Практическая работа № 1

Тема: Описание собственной автоматизированной системы на примере действующей организации.

Цель: Сформировать полное описание АС для выполнения последующих работ по защите информации на выбранной АС.

Пояснения к работе:

В практической работе №1 необходимо придумать организацию, можно взять реальную организацию/компанию/предприятие , в которой используются автоматизированные системы.

Придумать 5 разных типов сотрудников, которые работают в этой организации с использованием автоматизированной системы. Эти сотрудники должны работать с разной информацией в автоматизированной системе.

Нужно описать организацию, ее специфику в нескольких предложениях.

Описать сотрудников и то с какой информацией они работают.

Описать какие происходят процессы в выбранной АС (ввод, обработка, вывод, обратная связь), каким образом это происходит , какие сотрудники в каком процессе задействованы.

Задание:

Отчет должен содержать:

1. Описание организации, ее специфика.
2. Описание перечня защищаемых информационных ресурсов АС;
3. Описание перечня лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
4. Описание процессов в АС.

Практическая работа № 2

Тема: Угрозы безопасности информации в автоматизированных системах.

Цель: Научиться проводить анализ угроз на автоматизированных рабочих местах с целью дальнейшего обеспечения безопасности от выявленных угроз.

Пояснения к работе:

Перечислить все информационные ресурсы обрабатываемые на выбранной в практической работе №1 АС. Определить категории информационных ресурсов (общедоступная, для служебного пользования , конфиденциальная , персональная).

Общедоступная (Public): Открытая информация, при работе с которой нет никаких ограничений.

Для служебного пользования (Restricted Access): Информация ограниченного доступа.

Конфиденциальная (Confidential): Конфиденциальная информация, при работе с которой вводятся строгие ограничения в зависимости от уровней допуска пользователя.

Персональная (Private): Персональная информация (зарплатная ведомость, адресные и паспортные данные сотрудников, медицинские карточки, ИНН, СПС и пр.).

Провести анализ угроз безопасности информации, согласно этапам анализа:

1 Этап. "Область применения процесса определения угроз безопасности информации" подразумевает принятие решения о необходимости защиты информации в ИС и разработку требований к защите. На данном этапе должны быть определены физические и логические границы информационной системы, в которых принимаются и контролируются меры защиты информации, за которые ответственен оператор, а также определены объекты защиты и сегменты информационной системы.

2 Этап. "Идентификация источников угроз и угроз безопасности информации" необходимо выделить источники угроз. Оценивать целесообразно только те угрозы, у которых есть источники и эти источники имеют возможности и условия для реализации угроз. Источники угроз могут быть:

- антропогенные источники - лица, которые могут преднамеренно или непреднамеренно нарушить конфиденциальность, целостность или доступность информации
- техногенные источники - отказы или сбои в работе технических и программных средств
- стихийные источники - пожары, землетрясения, наводнения и т.п.

3 Этап. Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба. В Модель угроз включаются только актуальные угрозы , то есть в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность (возможность) реализации рассматриваемой угрозы нарушителем

с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу):

Построение модели угроз

Модель угроз безопасности информации должна содержать следующие разделы:

1. Общие положения.

2. Описание информационной системы и особенностей ее функционирования.

2.1. Цель и задачи, решаемые информационной системой.

2.2. Описание структурно-функциональных характеристик информационной системы.

2.3. Описание технологии обработки информации.

3. Возможности нарушителей (модель нарушителя).

3.1. Типы и виды нарушителей.

3.2. Возможные цели и потенциал нарушителей.

3.3. Возможные способы реализации угроз безопасности информации.

4. Актуальные угрозы безопасности информации.

Раздел "Общие положения" содержит назначение и область действия документа, информацию о полное наименование ИС, информацию об использованных для разработки модели угроз нормативных и методических документах, национальных стандартах. В данный раздел также включается информация об используемых данных и источниках, на основе которых определяются угрозы безопасности информации.

