Задания заключительного этапа
Всероссийской олимпиады профессионального мастерства обучающихся по специальностям среднего профессионального образования, входящим в укрупненную группу **10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**10.02.02 Информационная безопасность телекоммуникационных систем**

 **10.02.03 Информационная безопасность в автоматизированных системах**

|  |
| --- |
| Комплексное задание I уровня состояло из следующих теоретических вопросов и практических задач: |
| Атака «Отказ в обслуживании» осуществляется за счет … |
| - завладения паролем |
| - перехвата сетевых пакетов |
| - подмена IP - адреса |
| - превышения допустимых пределов функционирования сети |
| Блок информации, применяемый для защиты от навязывания ложной информации, зависящий от ключа и данных- это.. |
| - имитовставка |
| - имитозащита |
| - МАС |
| - ЭЦП |
| В алгоритмах электронной подписи подписывание производится … |
| - закрытым ключом отправителя |
| - закрытым ключом получателя |
| - открытым ключом отправителя |
| - открытым ключом получателя |
| В асимметричных алгоритмах зашифровывание производится … |
| - закрытым ключом отправителя |
| - закрытым ключом получателя |
| - открытым ключом отправителя |
| - открытым ключом получателя |
| Государственная тайна – это … |
| - защищаемая информация, получение либо использование которой может стать причиной ущерба РФ |
| - защищаемые государством сведения в военной, внешнеполитической, экономической, оперативной, разведывательно-контрразведывательной деятельности |
| - любая конфиденциальная информация, обрабатываемая в государственных организациях |
| - совокупность административных, организационных и технических мер безопасности |
| Действия злоумышленников относятся к … |
| - разглашению информации |
| - угрозам преднамеренных воздействий |
| - угрозам случайных воздействий |
| - угрозам утечки информации |
| Если операционная система позволяет следующему субъекту использовать некий объект без его предварительной надежной очистки, какую проблему безопасности это вызывает? |
| - компрометация домена выполнения |
| - несанкционированный доступ к привилегированным процессам |
| - раскрытие остаточных данных |
| - утечка данных по скрытым каналам |
| Идентификатор Проксимити-карт использует для активации… |
| - ИК-канал |
| - магнитное поле |
| - электрическое поле |
| - электро-магнитное поле |
| Интересы личности в информационной сфере заключаются в … |
| - защите данных от случайных или преднамеренных разглашений |
| - обеспечении суверенитета и территориальной целостности |
| - реализации конституционных прав человека и гражданина на доступ к информации |
| - реализации свобод человека и гражданина на доступ к информации |
| К средствам обеспечения защиты информации по акустическому каналу утечки информации относится: |
| - детектор излучений |
| - сканер частот |
| - тепловизор |
| - шумомер |
| К средствам обеспечения защиты информации по радиоэлектронному каналу утечки информации относится: |
| - индикатор электромагнитного поля |
| - мультиметр |
| - тепловизор |
| - шумомер |
| Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины с применением односторонних функций? |
| - кодирование |
| - сжатие |
| - хеширование |
| - шифрование |
| Как называется функция, эффективно вычисляемая за полиноминальное время на детерминированной машине Тьюринга, для которой не существует полиноминальной вероятностной машины Тьюринга, которая обращает функцию? |
| - вероятностная |
| - односторонняя |
| - полиноминальная |
| - экспоненциальная |
| Какая модель управления доступом является групповой? |
| - дискреционная |
| - мандатная |
| - на основе идентификации |
| - ролевая |
| Какое безопасное расстояние должно быть от глаз до монитора при работе на ПЭВМ |
| - 30…40 см |
| - 40…50 см |
| - 60…70 см |
| - 90…100 см |
| Какое из перечисленных ниже действий не является частью процесса управления конфигурациями? |
| - конфигурирование и настройка операционной системы |
| - конфигурирование и настройка приложения |
| - конфигурирование оборудования |
| - передача официального запроса |
| Какой из следующих пунктов лучше всего описывает ядро безопасности? |
| - программный компонент, который изолирует процессы, разделяет защищенный и реальный режимы |
| - программный компонент, который определяет, имеет ли пользователь право выполнять запрошенную операцию |
| - программный компонент, который отслеживает действия и записывает информацию о событиях безопасности в журнал регистрации событий |
| - программный компонент, который работает в самом центре колец защиты и обеспечивает интерфейсы между доверенными и недоверенными объектами |
| Какой уровень шума считается максимально допустимым при работе оператора ПЭВМ |
| - 30 дБ |
| - 50 дБ |
| - 70 дБ |
| - 80 дБ |
| Лицензирование это - |
| - подтверждение подлинности отправителя и получателя информации |
| - подтверждение соответствия продукции или услуг установленным требованиям и стандартам |
| - процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ |
| - средство защиты информации от несанкционированного доступа |
| На каком этапе проекта впервые должны быть учтены вопросы безопасности? |
| - на этапе внедрения |
| - на этапе интеграционного тестирования |
| - на этапе разработки технического задания |
| - на этапе функционального проектирования |
| Назовите показатель сравнительной эффективности капиталовложений на информационную безопасность предприятия: |
| - объем выполняемых работ |
| - производительность труда |
| - срок окупаемости |
| - трудоемкость |
| Ограждения объекта защиты сеткой относятся к : |
| - дополнительным |
| - заградительным |
| - основным |
| - предупредительным |
| Операционная система выполняет все, за исключением какой из перечисленных ниже задач? |
| - доступ пользователей к представлениям базы данных |
| - задачи ввода/вывода |
| - распределение памяти |
| - распределение ресурсов |
| Оптико-электронный извещатель предназначен для: |
| - обнаружения возникновения задымления |
| - обнаружения изменения потока ИК излучения |
| - обнаружения проникновения через двери и окна |
| - обнаружения разбития окон |
| Перехват сетевых пакетов, передаваемых по линиям передачи данных в сети – это… |
| - DoS –атака |
| - Атака «man-in-the-middle» |
| - Подмена (спуфинг) |
| - Подслушивание (сниффинг) |
