Частное профессиональное образовательное учреждение
Пермского краевого союза потребительских обществ
«Пермский кооперативный техникум»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность и управление доступом
в информационных системах

для специальности 09.02.04 Информационные системы (по отраслям)

Верещагино, 2018

ОДОБРЕНО:
Председатель цикловой комиссии
_____ Н.Н. Петрова
Протокол № 2
«07» сентября 2018г.

УТВЕРЖДАЮ:
заместитель по УВР
_____Н.Ю. Плешивых
«7» сентября 2018г

Составитель : Самгин В.Н. , преподаватель техникума

Программа предназначена для профессиональных образовательных организаций, реализующих основную профессиональную образовательную программу СПО по специальности 09.02.04 Информационные системы по (отраслям). Программа разработана в соответствии с требованиями ФГОС СПО по специальности.

СОДЕРЖАНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебно-методический комплекс учебной дисциплины «Безопасность и управление доступом в информационных системах» предназначена для реализации государственных требований к минимуму содержания и уровню подготовки студентов специальности 09.02.04 «Информационные системы (по отраслям)».

Учебная дисциплина «Безопасность и управление доступом в информационных системах» устанавливает базовые знания для освоения специальных дисциплин.

Базовый курс основан на знаниях и навыках, полученных студентами в процессе изучения таких дисциплин, как «Информатика», «Архитектура ЭВМ, систем и сетей», «Информационные системы», «Компьютерные сети», «Администрирование сетей».

Программа рассчитана на 120 часов (из них: 80 часов — аудиторные занятия; 40 часов — самостоятельные занятия).

При реализации учебно-методического комплекса учебной дисциплины преподаватель (в зависимости от специфики подготовки студентов) может вносить дополнения и изменения в содержание, последовательность изучения учебного материала и распределение учебных часов по темам, а также практических занятий при условии выполнения требований к уровню подготовки.

Учебно-методический комплекс рассмотрен предметной комиссией и утвержден заместителем директора по учебной работе.

При освоении дисциплины обращается внимание студентов на прикладной характер, на то, где и когда изучаемые теоретические положения и практические навыки могут быть использованы в будущей практической деятельности.

Программа дисциплины предполагает практическое осмысление ее модулей, разделов, тем на лабораторно-практических занятиях и в процессе самостоятельной работы.

Изучение материала ведется в форме, доступной пониманию студентов. В процессе обучения используются лекционные, лабораторно-практические занятия, ведется разбор реальных производственных ситуаций, проводятся дискуссии по актуальным проблемам информационной безопасности и системам защиты информации; осуществляется работа с методическими и справочными материалами; используются программно-технические средства обучения (вычислительная техника, мультимедийное и проекционное оборудование).

При изложении материала по соответствующим разделам и темам используются законодательные и нормативные акты РФ, а также инструктивные и руководящие материалы отраслевых министерств и ведомств.

В процессе изучения дисциплины проводятся тематические контрольные работы, а также индивидуальный итоговый экзамен по всему курсу дисциплины.

Цель:

Заложить методически правильные основы знаний об эффективных способах защиты, сохранности и безопасности информации, будущим специалистам в области информационных технологий. Обучить методам комплексного подхода обеспечения информационной безопасности (ИБ) предприятия на всех этапах технологического цикла обработки информации.

Задачи:

- усвоение базисных положений информационной безопасности как отдельной области информационных технологий (ИТ);
- изучение основных концептуальных положений систем защиты информации;
- изучение основных направлений обеспечения информационной безопасности предприятия;
- формирования представления о способах защиты информации; мерах противодействия несанкционированному доступу к источникам конфиденциальной информации; использовании средств аудита и анализа защищенности ИС предприятия.

Обязательный минимум:

- роль безопасности информации, средств управления доступом, систем защиты информации в информационной среде современного общества; защита субъектов и объектов информационных отношений в информационных системах.
- использование административного, законодательного, процедурного уровней безопасности информации, их применение в системах защиты информации;
- организация сервисов безопасности; внедрение и сопровождение основных программно-технических мер обеспечения информационной безопасности.

