Комплексное задание II уровня состояло из следующих практических заданий:

I. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

1. Общие положения
2. Порядок доступа к конфиденциальной информации
3. Работа с криптографическими системами
4. Физическая безопасность
5. Разграничение прав доступа к программному обеспечению и системам хранения данных
6. Работа в глобальной сети Интернет
7. Дублирование, резервирование и раздельное хранение конфиденциальной информации

Структура Компании представляет собой:

- Руководство Компании;
- Отдел Защиты информации;
- Отдел информационных технологий;
- Офисный центр;
- Службу безопасности Компании;
- Пост охраны.

1. Общие положения

1.1 Настоящая Политика разработана в соответствии с действующим законодательством, нормативными актами и соотносимыми с ними положениями внутренних документов Компании. Она регламентирует порядок организации с целью обеспечения сохранности информации и ее безопасности в Компании, как в осуществлении текущей деятельности, так и в обозримом будущем.

1.2. Целями настоящей Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
-
-
-
-
-

1.3. К конфиденциальной информации Компании относится информация:

- относящаяся к коммерческой тайне в соответствии Федеральным законом от 29.07.2004 № 89-ФЗ "О коммерческой тайне";
- относящаяся к персональным данным в соответствии с Федеральным законом от 27.07.2016 № 152-ФЗ "Об информации, информационных технологиях и защите информации".

Общедоступная информация защите не подлежит, т.к. ее потеря не нанесет ущерб конфиденциальности.

2. Порядок доступа к конфиденциальной информации

2.1. В целях обеспечения защиты информации в Компании, устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

Решение о доступе работника к определенному разделу конфиденциальной информации принимает системный администратор Компании.

Отдел информационных технологий обеспечивает защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.

Доступ к компьютерной сети Компании осуществляется только с персональным паролем. Первоначальный пароль пользователя формируется системным администратором и не меняется во избежание забывания его пользователем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается. Имя пользователя и пароль на вход в АРМ должны быть одинаковы. Категорически запрещается снимать несанкционированные копии с носителей

конфиденциальной информации, разрешено только знакомить с содержанием электронной информации лиц, не допущенных к этому.

2.2 Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен скачать программу с общедоступных ресурсов сети Интернет. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования.

2.3 Работникам Компании запрещается:

-
-
-
-
-
-

3. Работа с криптографическими системами

3.1. К работе с криптографическими системами допускаются все работники Компании.

3.2. Секретные ключи электронно-цифровых подписей и шифрования могут храниться в сейфах или в других местах под ответственность лиц на то уполномоченных. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования должен быть обеспечен.

3.3. Выборочно разрешено:

- выводить секретные ключи и шифрования на дисплей компьютера или принтер;
- устанавливать в компьютер носитель секретных ключей и шифрования в непредусмотренных режимах функционирования;
- записывать на носитель секретных ключей и шифрования постороннюю информацию.

3.4. При компрометации секретных ключей, шифрования и прочей электронной информации в случае существования угрозы утечки информации Отделом информационных технологий принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и шифрования, паролей. По факту компрометации организуется уведомление Руководства Компании.

4. Физическая безопасность

4.1. Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, основной маршрутизатор, файервол) находятся внутри офисного центра, доступ в который разрешен работникам, имеющими соответствующее разрешение от Руководства Компании.

4.2. Вход в помещение осуществляется через металлическую дверь, оснащенную замками (не менее двух) и переговорным устройством. Копии ключей находятся у вахтера.

4.3. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Вход в помещение контролируется системой видео наблюдения с выходом на мониторы установленные внутри помещения.

4.4. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах. Запасные ключи от сейфов хранятся у системного администратора.

4.5. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находиться в помещении в связи с выполнением своих должностных обязанностей.

4.6. Доступ в помещение в неурочное время или в выходные и праздничные дни осуществляется с устного разрешения Руководства компании

5. Разграничение прав доступа к программному обеспечению и системам хранения данных

5.1. Для входа в компьютерную сеть Компании работник должен ввести имя и пароль. Не допускается режимы беспарольного (гостевого) доступа к какой-либо конфиденциальной информации.