| Побочные излучения и наводки относятся к … |
| - разглашению информации |
| - угрозам преднамеренных воздействий |
| - угрозам природного характера |
| - угрозам утечки информации |
| Под информационной безопасностью Российской Федерации понимается состояние … |
| - защищенности национальных интересов в информационной сфере |
| - неприкосновенности национальных интересов в информационной сфере |
| - развития национальных интересов в информационной сфере |
| - стабильности национальных интересов в информационной сфере |
| Политика безопасности оформляется |
| - в виде документа, включающего описание проблемы, область применения, позицию организации, распределение ролей, санкции |
| - в виде инструкции по действию сотрудников в критических ситуациях |
| - в виде отчета обо всех действиях пользователей; |
| - в виде приказа о назначении ответственных лиц |
| Политика безопасности строится на основе |
| - анализа рисков, признанных реальными для данной организации |
| - программы действий, реализация которых обеспечит информационную безопасность; |
| - стратегии управления защиты |
| - финансовых данных |
| Предназначение стандартов информационной безопасности |
| - оценка уровня безопасности, обеспечиваемый продуктами ИТ |
| - практического решения вопросов управления информационной безопасностью |
| - создание основы для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов ИТ |
| - средство сравнения конкретных продуктов ИТ |
| Принцип обеспечения безопасности аппаратно-программного модуля доверенной загрузки: |
| - перехватывает работу компьютера до загрузки BIOS, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера. |
| - перехватывает работу компьютера после загрузки BIOS, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера. |
| - перехватывает работу компьютера прерывая загрузку BIOS, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера. |
| - перехватывает работу компьютера прерывая загрузку ОС, загружает CriptoBIOS и идентифицирует пользователя по ключу и паролю, после чего продолжает загрузку компьютера. |
| Сертификация ... |
| - выпуск удостоверяющим центром электронного или печатного документа, подтверждающего принадлежность владельц открытого ключа или каких-либо атрибутов |
| - основывается на Законе РФ "О государственной тайне" |
| - регулируется секретными нормативными документами |
| - это подтверждение соответствия продукции или услуг установленным требованиям или стандартам |
| Подмена (спуфинг) –это… |
| - анализ сетевого трафика |
| - перехват данных |
| - посредничество в обмене незашифрованными ключами |
| - фальсификация IP-адреса |
| Структура затрат на информационную безопасность предприятия - это: |
| - все статьи затрат на информационную безопасность |
| - калькуляция себестоимости затрат на информационную безопасность |
| - состав затрат и часть каждого элемента в их общем объеме |
| - часть каждого элемента затрат на информационную безопасность |
| Что из перечисленного ниже входит в состав ядра безопасности? |
| - политика безопасности, защитные механизмы и структура системы |
| - политика безопасности, механизмы защиты и программное обеспечение |
| - программное обеспечение, аппаратное обеспечение и прошивки |
| - программное обеспечение, аппаратное обеспечение и структура системы |
| Что из перечисленного ниже, лучше всего описывает удостоверяющий центр? |
| - организация, которая выпускает закрытые ключи и соответствующие алгоритмы |
| - организация, которая выпускает сертификаты |
| - организация, которая проверяет ключи шифрования |
| - организация, которая проверяет процессы шифрования |
| Что подразумевается, когда говорят, что компьютеры взаимодействуют друг с другом физически и логически? |
| - они взаимодействуют физически при подключении к магистральной сети, а логически – при взаимодействии в рамках одной локальной сети (LAN) |
| - они взаимодействуют физически с помощью заголовков и окончаний, а логически – посредством физических соединений |
| - они взаимодействуют физически с помощью электронов и сетевых кабелей, а логически – посредством различных уровней модели OSI |
| - они взаимодействуют физически через PVC, а логически – через SVC |
| Что такое процедура? |
| - обязательные действия |
| - пошаговая инструкция по выполнению задачи |
| - правила использования программного и аппаратного обеспечения в компании |
| - руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах |
| Что является заключительным этапом жизненного цикла процесса разработки системы? |
| - аккредитация |
| - разработка |
| - сертификация |
| - тестирование модулей |
| Электронный ключ Touch memory использует для хранения идентификатора: |
| - магнитные носители |
| - полупроводниковые элементы электронного носителя ОЗУ |
| - полупроводниковые элементы электронного носителя ПЗУ |
| - химико-физические свойства оптического носителя |
| Прочитать предложенный текст, выбрать:- этапы построения системы защиты информации- перечень должностей, которые должны быть вовлечены в создание и подготовку документов по политике безопасности.Выполнить их перевод на русский язык.Network Working Group B. FraserRequest for Comments: 2196 EditorFYI: 8 SEI/CMUObsoletes: 1244 September 1997Category: Informational...1.5 Basic ApproachThis guide is written to provide basic guidance in developing asecurity plan for your site. One generally accepted approach tofollow is suggested by Fites, et. al. [Fites 1989] and includes thefollowing steps:Identify what you are trying to protect. Determine whatyou are trying to protect it from. Determine how likely the threats are.Implement measures which will protect your assets in a cost-effectivemanner. Review the process continuously and make improvements each timea weakness is found.Most of this document is focused on item 4 above, but the other stepscannot be avoided if an effective plan is to be established at yoursite. One old truism in security is that the cost of protectingyourself against a threat should be less than the cost of recoveringif the threat were to strike you. Cost in this context should beremembered to include losses expressed in real currency, reputation,trustworthiness, and other less obvious measures. Without reasonableknowledge of what you are protecting and what the likely threats are,following this rule could be difficult.1.6 Risk Assessment1.6.1 General