Министерство образования и науки Пермского края
государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

для специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»
по МДК.01.04 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении»

2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
ПРАКТИЧЕСКИЕ РАБОТЫ 6
Практическая работа № 1 6
Практическая работа № 2 7
Практическая работа № 3 10
Практическая работа № 4 12
Практическая работа № 5 14
Практическая работа № 6 16
Практическая работа № 7 17
Практическая работа № 8 18
Практическая работа № 9 19
Практическая работа № 10 20
Практическая работа № 11 21
Практическая работа № 12 22
Практическая работа № 13 23
Практическая работа № 14 24
Практическая работа № 15 25
Практическая работа № 16 26
Практическая работа № 17 27
Практическая работа № 18 28
Практическая работа № 19 29
Практическая работа № 20 30
Практическая работа № 21 31
Практическая работа № 22 32
Практическая работа № 23 33
Практическая работа № 24 34
Практическая работа № 25 35
Практическая работа № 26 36
Практическая работа № 27 37
Практическая работа № 28 38
Практическая работа № 29 39
Практическая работа № 30 40

ВВЕДЕНИЕ

Место дисциплины в основной образовательной программе: МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» является обязательным разделом профессионального модуля ПМ.01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Формируемые МДК.01.04. «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» компетенции:

Код и наименование компетенции	Показатели освоения компетенции
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	***Умения:*** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем
	Знания: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	***Умения:*** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
	Знания: теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	***Умения:*** настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
	Знания: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях
ПК 1.4. Осуществлять проверку технического состояния,	***Умения:*** обеспечивать работоспособность, обнаруживать и устранять неисправности

техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	***Знания:*** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника). **Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	**Умения:** определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска **Знания** номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	**Умения**: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития **Знания**: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	**Умения**: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами **Знания**: психология коллектива; психология личности; основы проектной деятельности
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	**Умения:** излагать свои мысли на государственном языке; оформлять документы **Знания:** особенности социального и культурного контекста; правила оформления документов
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	**Умения:** описывать значимость своей профессии Презентовать структуру профессиональной деятельности по специальности **Знания:** сущность гражданско-патриотической позиции; Общечеловеческие ценности; Правила поведения в ходе выполнения профессиональной деятельности
ОК 07. Использовать информационные технологии в профессиональной деятельности.	**Умения: п**рименять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение **Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности

Методические указания предназначены для проведения практических занятий по МДК.01.04, закрепления теоретических знаний и получения навыков работы в области защиты информации.

Методические указания разработаны в соответствии с рабочей программой профессионального модуля ПМ.01. «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

По учебному плану, и в соответствии с рабочей программой профессионального модуля ПМ.01, на изучение МДК.01.04. обучающимися предусмотрено 250 часов, из них практических – 86.

Методические указания включают 30 практических работ. Каждая практическая работа содержит сведения о теме, цели ее проведения и формируемых компетенциях, включает пояснения к работе, содержание отчета, контрольные задания или вопросы, список литературы.

К выполнению практических работ обучаемые приступают после подробного изучения соответствующего теоретического материала и прохождения инструктажа по технике безопасности.

Характер практических работ репродуктивный и частично-репродуктивный.

ПРАКТИЧЕСКИЕ РАБОТЫ

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.

Формируемые компетенции: ПК 1.3, ОК 02, ОК 05

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.

Контрольные вопросы

1. Понятие автоматизированной системы.
2. Классификация автоматизированных систем.
3. Процессы в автоматизированных системах.

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.

Формируемые компетенции: ПК 1.3, ПК 1.4, ОК 01, ОК 02.

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

Контрольные вопросы

1. Перечислите категории информации и особенности каждого грифа.
2. Перечислите этапы анализа угроз и специфику каждого этапа.
3. Перечислите что входит в модель угроз и суть каждого раздела.

