Лабораторная работа № 6
«Защита ПК от несанкционированного доступа»

Цель работы:

Закрепление теоретического материала по изучению особенностей защиты ПК от несанкционированного доступа (НСД).

Изучение способов и систем защиты ПК.

Приборы и оборудование:

Персональный компьютер
ОС MS Windows 7 (MS Windows 10), MS Office, Браузер Microsoft Internet Explorer (Edge)

Пояснения к работе и задание:

Технические, организационные и программные средства обеспечения сохранности и защиты от несанкционированного доступа

Существует четыре уровня защиты компьютерных и информационных ресурсов:

1. Предотвращение предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.
2. Обнаружение предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.
3. Ограничение уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.
4. Восстановление обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.
5. Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблений.

1. Аутентификация пользователей.

Данная мера требует, чтобы пользователи выполняли процедуры входа в компьютер, используя это как средство для идентификации в начале работы. Для аутентификации личности каждого пользователя нужно использовать уникальные пароли, не являющиеся комбинациями личных данных пользователей, для пользователя. Необходимо внедрить меры защиты при администрировании паролей, и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению. Если в компьютере имеется встроенный стандартный пароль, его нужно обязательно изменить.

2. Правила соблюдения защиты пароля

Следующие *правила* полезны для защиты пароля:

· нельзя делится своим паролем ни с кем;
· пароль должен быть трудно угадываемым;
· для создания пароля нужно использовать строчные и прописные буквы, а еще лучше позволить компьютеру самому сгенерировать пароль;
· не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;

· предпочтительно использовать длинные пароли, так как они более безопасны, лучше всего, чтобы пароль состоял из 6 и более символов;
· пароль не должен отображаться на экране компьютера при его вводе;
· пароли должны отсутствовать в распечатках;
· нельзя записывать пароли на столе, стене или терминале, его нужно держать в памяти;
· пароль нужно периодически менять и делать это не по графику;
· на должности администратора паролей должен быть самый надежный человек;
· не рекомендуется использовать один и тот же пароль для всех сотрудников в группе;
· когда сотрудник увольняется, необходимо сменить пароль;
· сотрудники должны расписываться за получение паролей.

3. Процедуры авторизации

В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям.

В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

Практическая часть:
Выполнить программу на одном из языков программирования (например, PASCAL), осуществляющую функцию защиты файла паролем.

Ход выполнения задания:

1. Составить алгоритм
2. Использовать условные операторы
3. Создать необходимые циклы, один из которых использует функцию сравнения пароля 1 цикл на запуск программы используя число ввода пароля до 3
4. Завершение программы неудачей, если число ввода неверного пароля превысило N=3
5. Можете использовать следующие текстовые сообщения (примерные):

- «ВВЕДИТЕ ПАРОЛЬ ДЛЯ ВХОДА В ПРОГРАММУ» (Начало выполнения загрузки)
- «ПАРОЛЬ НЕВЕРНЫЙ! ИСПОЛЬЗУЙТЕ ЕЩЕ ОДНУ ПОПЫТКУ» (Если пароль введен некорректно)
- ДОБРО ПОЖАЛОВАТЬ! (Если пароль введен корректно)
- «ВЫ ПРЕВЫСИЛИ ДОПУСТИМОЕ ЧИСЛО ПОПЫТОК! ДО СВИДАНИЯ!» (Если количество неверных попыток ввода пароля превысило допустимое число N=3)

Ход выполнения лабораторной работы:

1. Изучить приведенный в методическом описании к лабораторной работе материал.
2. Ознакомиться с разделами с применением возможностей лаборатории.
3. Выполнить задание согласно практической части методического пособия.

4. Оформить отчет в установленной форме по разделам.
5. Ответить на контрольные вопросы.
6. Представить результаты работы преподавателю.

Контрольные вопросы:

1. Перечислите уровни защиты компьютерных и информационных ресурсов.
2. Сформулируйте функцию аутентификации и перечислите требования, предъявляемые к процедуре аутентификации.
3. Перечислите правила защиты пароля. Какие из них наиболее необходимы для выполнения?

Какие действия в рамках организационной защиты требуется выполнять для осуществления процедуры авторизации?