатного контролю доступу.
2. Де використовується мандатний контроль доступу?
3. З яких компонентів складається мандатний контроль доступу?

Лабораторна робота №9

РОЗМЕЖУВАННЯ ДОСТУПУ ЗА ДОПОМОГОЮ МОДЕЛЕЙ БЕЗПЕКИ BELL-LAPADULA ТА BIBA

Навчальні питання:

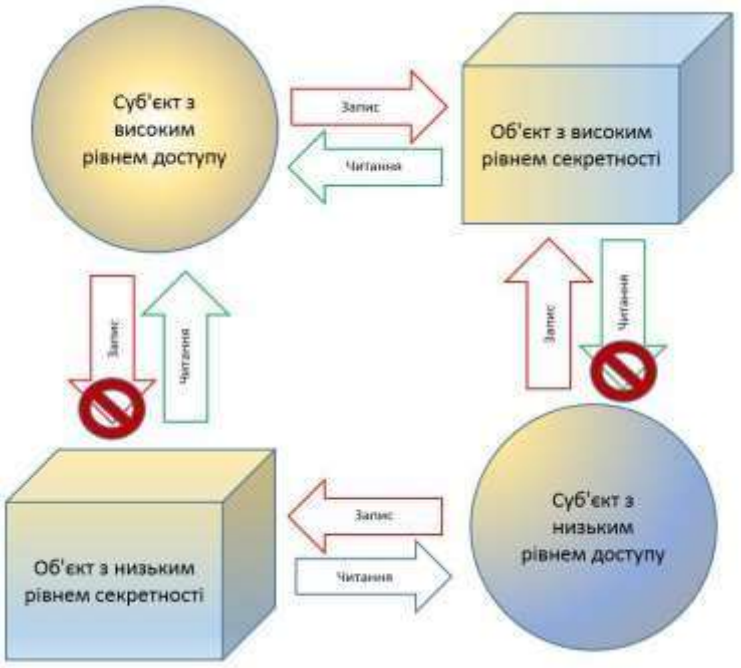
1. Модель контролю і управління доступом Белла-ЛаПадула.
2. Модель контролю і управління доступом Biba.

Завдання

Реалізувати систему надання доступів Белла-Лападули та Біби програмно або візуалізовано у вигляді схеми на реальному прикладі довільного інформаційного середовища. Пояснити роботу такої моделі.

Методичні рекомендації

Основною проблемою інформаційної безпеки та систем технічного захисту інформації є проблема розмежування доступу. Справді, якби не існувало проблеми розмежування доступу і вся інформація була б відкритою і загальнодоступною, то не було б потреби і в самій інформаційній безпеці, а також у винайденні нових моделей безпеки.



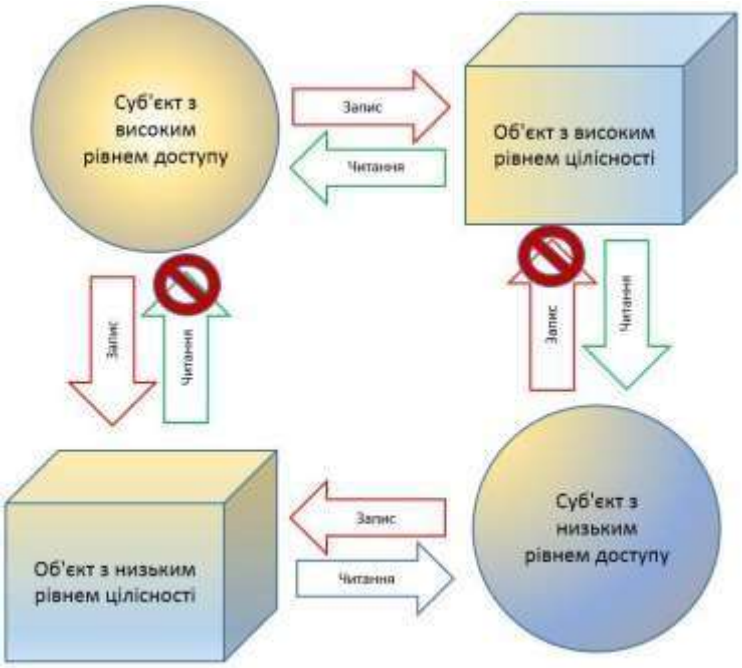
Модель Белла-Лападули

Модель контролю і управління доступом Белла-ЛаПадула заснована на мандатної моделі управління доступом, але не повністю повторює її. У моделі Белла-ЛаПадула аналізуються умови, при яких неможливе створення інформаційних потоків від суб'єктів з більш високим рівнем доступу до суб'єктів з більш низьким рівнем доступу.