Практическая работа № 3

Тема: Особенности разработки информационных систем персональных данных

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

Формируемые компетенции: ПК 1.3, ОК 02, ОК 07.

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.

Контрольные вопросы
1. Понятие персональных данных.
2. Виды информационных систем обрабатывающих персональные данные.
3. Категории персональных данных и их специфика.
4. Классы ИС и их специфика.

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.

Формируемые компетенции: ПК 1.3, ОК 02, ОК 07

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.

Контрольные вопросы

1. Перечислите классы защищенности АС от НСД и их основные характеристики.
2. Перечислите особенности модели DAC.
3. Перечислите особенности модели MAC.
4. Перечислите особенности модели RBAC.

Список литературы

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

Практическая работа № 5

Тема: СЗИ от НСД.
Цель: Изучить возможности ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE) для защиты информации от НСД.

Формируемые компетенции: ПК 1.1, ПК 1.2, ОК 01,ОК 02, ОК 07.

Пояснения к работе:

Необходимо изучить документацию программно-аппаратного комплекса Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE) и подготовить отчет, в котором должны быть отражены основные действия по настройке комплекса на АС, а именно:

Программно-аппаратные комплексы средств защиты информации (ПАК СЗИ) Аккорд-Win32 и Аккорд-Win64 предназначены для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам под управлением ОС семейства Windows – 32-х и 64-х разрядных соответственно.

Возможности:

- Защита от несанкционированного доступа к ПЭВМ;
- Идентификация/ аутентификация пользователей до загрузки операционной системы с последующей передачей результатов успешной идентификации/аутентификации в операционную систему;
- Аппаратный контроль целостности системных файлов и критичных разделов реестра;
- Доверенная загрузка ОС;
- Контроль целостности программ и данных, их защита от несанкционированных модификаций;
- Создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
- Запрет запуска неразрешенных программ;
- Разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
- Разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
- Автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса;
- Усиленная аутентификация терминальных станций с помощью контроллера Аккорд или ПСКЗИ ШИПКА;
- Идентификация/аутентификация пользователей, подключающихся к терминальному серверу (с использованием ТМ-идентификатора или ПСКЗИ ШИПКА);
- Опциональная автоматическая идентификация в системе Windows NT+ и на терминальном сервере пользователей, аутентифицированных защитными механизмами контроллера АМДЗ (при таком подходе, избегая повторной идентификации пользователей, можно гарантировать, что ОС будет загружена под именем того же пользователя, который был аутентифицирован в контроллере АМДЗ, и к терминальному серверу подключится тот же самый пользователь);
- Управление терминальными сессиями;
- Контроль печати на принтерах, подключенных как к терминальным серверам, так и к пользовательским терминалам, который позволяет протоколировать вывод документов на печать и маркировать эти документы (в качестве маркера может

выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

- Контроль доступа к USB устройствам

Задание:

Отчет должен содержать:

1. Описание установку и настройку СЗИ от НСД
2. Описание реализации защиты входа в систему (идентификация и аутентификация пользователей).
3. Описание реализации разграничение доступа к устройствам.
4. Описание реализации управлением доступа.
5. Описание реализации использования принтеров для печати конфиденциальных документов. Описание реализации контроля печати.
6. Описание реализации настройки системы для задач аудита.
7. Описание реализации настройки контроля целостности и замкнутой программной среды.
8. Описание реализации централизованного управления системой защиты, оперативного мониторинга и аудита безопасности.

Контрольные вопросы

1. Перечислите основные особенности и функции ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE)

Список литературы

Интернет-ресурс: Сайт ОКБ САПР — компания разработчик программно-аппаратных средств защиты информации (СЗИ) от несанкционированного доступа (НСД) https://www.okbsapr.ru/products/accord/pak-accord-win32-64-tse/

Практическая работа № 6

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

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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"

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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.
Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.2, ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.2, ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.2, ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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.

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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
Формируемые компетенции: ПК 1.2, ПК 1.3, ОК 02, ОК 03, ОК 05.