2.СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Вид учебной нагрузки	Объем часов
Максимальная учебная нагрузка (всего)	120
Обязательная аудиторная нагрузка (всего)	80
в том числе:	
лекции	60
практические работы	20
Самостоятельная работа	40
Итоговая аттестация в форме экзамена	

2.2 Примерный тематический план и содержание учебной дисциплины «Основы проектирования баз данных»

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа	Объем часов		
		Теоретическое обучение	практические	Самостоятельная нагрузка
1	2	3	4	5
Раздел 1. Основные понятия и определения информационной безопасности и систем защиты информации.				
Введение.	Учебная дисциплина «Безопасность и управление доступом в информационных системах», ее основные задачи и связи с другими дисциплинами. Роль и место знаний по дисциплине в сфере профессиональной деятельности.	2		
Тема 1.1 Понятия информационной безопасности и систем защиты информации. Основные составляющие и терминология ИБ.	Понятие информации, формы представления информации, ее свойства. Качество информации с точки зрения потребителя и обладателя. Понятие информационной безопасности и системы защиты информации. Цели и задачи СЗИ. Основные компоненты систем защиты информации. Требования к СЗИ. Условия существования СЗИ. Виды собственного обеспечения СЗИ.	2		
Тема 1.2. Эволюция подходов к обеспечению информационной безопасности.	Информация как важнейший ресурс современного общества Информационные ресурсы, их классификация. Ценность и качество информационных ресурсов. Информация в условиях рыночной экономики и конкурентной борьбе. Цели защиты информации. Многогранность проблемы защиты информации	2		
Самостоятельная работа	Подготовка презентаций на тему «Государственное и отраслевое использование информационных ресурсов».			2

Практическая работа	Изучение формирования учетной политики, прав и полномочий доступа в компьютерной сети ЧПОУ ПКТ.		2	
Практическая работа	Управление ресурсами общего доступа ЧПОУ ПКТ.		2	
Раздел 2. Информационные, программно - математические, физические и организационные угрозы				
Тема 2.1. Концепция и структура защиты информации	Определение угроз безопасности информации. Определение источников угроз. Способы реализации угроз. Цели угроз. Меры защиты. Методы моделирования безопасности информации.	2		
Самостоятельная работа	Анализ и моделирование компонентов информационной системы. Объектно-ориентированные подходы к рассмотрению защищаемых систем			2
Тема 2.2. Тенденции и направления развития ИБ	Инфраструктура современных ИТ. Основные составляющие ИБ. Мероприятия, направленные на обеспечение ИБ. Важность и сложность проблемы ИБ.	2		
Самостоятельная работа	Доктрина информационной безопасности России на основе ФЗ РФ « Об информации, информатизации…»			2
Тема 2.3. Требования и условия обеспечения защиты информации	Зарубежный и отечественный опыт использования СЗИ. Требования к системе безопасности в ИТ. Характеристики обеспечения СЗИ. Взаимодействие субъектов и объектов в СЗИ.	2		
Тема 2.4. Концептуальные модели ИБ	Анализ и характеристика компонентов модели. Уровни декомпозиции создаваемой модели. Объекты угроз. Источники угроз. Цели угроз. Источники информации. Способы овладения информацией. Направления защиты. Способы и средства защиты	2		
Самостоятельная работа	Обеспечение конфиденциальности, целостности и доступности информации в ИС. Разновидности противоправных действий по отношению к информационным ресурсам**.**			2
Практическая работа	Реализация на программном уровне сервисов управления доступом в ГВС.		2	