Раздел "Описание информационной системы и особенностей ее функционирования" содержит общую характеристику ИС, описание структурно-функциональных характеристик, взаимосвязей между сегментами, описание взаимосвязей с другими ИС и информационно-телекоммуникационными сетями, описание технологии обработки информации.

Также в данном разделе приводятся предположения, касающиеся информационной системы и особенностей ее функционирования (в частности предположения об отсутствии неучтенных беспроводных каналов доступа или динамичность выделения адресов узлам информационной системы, иные предположения). В раздел включаются любые ограничения, касающиеся ИС и особенностей ее функционирования.

Раздел "Возможности нарушителей (модель нарушителя)" содержит описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в ИС, способов реализации угроз безопасности информации. В данный раздел также включаются предположения, касающиеся нарушителей (в частности предположение об отсутствии у нарушителя возможности доступа к оборудованию, сделанному на заказ и применяемому при реализации угрозы, предположение о наличии (отсутствии) сговора между внешними и внутренними нарушителями или иные предположения). В раздел включаются любые ограничения, касающиеся определения нарушителей (в частности исключение администраторов информационной системы или администраторов безопасности из числа потенциальных нарушителей или иные предположения).

Раздел "Актуальные угрозы безопасности информации" содержит описание актуальных угроз безопасности, включающее наименование угрозы безопасности информации, возможности нарушителя по реализации угрозы, используемые уязвимости информационной системы, описание способов реализации угрозы безопасности информации, объекты воздействия, возможные результат и последствия от реализации угрозы безопасности информации.

Задание:

Содержание отчета

1. Категорирование информационных ресурсов
2. Анализ угроз безопасности информации
3. Построение модели угроз

Практическая работа № 3

Тема: Особенности разработки информационных систем персональных данных

Цель: Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.

Пояснения к работе:

Необходимо описать выбранную организацию.

Перечислить какие персональные данные обрабатываются в организации.

Выбрать класс информационной системы.

Классификация ИС проводится на этапе ее создания или в ходе эксплуатации, но обязательно до построения средств защиты персональных данных. В общем случае все информационные системы, обрабатывающие персональные данные, подразделяются на 2 класса в зависимости от характеристик безопасности обрабатываемых данных:

Типовые информационные системы – системы, где требуется обеспечить только конфиденциальность обрабатываемых персональных данных.

Специальные информационные системы – системы, где требуется обеспечить хотя бы одну из характеристик безопасности, отличную от конфиденциальности (например, целостность или доступность). К специальным информационным системам должны быть отнесены:

1. ИС, связанные с обработкой ПД о состоянии здоровья субъектов ПД;
2. ИС, принимающие решения на основании исключительно автоматизированной обработки ПД. При этом принятые решения могут повлечь за собой юридические последствия для субъекта ПД или иным способом затронуть его законные права и интересы.

Согласно предлагаемой в Приказе методике ИС классифицируется в зависимости от количества субъектов, чьи данные обрабатываются, и типа обрабатываемых персональных данных.

В зависимости от объема обрабатываемых в ИСПД данных ХНПД выделяют следующие категории ИС:

1 категория – в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов ПД или персональные данные субъектов ПД в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 категория – в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов ПД или персональные данные субъектов ПД, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 категория – в информационной системе одновременно обрабатываются персональные данные менее чем 1000 субъектов ПД или персональные данные субъектов ПД в пределах конкретной организации.

Таким образом, данная категория ИС определяется на основании количества субъектов ПД, чьи данные обрабатываются в системе.

Определяются следующие категории обрабатываемых в информационной системе персональных данных :

категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных;
категория 4 – обезличенные и (или) общедоступные персональные данные.
По результатам анализа вышеперечисленных данных определяется класс ИС в соответствии с таблицей 1.
Таблица 1. Определение класса информационной системы

Таблица 1. Определение класса информационной системы			
ХНПД	**Категория 3**	**Категория 2**	**Категория 1**
ХПД			
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Рассмотрим, что значит каждый класс ИСПД в отдельности:
- класс 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПД;
- класс 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;
- класс 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПД;
- класс 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.