DiscussionOne of the most important reasons for creating a computer securitypolicy is to ensure that efforts spent on security yield costeffective benefits. Although this may seem obvious, it is possibleto be mislead about where the effort is needed. As an example, thereis a great deal of publicity about intruders on computers systems;yet most surveys of computer security show that, for mostorganizations, the actual loss from "insiders" is much greater.Risk analysis involves determining what you need to protect, what youneed to protect it from, and how to protect it. It is the process ofexamining all of your risks, then ranking those risks by level ofseverity. This process involves making cost-effective decisions onwhat you want to protect. As mentioned above, you should probablynot spend more to protect something than it is actually worth.A full treatment of risk analysis is outside the scope of thisdocument. [Fites 1989] and [Pfleeger 1989] provide introductions tothis topic. However, there are two elements of a risk analysis thatwill be briefly covered in the next two sections.Identifying the assetsIdentifying the threatsFor each asset, the basic goals of security are availability,confidentiality, and integrity. Each threat should be examined withan eye to how the threat could affect these areas.1.6.2 Identifying the AssetsOne step in a risk analysis is to identify all the things that needto be protected. Some things are obvious, like valuable proprietaryinformation, intellectual property, and all the various pieces ofhardware; but, some are overlooked, such as the people who actuallyuse the systems. The essential point is to list all things that couldbe affected by a security problem.One list of categories is suggested by Pfleeger [Pfleeger 1989]; thislist is adapted from that source: Hardware: CPUs, boards, keyboards,terminals, workstations, personal computers, printers, diskdrives, communication lines, terminal servers, routers. Software: sourceprograms, object programs, utilities, diagnostic programs, operatingsystems, communication programs. Data: during execution, stored on-line,archived off-line, backups, audit logs, databases, in transit overcommunication media. People: users, administrators, hardware maintainers.Documentation: on programs, hardware, systems, localadministrative procedures. Supplies: paper, forms, ribbons, magneticmedia.1.6.3 Identifying the ThreatsOnce the assets requiring protection are identified, it is necessaryto identify threats to those assets. The threats can then beexamined to determine what potential for loss exists. It helps toconsider from what threats you are trying to protect your assets.The following are classic threats that should be considered.Depending on your site, there will be more specific threats thatshould be identified and addressed.Unauthorized access to resources and/or informationUnintented and/or unauthorized Disclosure of informationDenial of service2.1.3 Who Should be Involved When Forming Policy?In order for a security policy to be appropriate and effective, itneeds to have the acceptance and support of all levels of employeeswithin the organization. It is especially important that corporatemanagement fully support the security policy process otherwise thereis little chance that they will have the intended impact. Thefollowing is a list of individuals who should be involved in thecreation and review of security policy documents.Site security administrator. Information technology technical staff(e.g., staff from computing center). Administrators of large user groupswithin the organization (e.g., business divisions, computer sciencedepartment within a university, etc.). Security incident response teamRepresentatives of the user groups affected by the securitypolicy. Responsible management. Legal counsel (if appropriate).The list above is representative of many organizations, but is notnecessarily comprehensive. The idea is to bring in representationfrom key stakeholders, management who have budget and policyauthority, technical staff who know what can and cannot be supported,and legal counsel who know the legal ramifications of various policychoices. In some organizations, it may be appropriate to include EDPaudit personnel. Involving this group is important if resultingpolicy statements are to reach the broadest possible acceptance. Itis also relevant to mention that the role of legal counsel will alsovary from country to country.... |
| Проект по созданию системы обеспечения информационной безопасности для организации состоит из ряда этапов. Фрагмент проекта представлен в таблице и содержит наименование этапов, продолжительность в рабочих часах при выполнении работы сотрудниками, календарные сроки и последовательность этапов.На выполнении каждого этапа задействованы сотрудники, фрагмент перечня которых с распределением по этапам представлен в таблице.Для выполнения работ привлечены 2 специалиста ИБ и 3 техника.Дата начала работ 01.04.2016 г.Распределить специалистов с учетом сроков проведения каждого этапа, выходных и предпраздничных дней.Продолжительность одного рабочего дня составляет 8 часов, каждый сотрудник занят полный рабочий день.Определить дату окончания работ.Дать ответ в следующей форме ДД.ММ.ГГГГ |
| Рассчитать горизонтальный угол обзора объектива видеокамеры.Ответ в градусах, округлить в меньшую сторону до целого, ввести только число. |
| Определить секретный ключ шифрования с применением алгоритма Диффи-Хелмана. Вводные данные У=7; Р=11; Х(Алисы)= 2; Х(Боба)=4.Ввод ответа в числовой форме |
| Расшифруйте сообщение "БКЮДЬОЯБ ДЕЩТА ПЯЛЗ ЪЕИЙ".Шифр Цезаря. Буква Ё не используется.Ответ дается заглавными буквами, с соблюдением пробелов. |
| Вычислить с применением алгоритма RSA для формирования пары открытого/закрытого ключей значения n, m, d.Алгоритм RSA, p = 5, q = 11, e =7Ввод ответов в числовой форме через пробел, например, при решении n=15, m=10, d=12, в ответ ввести: 15 10 12 |
| Определите количество возможных вариантов замены знаков в сообщении из символов равных ответу из Практической задачи 5. Алфавит сообщения английский, прописной, 26 символов, знаки и цифры не используются.Ввод ответа в числовой форме |
| Рассчитать допустимую длину линии питания системы видеонаблюдения в метрах.Ответ сократить в меньшую сторону до целого числа. |