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

Формируемые компетенции: ПК 1.1, ПК 1.3, ОК 02, ОК 03, ОК 05.

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

Формируемые компетенции: ПК 1.3, ОК 02, ОК 03, ОК 05.

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

Практическая работа № 19

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программно-аппаратного средства «Security Studio» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Security Studio» . Вычленить основные функции и назначение «Security Studio».Определить какие функции «Security Studio» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Security Studio»
3. Перечень функции «Security Studio» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 20

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программно-аппаратного средства «SecretNet» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «SecretNet» . Вычленить основные функции и назначение «SecretNet».Определить какие функции «SecretNet» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «SecretNet»
3. Перечень функции «SecretNet» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 21

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программно-аппаратного средства «ПАК Соболь» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «ПАК Соболь». Вычленить основные функции и назначение «ПАК Соболь». Определить какие функции «ПАК Соболь» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «ПАК Соболь»
3. Перечень функции «ПАК Соболь» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 22

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программного средства «Ревизор 1 и Ревизор 2» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Ревизор 1 и Ревизор 2» . Вычленить основные функции и назначение «Ревизор 1 и Ревизор 2».Определить какие функции «Ревизор 1 и Ревизор 2» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Ревизор 1 и Ревизор 2»
3. Перечень функции «Ревизор 1 и Ревизор 2» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 23

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программно-аппаратного средства «АКПШ Континент» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «АКПШ Континент» . Вычленить основные функции и назначение «АКПШ Континент». Определить какие функции «АКПШ Континент» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «АКПШ Континент»
3. Перечень функции «АКПШ Континент» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 24

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программного средства «TrustAccess» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «TrustAccess» . Вычленить основные функции и назначение «TrustAccess». Определить какие функции «TrustAccess» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «TrustAccess»
3. Перечень функции «TrustAccess» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 25

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программного средства «Dallas Lock» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Dallas Lock» . Вычленить основные функции и назначение «Dallas Lock».Определить какие функции «Dallas Lock» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Dallas Lock»
3. Перечень функции «Dallas Lock» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 26

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программного средства «Агент инвентаризации» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Агенту инвентаризации» . Вычленить основные функции и назначение «Агента инвентаризации». Определить какие функции «Агента инвентаризации» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Агента инвентаризации»
3. Перечень функции «Агента инвентаризации» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 27

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программного средства «Фикс» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Фиксу» . Вычленить основные функции и назначение «Фикс». Определить какие функции «Фикса» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Фикса»
3. Перечень функции «Фикса» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 28

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программного средства «Terrier» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Terrier» . Вычленить основные функции и назначение «Terrier».Определить какие функции «Terrier» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Terrier»
3. Перечень функции «Terrier» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 29

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программно-аппаратного средства «Аккорд-АМДЗ» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Аккорд-АМДЗ». Вычленить основные функции и назначение «Аккорд-АМДЗ». Определить какие функции «Аккорд-АМДЗ» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Аккорд-АМДЗ»
3. Перечень функции «Аккорд-АМДЗ» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций

Практическая работа № 30

Тема: Программно-аппаратные средства обеспечения информационной безопасности
Цель: Изучение программно-аппаратного средства «Страж NT» для обеспечения информационной безопасности.

Формируемые компетенции: ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК 01, ОК 02, ОК 03, ОК 06, ОК 07.

Пояснения к работе:

Самостоятельно найти и изучить официальную документацию к «Страж NT» . Вычленить основные функции и назначение «Страж NT». Определить какие функции «Страж NT» можно применить в своей организации (из практической работы №1) и для чего именно нужны эти функции в вашей организации. Описать краткие шаги по настройке и реализации выбранных функции.

Задание:

Отчет должен содержать:

1. Описание организации
2. Описание «Страж NT»
3. Перечень функции «Страж NT» применимый в организации
4. Описание назначения выбранных функций
5. Описание настройки выбранных функций