Модель Biba захищає цілісність інформації в рамках системи і що відбуваються в ній процесів. Вона враховує першу мету цілісності:

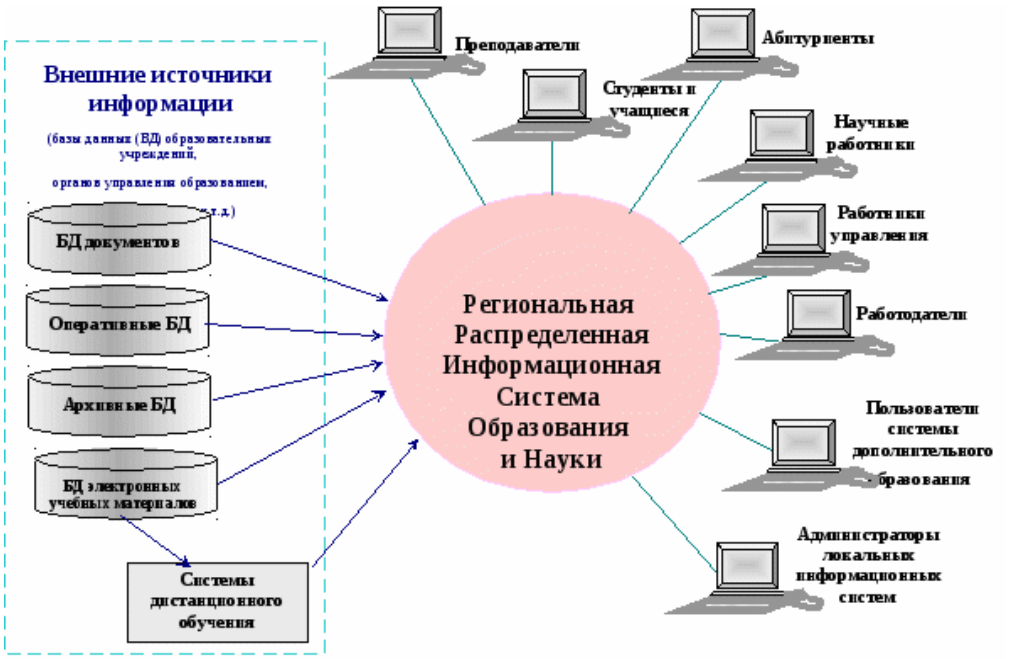
1. Суб'єкт не може читати дані з більш низького рівня цілісності («не читати знизу»).

2. Суб'єкт не може змінювати об'єкт на більш високому рівні цілісності («не писати вгору»).



Модель Біба

Приклад інформаційного середовища



Список джерел, необхідних для виконання завдання:

https://www.olifer.co.uk/new_rus/CN-5ed/cn5-aditions/formal-models.htm

Контрольні запитання

4. Надати визначення наступним поняттям: модель безпеки, доступ до інформації, управління доступом, повноваження доступу, право доступу, суб’єкт та об’єкт доступу, правила розмежування доступу.
5. Коротко охарактеризувати модель мандатного доступу.
6. Коротко охарактеризувати модель безпеки Белла-ЛаПадула.
7. В чому полягає основна відмінність між дискреційним і мандатним розмежуванням доступу?
8. Коротко охарактеризувати модель безпеки Біба.

Лабораторна робота №10
ОРГАНІЗАЦІЯ СИСТЕМ НАДАННЯ ДОСТУПУ В ОПЕРАЦІЙНИХ СИСТЕМАХ, СЕСІЙНИЙ КОНТРОЛЬ ДОСТУПУ

Навчальні питання:

1. Протокол шифрування даних.
2. Цифровий сертифікат.

Завдання

Проаналізувати всі моделі контролю надання доступів в системах технічного захисту інформації та інформаційних середовищах, визначити їх сильні та слабкі сторони та реалізувати систему надання доступу в будь-якій ОС (або іншому інформаційному середовищі) – сертифікат безпеки.