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.

* 1. **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:

-

-

-

-

-

-

* 1. **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.

* 1. **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

* 1. **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.

* 1. **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.

* 1. **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.

Количество выполняемых пунктов задания 30.

Каждый выполненный пункт – 1 балл.

Максимальная оценка – 30 баллов.

Время выполнения задания 3 часа.

Выполнение пункта подтверждается созданием скриншота экрана – нажатием кнопки PrintScreen.

Вводные данные:

Конфигурация компьютера: Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz ОЗУ 2048 МБ HDD160 Гб NVIDIA GeForce 9600 GT (512 МБ)

ОС Windows 7 Professional SP1

Аппаратно-программный ключ Рутокен S 32К (PIN пользователя - 12345678, PIN администратора – 87654321, драйверы, утилиты, описание на USB носителе)

 Программа шифрования VeraCrypt v1.7 (программа, описание на USB носителе)

Программа восстановления и надежного удаления файлов Recuva(программа, описание на USB носителе)

Межсетевой экран D-Link DFL-260E, патч-корд, COM-кабель, (описание на USB носителе).

USB носитель 8Гб

**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 С:\\ 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 «Aдминистратора 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 «Aдминистратора 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 «Aдминистратора 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 ТОМ1 с применением алгоритма Twofish и алгоритма хеширования Whirlpool, сохранить его на USB-накопитель и организовать доступ ТОМ1 по ключевому файлу на Рутокене без пароля – 1 балл

 6.4 Создать скрытый зашифрованный контейнер ТОМ2, 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 ТОМ2 – 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 С:\\ «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 OC 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 c 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

Интернет-провайдер

LAN

WAN

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 OC 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