5.2. В целях защиты конфиденциальной информации Компании организационно и технически разделяются подразделения Компании, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности, секретности и смысловой направленности). Данная задача решается с использованием сетевой операционной системы, где в целях обеспечения защиты данных доступ и права пользователей ограничивается персональными каталогами. Права назначаются в соответствии с производственной необходимостью, определяемой начальником подразделения.

5.3. Параметры входа в сеть, имя и пароль, пользователем не разглашаются. Копии на бумажном носителе сдаются системному администратору. В случае компрометации пароля пользователь должен незамедлительно самостоятельно поменять пароль.

5.4. При работе с АРМ имя пользователя и пароль должны быть отличны от имени пользователя и пароля при входе общую компьютерную сеть Компании. Пароль должен быть не менее восьми символов. Категорически запрещается сообщать свой пароль другим лицам, а также пользоваться чужими паролями. Все действия пользователя, работающего с АРМ, протоколируются. Журнал операций храниться не менее шести месяцев.

6. Работа в глобальной сети Интернет

6.1. К работе с ресурсами сетью Интернет допускаются все работники.

6.2. Работа работников Компании с электронной корпоративной почтой сети Интернет допускается на основании отдельного разрешения от Руководства Компании.

6.3. При работе с сетью Интернет работникам разрешено:

Скачивать и устанавливать на компьютер программное обеспечение.

Посещать ресурсы, не имеющие непосредственного отношения к работе и служебным обязанностям.

Осуществлять подписку на рассылку информации непроизводственного характера.

Сообщать адрес электронной почты в непроизводственных целях.

Пользоваться различными Интернет-пейджерами.

Использовать Интернет для получения материальной выгоды или непроизводственных целях, в том числе осуществляя торговлю через Интернет.

7. Дублирование, резервирование и раздельное хранение конфиденциальной информации

7.1. В целях защиты конфиденциальной информации от преднамеренного или же непреднамеренного ее уничтожения, фальсификации или разглашения обеспечить ежедневное обязательное резервирование всей информации, имеющей конфиденциальный характер.

Дублирование информации с использованием различных физических и аппаратных носителей.

7.2. Ответственность за хранение и резервирование информации в электронном виде возложить на пользователей ресурсов.

Сохранить исправленный файл под своим шифром на рабочем столе компьютера.

II Задание: Обеспечить защиту автоматизированных рабочих мест с учетом специфики специальности.

Вводные данные:

1 Организация восстановления штатными средствами ОС Windows 7 Professional SP1

1.1 Зайти в систему под учётной записью «Администратор» без ввода пароля.

ВНИМАНИЕ!!! Пароль учетной записи «Администратор» не устанавливать - для итоговой проверки жюри.

1.2 Включить настройку восстановления системы для диска C:\\ и отвести под создание точек восстановления 10% дискового пространства.

Создать вручную контрольную точку восстановления с названием ПКТ - Первая Контрольная Точка.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

2 Организация доступа в систему штатными средствами ОС Windows 7 Professional SP1

2.1 Организовать доступ в ОС по ключевому USB носителю.

Организовать защиту БД учётных записей Windows (SAM) при помощи системной команды «syskey». Ключевой файл разместить на USB носитель.

При перезагрузке вход в систему должен быть возможен только по наличию USB носителя с ключевым файлом.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

3 Администрирование учетных записей штатными средствами ОС Windows 7 Professional SP1

3.1 Создать учетную запись с правами Пользователя, с именем личного шифра участника и паролем на учётную запись: Do$tUp2.

Создать учётную запись «Администратора безопасности» с именем «Sec_Admin», пароль 735P@roL -1 балл

3.2 Скрыть отображение учётной записи «Администратора безопасности» «Sec_Admin» из панели управления учётных записей, при этом учетная запись должна оставаться активной.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

3.3 Под учётной записью «Администратора безопасности» «Sec_Admin», настроить общие параметры пользователей: - 1 балл

- максимальный срок действия пароля – 60 дней;
- использование сложных паролей;
- длина пароля - 8 знаков;
- хранить пароли с учетом обратимого шифрования.

3.4 Под учётной записью «Администратора безопасности» «Sec_Admin», настроить параметры блокировки: – 1 балл

- количество ошибок ввода пароля – 2;
- продолжительность блокировки учётной записи – 2 мин.