Тема 2.5. Методы моделирования и анализа компонентов модели	Способы моделирования. Основные компоненты модели. Анализ элементов концептуальной модели. Направления применения.	2		
Самостоятельная работа	Уровни декомпозиции разрабатываемой модели. Возможности практического применения концептуальной модели в реальных системах.			2
Тема 2.6. Угрозы конфиденциальной информации и действия, приводящие к их неправомерному овладению	Понятие угрозы конфиденциальной информации. Противоправные действия с конфиденциальной информацией. Способы овладения конфиденциальной информации. Классификация угроз. Внешние и внутренние угрозы. Источники угроз. Разглашение, утечка и несанкционированный доступ. Наиболее распространенные формы и методы получения охраняемых сведений.	2		
Самостоятельная работа	Условия, способствующие неправомерному овладению информацией. Характерные для РФ разновидности угроз конфиденциальной информации.			2
Практическая работа	Кэширующие (proxy) сервера доступа на основе ПО «UserGate». Изучение функциональности, настройка, сопровождение.		2	
Раздел 3. Организационно-правовое обеспечение информационной безопасности. Нормативно-правовые категории обеспечения ИБ.				
Тема 3.1. Нормативно-правовые категории обеспечения ИБ. Законодательный уровень защиты информации	Назначение нормативно-правовых категорий. Определение правовой защиты информации. Классификация блоков правовой защиты. Федеральные законы об информации и ее защите. Государственная и коммерческая тайны. Страхование - как форма правовой защиты. Патентование. Авторское право. Анализ действующего законодательства РФ в области защиты информации.	2		
Самостоятельная работа	Дополнительные формы правовой защиты: обязательства сторон, лицензии и сертификаты. Отраслевые и ведомственные нормативно-правовые документы: уставы, правила, ин-			2

	струкции, положения и т.д.			
Тема 3.2. Административный уровень защиты информации - организационная защита	Определение организационной защиты. Функции организационной защиты. Основные организационные мероприятия. Организационные средства защиты ПЭВМ и сетей. Назначение службы безопасности предприятия. Структура и задачи службы безопасности.	2		
Самостоятельная работа	Функции службы безопасности на крупных, средних и мелких предприятиях и в организациях. Регламентация деятельности сотрудников средствами организационной защиты.			2
Практическая работа	Реализация на программном уровне сервисов защиты компьютерных сетей.		2	
Тема 3.3. Виды регламентации производственной деятельности, взаимоотношений исполнителей и мероприятии.	Политика безопасности. Программа безопасности. Жизненный цикл информационных систем. Области применения. Этапы реализации политики безопасности	2		
Тема 3.4. Процедурный уровень защиты информации – инженерно-техническая защита	Классы мер процедурного уровня. Определение инженерно-технической защиты. Классификация средств инженерно-технической защиты. Физическая защита. Аппаратная защита. Программная защита. Криптографические средства.	2		
Тема 3.5. Защита от несанкционированного доступа, модели и основные принципы защиты информации Классификация и назначение средств защиты, основные характеристики средств и оборудования, способы и	Определение физических средств защиты. Классификация физических средств. Системы контроля доступа. Охранные системы. Определение аппаратных средств защиты. Классификация аппаратных средств. Комплексы обнаружения и измерения. Определение программных средств защиты. Классификация программных средств. Направления использования программной защиты. Защита от НСД программными средствами. Защита от копирования. Защита информации от разрушения. Определение криптографических средств защиты. Классификация криптографических средств. Техно-	2		

методы противодействия.	логии шифрования.			
Самостоятельная работа	Характеристика защиты информации на уровне системного, прикладного и специального программного обеспечения. Средства защиты данных и информации.			2
Практическая работа	Межсетевые экраны firewalls на основе ПО «Outpost», «Zonealarm». Изучение функциональности, настройка, сопровождение.		2	
Раздел 4. Основные направления обеспечения ИБ.				
Тема 4.1. Основные направления обеспечения ИБ. Характеристики мероприятий и защитных действий.	Способы защиты информации. Меры предупреждения угроз. Меры обнаружения угроз. Меры выявления угроз. Меры локализации и ликвидации угроз. Характеристика защитных действий. Организационно-технические мероприятия по защите информации: пространственные, режимные, энергетические, технические.	2		
Самостоятельная работа	Ограничительные меры организационно-технических мероприятий. Практические способы защиты от разглашения, утечки, несанкционированного доступа.			2
Тема 4.2. Организационно-технические меры обеспечения защиты информации от разглашения, утечки, несанкционированного доступа. проблема вирусного заражения программ, структура современных вирусных программ, основные классы антивирусных программ, перспективные методы антивирусной защиты.	Классификация организационно-технических мероприятий по защите информации. Пространственные способы защиты. Режимные способы защиты. Энергетические способы защиты. Направления защитных мер от разглашения, утечки, несанкционированного доступа	2		