Задание:
Отчет должен содержать:
1. Описание организации
2. Перечень персональных данных
3. Выбор класса информационной системы
4. Обоснование выбора
5. Перечислить требования предъявляемые к выбранному классу персональных данных.

Список литературы:

Интернет ресурс: НОУ Интуит, https://intuit.ru/studies/courses/697/553/lecture/12450

Практическая работа № 4

Тема: Защита от несанкционированного доступа к информации.
Цель: Определения класса защищенности автоматизированной системы. Определение требований предъявляемых к защите АС, согласно выбранному классу. Описание реализации разграничения доступа в АС. Определение модели доступа для АС. Описание реализации выбранной модели доступа.

Пояснения к работе:

Составить необходимый перечень исходных данных для проведения классификации конкретной АС:
- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

Устанавливается девять классов защищенности АС от НСД к информации.
Каждый класс характеризуется определенной минимальной совокупностью требований по защите.
Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.
В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.
Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.
Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.
Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.
Требования предъявляемые к каждому из классов содержаться в руководящих документах ФСТЭК.

Модель управления доступом – это структура, которая определяет порядок доступа субъектов к объектам.
Существует три основных модели управления доступом:
- дискреционная (DAC – Discretionary Access Control),
- мандатная (MAC – Mandatory Access Control)
- ролевая (недискреционная) (RBAC – Role-based Access Control).

Каждая модель использует различные методы для управления доступом субъектов к объектам, и имеет свои преимущества и ограничения.
Выбор оптимальной модели управления доступом следует производить на основе целей бизнеса и целей безопасности компании, а также на основе ее культуры и стиля

управления бизнесом. Некоторые компании используют только одну модель, другие комбинируют их для получения необходимого уровня защиты.
Важно понимать основные характеристики трех моделей управления доступом:

DAC – владельцы данных решают, кто имеет доступ к ресурсам. Политика безопасности реализуется с помощью ACL.
MAC – политика безопасности реализуется операционной системой посредством меток безопасности.
RBAC – решения о предоставлении доступа принимаются системой на основании ролей и/или должностей субъектов.

Задание:
Отчет должен содержать:

1. Описание организации.
2. Выбор и обоснование класса АС (1А, 1Б ... и т.д.).
3. Перечислить требования предъявляемые к АС. Описать как выполняются или не выполняются перечисленные требования в организации.
4. Описать как реализовано разграничение доступа к ресурсам АС.
5. Выбрать модель доступа для АС и аргументировано обосновать, почему именно эта модель. Описать как реализована эта модель, с помощью каких средств, ресурсов.

Список литературы

Руководящий документ: Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

Практическая работа № 6

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание документации: "Описание технологического процесса обработки информации в АС".

Пояснения к работе:

В практической работе нужно создать «Описание технологического процесса обработки информации в АС"» для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №6.

Задание:
Отчет должен содержать : "Описание технологического процесса обработки информации в АС". для конкретной организации.

Список литературы

Интернет-ресурс: SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BE%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BE%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B8

Практическая работа № 7

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание документации: "Технический паспорт автоматизированной системы"

Пояснения к работе:

В практической работе нужно создать «Технический паспорт автоматизированной системы» для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №7.

Задание:
Отчет должен содержать: "Технический паспорт автоматизированной системы" для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BF%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82

Практическая работа № 8

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание организационно-распорядительной документации разрешительной системы доступа персонала к защищаемым ресурсам АС.

Пояснения к работе:

В практической работе нужно создать организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №8.

Задание:
Отчет должен содержать: организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BE%D1%80%D0%B4

Практическая работа № 9

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание инструкции администратору безопасности информации АС.

Пояснения к работе:

В практической работе нужно создать инструкцию администратору безопасности информации АС для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №9.