3.5 Настроить запрет на отображение при входе в систему последнего активного пользователя.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

3.6 Под учётной записью «Администратора безопасности» «Sec_Admin», настроить аудит входа в систему - по отказу.

Очистить журнал просмотра событий безопасности, завершить сеанс текущего пользователя.

Заблокировать учетную запись «Пользователя с именем шифра участника» путем ввода неправильного пароля. Найти событие блокировки пользователя с демонстрацией имени заблокированной учёной записи.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

4 Настройка автозагрузки носителей штатными средствами ОС Windows 7 Professional SP1

4.1 Отключить автозагрузку носителей для «Пользователя с именем шифра участника» через панель управления компьютером.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

4.2 Отключить автозагрузку носителей для «Пользователя с именем шифра участника» в редакторе локальной групповой политики.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

5 Настройка дискреционной и ролевой моделей доступа штатными средствами ОС Windows 7 Professional SP1

5.1 Настройка ролевой модели доступа.

Создать новую группу для пользователей с названием «Участник», добавить в эту группу «Пользователя с именем шифра участника».

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

5.2 Настройка дискреционной модели доступа.

Администратором безопасности создать на локальном диске C:\\ папку с именем «Хранилище» содержащую в себе: папку с названием «Оборудование», сжатую ZIP-папку с именем «Документы» и папку «Отчётность».

Настроить следующие права доступа к папке для «Пользователя с именем шифра участника»:

- возможность чтения данных во всех папках кроме папки «Отчётность» – 1 балл

- возможность чтения документов в остальных папках без возможности их удаления – 1 балл

- в папке «Оборудование» должна быть возможность создавать, но не изменять существующие документы – 1 балл

6 Применение прикладной программы шифрования VeraCrypt. Применение токенов безопасности.

6.1 Установить программу VeraCrypt с USB носителя.

6.2 Создать зашифрованный контейнер TOM1 с применением алгоритма Twofish и алгоритма хеширования Whirlpool, сохранить его на USB-накопитель и организовать доступ TOM1 по ключевому файлу на Рутокене без пароля – 1 балл

6.4 Создать скрытый зашифрованный контейнер TOM2, установив в качестве пароля шифр участника – 1 балл

7 Архивирование, информации штатными средствами ОС Windows7 Professional SP1. Восстановление и надежное удаление с применением прикладной программы Recuva.

7.1 Установить ПО Recuva с USB накопителя

7.2 Проверить USB накопитель на наличие остаточных данных, восстановить их и перенести в созданный ранее скрытый зашифрованный контейнер TOM2 – 1 балл

7.3 Надежно удалить с USB накопителя файл «Политика информационной безопасности» методом Гуттмана, отобразив выбранный метод на отснятом скриншоте.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

7.4 В папке C:\\ «Хранилище»\ «Оборудование» создать папку с именем «Аудит»\ содать в ней документ в формате RTF с произвольным содержанием. Произвести настройку политики аудита данного каталога со следующими параметрами: удаление по ‘успеху’ и ‘отказу’ для «Пользователя с именем шифра участника» .

Для контроля выполнения данного пункта под «Пользователем с именем шифра участника» и произвести попытку удаления файла с расширением RTF.

Найти в журнале строку с адресом и действием данного события.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

7.5 Настроить ежедневное архивирование всех файлов «Пользователя с именем шифра участника» с на USB накопитель за исключением библиотеки «Музыка», дополнительного расположения «Ссылки» и «Загрузки».

Перед запуском архивации Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

10.02.02 Вариативная часть

8 Настройка активных соединения и открытых портов штатными средствами ОС Windows 7 Professional SP1.

8.1 Определить открытые порты и процессы использующие их, выявить процессы использующие «опасные» порты 135-139,445.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

8.2 По PID определить тип процесса через командную строку или диспетчер задач использующие «опасные» порты.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

8.3 Закрыть «опасные» соединения 135-139 брандмауэром ОС Windows7 Professional SP1.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

8.4 Закрыть порт 445 с применением команды «Netsh».