Методичні рекомендації

SSL (Secure Socket Layer) - протокол шифрування даних, якими обмінюються клієнт і сервер, - став найбільш поширеним методом захисту в Інтернеті. Колись він був розроблений компанією Netscape. Безпечний обмін забезпечується за рахунок шифрування і аутентифікації цифрового сертифікату. Цифровий сертифікат - файл, який унікальним чином ідентифікує сервери. Зазвичай цифровий сертифікат підписується і завіряється спеціалізованими центрами. Їх називають центрами сертифікації або засвідчуючими центрами.

Список джерел, необхідних для виконання завдання:

1. https://habr.com/ru/post/352722/
2. https://habr.com/ru/company/tuthost/blog/150433/

Контрольні запитання

1. Що таке протокол шифрування даних?
2. Які є права доступу?
3. Який компонент операційної системи є її центральною частиною, що керує виконанням програм та їх доступом до ресурсів комп’ютера?

4. Які є моделі контролю та надання доступу?
5. Що таке системи технічного захисту інформації?

Теми для самостійної роботи

1. Побудова системи інформаційної безпеки організації з використанням можливостей СКУД (система контролю і управління доступом).
2. Захист інформації в локальних обчислювальних мережах організації.
3. Забезпечення інформаційної безпеки організації.
4. Основні види політик управління доступом та інформаційними потоками.
5. Політики дискреційного, мандатної, рольового управління доступом, ізольованою програмного середовища і безпеки інформаційних потоків.
6. Модель матриці доступів Харрісона-Руззо-Ульмана.
7. Класична модель поширення прав доступу Take-Grant.
8. Правила перетворення графів доступів та інформаційних потоків.
9. Інтерпретації моделі Белла-ЛаПадули.
10. Модель систем військових сполучень.
11. Автоматна модель безпеки інформаційних потоків.
12. Програмна модель контролю інформаційних потоків.
13. Суб’єктно-орієнтована модель ізольованого програмного середовища.
14. Базова модель рольового управління доступом.
15. Модель мандатного рольового управління доступом.
16. Взаємозв’язок положень і основні напрямки розвитку формальних моделей безпеки комп'ютерних систем.
17. Моделі цінності інформації.
18. Методи доступу до мережі.
19. Формальні моделі безпеки комп’ютерних систем.
20. Забезпечення безпеки комп'ютерних систем і мереж.

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ ТА ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

Базова література

1. Широчин В.П., Широчин С.В., Мухін В.Є. Основи безпеки комп'ютерних систем. Навч. посібник. - К.: "Корнійчук", 2009. – 286 с.
2. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев. – 2-е изд., испр. И доп. – М. : ФОРУМ: ИНФРА-М, 2019. – 352 с.
3. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
4. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие.– СПб: Университет ИТМО, 2014. – 95с.
5. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях М.: ДМК Пресс, 2012. – 592 с.
6. Деревянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2013. – 339с.

Допоміжна література

1. Куликов С. С. Модели безопасности компьютерных систем: учеб. пособие – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015. – 179с.
2. Юрий Диогенес Эрдаль Озкайя Кибербезопасность. Стратегии атак и обороны, ДМК Пресс, 2020. – 326с.

Інформаційні ресурси

1. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. защита программного обеспечения. Учебник и практикум для вузов - М.: Издательство Юрайт - 2019 - 312с. Режим доступу до ресурсу:

https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-437163

2. Landwehr, Carl. "Formal Models for Computer Security" Режим доступу до ресурсу: https://clck.ru/9ZtTv
3. Обзор и сравнение существующих методов управления доступом. Режим доступу до ресурса: http://www.ict.nsc.ru/ws/YM2003/6312/
4. RSBAC. RSBAC Security Modules. Режим доступу до ресурсу: https://clck.ru/9ZtQm

ЗМІСТ

ЕЛЕКТРОННЕ НАВЧАЛЬНЕ ВИДАННЯ

Сергій Вікторович Кухаренко

КОМПЛЕКСНІ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Методичні вказівки
до виконання лабораторних та самостійних робіт
з дисципліни

«Комплексні системи контролю та управління доступом»

для підготовки здобувачів вищої освіти
галузі знань 12 «Інформаційні технології»