Задание:
Отчет должен содержать: инструкцию администратору безопасности информации АС для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F_%D0%B0%D0%B1

Практическая работа № 10

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание инструкции по проведению антивирусного контроля на АС.

Пояснения к работе:

В практической работе нужно создать инструкцию по проведению антивирусного контроля на АС для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №10.

Задание:
Отчет должен содержать: инструкцию по проведению антивирусного контроля на АС для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F_%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81

Практическая работа № 11

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание инструкции по работе пользователей на АС.

Пояснения к работе:

В практической работе нужно создать инструкцию по работе пользователей на АС для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №11.

Задание:
Отчет должен содержать: инструкцию по работе пользователей на АС для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F_%D0%BF%D0%BE_%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B5

Практическая работа № 12

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание предписания на эксплуатацию объекта вычислительной техники в целом с приложением протоколов защищенности технических средств.

Пояснения к работе:

В практической работе нужно создать предписание на эксплуатацию объекта вычислительной техники в целом с приложением протоколов защищенности технических средств для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №12.

Задание:
Отчет должен содержать: предписание на эксплуатацию объекта вычислительной техники в целом с приложением протоколов защищенности технических средств для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BE%D0%B2%D1%82

Практическая работа № 13

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание протокола оценки эффективности, установленных на объекте средств защиты информации.

Пояснения к работе:

В практической работе нужно создать протокола оценки эффективности, установленных на объекте средств защиты информации для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №13.

Задание:
Отчет должен содержать: протокол оценки эффективности, установленных на объекте средств защиты информации для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%8D%D1%84%D1%84%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D0%B8

Практическая работа № 14

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание инструкции по эксплуатации СЗИ.

Пояснения к работе:

В практической работе нужно создать инструкцию по эксплуатации СЗИ для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №14.

Задание:
Отчет должен содержать: инструкцию по эксплуатации СЗИ для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F_%D1%81%D0%B7%D0%B8

Практическая работа № 15

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание протокола испытаний на соответствие требованиям по защите информации от НСД.

Пояснения к работе:

В практической работе нужно создать протокол испытаний на соответствие требованиям по защите информации от НСД для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №15.

Задание:
Отчет должен содержать: протокол испытаний на соответствие требованиям по защите информации от НСД для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%B8%D1%81%D0%BF%D1%8B%D1%82%D0%B0%D0%BD%D0%B8%D0%B9

Практическая работа № 16

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание аттестата соответствия по требованиям безопасности информации

Пояснения к работе:

В практической работе нужно создать аттестат соответствия по требованиям безопасности информации для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №16.

Задание:
Отчет должен содержать: аттестат соответствия по требованиям безопасности информации для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%82

Практическая работа № 17

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание заключения по результатам аттестационных испытаний с приложением протоколов аттестационных испытаний

Пояснения к работе:

В практической работе нужно создать заключение по результатам аттестационных испытаний с приложением протоколов аттестационных испытаний для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №17.

Задание:
Отчет должен содержать: заключение по результатам аттестационных испытаний с приложением протоколов аттестационных испытаний для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B7%D0%B0%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%B8%D1%81%D0%BF%D1%8B%D1%82%D0%B0%D0%BD%D0%B8%D1%8F%D0%BC

Практическая работа № 18

Тема: Документация на защищаемую автоматизированную систему
Цель: Создание документации заключения по результатам контроля состояния и эффективности защиты информации на объекте

Пояснения к работе:

В практической работе нужно создать заключение по результатам контроля состояния и эффективности защиты информации на объекте для выбранной организации из практической работы №1 по шаблону из списка литературы практической работы №18.

Задание:
Отчет должен содержать: заключение по результатам контроля состояния и эффективности защиты информации на объекте для конкретной организации.

Список литературы

Интернет-ресурс:

SecurityPolicy.ru документация по информационной безопасности: http://securitypolicy.ru/%D0%B0%D1%82%D1%82%D0%B5%D1%81%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%B0%D1%81/%D0%B7%D0%B0%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E