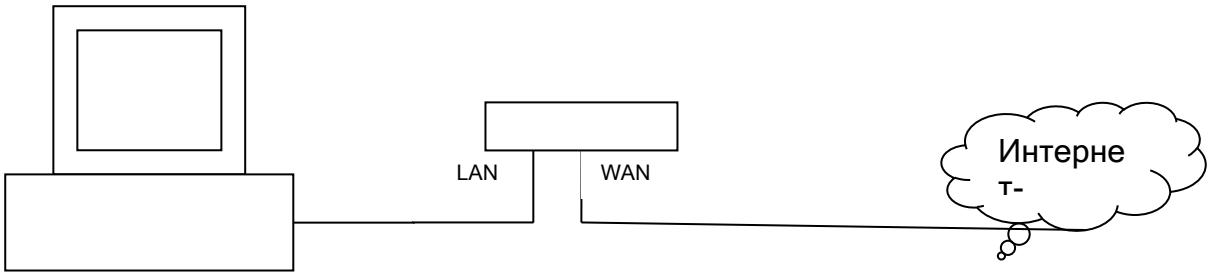
Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

9 Организация VPN соединения с применением межсетевого экрана D-Link DFL-260E

9.1 Для доступа к веб интерфейсу использовать по умолчанию URL https://192.168.1.1 . Имя – admin, пароль – admin. Проверить корректность физических подключений устройства, работоспособность патч-кордов, индикацию на устройстве, проверить корректность сетевых настроек компьютера -1 балл

9.2 Организовать подключение к Интернет провайдеру с применением межсетевого интерфейса, настроить сетевые настройки компьютера, произвести настройку межсетевого экрана, lan, wan – интерфейсов, организовать пользователя user, группу localusers

-1 балл



9.3 Проверить соединение с Интернет провайдером утилитой ping, проверить соединение до межсетевого экрана.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

9.4 Создать правила IP Rule со следующими параметрами:

Имя - all_services,

Action - NAT

service - all_services

Настроить Sourse Interface, Source Network, Destination Interface, Destination Network

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

9.5 Настроить L2TP/PPTP- туннель. Для выхода в Интернет через L2TP/PPTP- туннель изменить правила доступа, где в качестве параметров Source Interface использовать созданный интерфейс L2TP/PPTP

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

9.6 Настроить PPPoE-подключения. Для выхода в Интернет через - PPPoE - туннель изменить правила доступа IP Rules, где в качестве параметра wan использовать созданный интерфейс PPPoE(PPPoE_inet)

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл.

10.02.03 Вариативная часть

8 Проверка и восстановление целостности системных файлов ОС Windows при помощи команды ‘SFC’

8.1 Выполнить проверку целостности системных файлов и определить нарушение целостности ОС. Зафиксировать отсутствие конкретного системного файла.

сделать скриншот экрана - нажатием кнопки PrintScreen -1балл

8.2 Найти и скопировать файл журнала отчёта о проверке целостности в папку «Аудит» – 1 балл

8.3 Штатными средствами ОС восстановить повреждённый системный файл, зафиксировав его имя и процесс восстановления.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

8.4 Скопировать файл журнала отчёта с указанием имени восстановленного системного файла и его пути в папку «Аудит».

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

8.5 Настроить проверку целостности всех защищаемых системных файлов при каждой загрузке ОС.

Сделать скриншот экрана - нажатием кнопки PrintScreen – 1 балл

9 Создание ключей и сертификатов штатными средствами ОС Windows7

9.1 Используя приложение CMD Shell Microsoft Windows SDK 7.0, при помощи команды makecert.exe, создать сертификат конечного пользователя со следующими параметрами:

- ключ экспортируемый;
- сертификат самозаверяющийся;
- область применение ключа - ЭЦП.

Сохранить ключ (key.pvk) и сертификат (key.cer) в папку C:\\CERT' с паролем 100203 – 1 балл

9.2 Используя команду 'pvk2pfx' создать 'key.pfx' с поддержкой Software Publisher Certificate (SPC), с паролем 100203 – 1 балл

9.3 Импортировать полученный сертификат на рутокен – 1 балл

9.4 Настроить применение сертификата для подписи документа. Разместить сертификат в папке: Доверенные корневые центры сертификатов и в папку «Личные» – 1 балл

9.5 Выполнить подпись ЭЦП документа формата PDF на USB носителе в Adobe Acrobat - 1 балл