Самостоятельная работа	Практическое применение защитных действий направленных на персонал, финансовые, материальные и информационные ресурсы.			2
Практическая работа	Реализация на программном уровне сервисов защиты от нежелательного трафика данных.		2	
Тема 4.3. Противодействие к источникам конфиденциальной информации	Общие положения. Классификация мероприятий, направленных на пресечение разглашения информации. Способы пресечения разглашения информации. Воспитательно-профилактическая деятельность на предприятии. Характеристика сред передачи информации. Структура канала утечки информации. Классификация потенциальных каналов утечки информации. Защита информации от утечки по техническим каналам. Средства и способы защиты. Оценка опасности реальных каналов передачи данных. Средства контроля за качеством защиты каналов передачи. Способы несанкционированного доступа. Защита от наблюдения и съемки. Защита от просушивания. Защита от перехвата.	2		
Самостоятельная работа	Формальные и неформальные каналы распространения информации. Причины, факторы и обстоятельства, приводящие к разглашению информации. Виды применяемого оборудования для диагностики и локализации потенциальных каналов утечки информации и несанкционированного доступа.			2
Тема 4.4. Направления взаимоотношений с партнерами и конкурентами.	Характеристика научно-технического сотрудничества. Соглашения о совместном сотрудничестве. Защита интеллектуальной собственности. Технологический обмен и его регулирование. Условия разглашения сведений коммерческой тайны. Экспертиза ценности передаваемой информации. Организация деловых встреч и переговоров.	2		
Самостоятельная работа	Порядок защиты информации с партнерами и конкурентами.			2
Тема 4.5. Средства аудита	Определение аудита состояния защиты. Направления дея-	2		

состояния защиты информации	тельности в области аудита безопасности информации. Задачи и функции аудита безопасности информации. Средства активного аудита.			
Практическая работа	Антиспамерские наборы ПО. Интеграция в существующие системы, настройка, сопровождение, анализ функциональности.		2	
Раздел 5. Принципы организации разноуровневого доступа в автоматизированных информационных системах (АИС); Основные понятия и особенности современных информационных систем				
Тема 5.1. Основные понятия и особенности современных информационных систем	Основные аспекты современных информационных технологий. Характеристики информационных систем. Конфигурация информационных сервисов. Активные агенты информационных систем. Анализ защищенности информационных сервисов.	2		
Самостоятельная работа	Структурные элементы информационных сервисов. Важнейшие показатели функционирования ИС. Задачи сотрудников по обеспечению качества функционирования информационного пространства организации.			2
Тема 5.2. Архитектурная безопасность, классификация сервисов безопасности	Понятие архитектурной безопасности. Классификация сервисов безопасности. Основные принципы архитектурной безопасности. Безопасное состояние информационного сервиса. Разделение обязанностей и мининимизация привилегий. Эшелонированность обороны информационных сервисов. Обеспечение высокой доступности сервиса. Объемы защитных средств клиентских и серверных систем	2		
Самостоятельная работа	Аппаратная реализация защиты и безопасности обработки информации в вычислительных системах, реализованная производителями оборудования.			2
Тема 5.3. Понятия клиента, прав доступа, объекта доступа, групп, ролей, политики	Идентификация и аутентификация. Основные понятия. Парольная аутентификация. Стандартные средства иде- аутентификации ИС. Сервер аутентификации Kerberos. Иде- ау-	4		

безопасности в современных АИС Идентификация и аутентификация, управление доступом	тентификация биометрических данных. Управление доступом. Основные понятия. Логическое и физическое управление доступом. Разновидности управления доступом пользователей. Контроль прав доступа. Возможные подходы к управлению доступом			
Самостоятельная работа	Особенности использования в современных компьютерных сетях и вычислительных системах.			2
Тема 5.4. Протоколирование и анализ защищенности информации	Основные понятия. Задачи и способы протоколирования и анализа защищенности. События информационной системы, подлежащие фиксированию. Классификация журналов событий ИС. Состав средств анализа защищенности информационного сервиса. Разновидности контроля систем анализа защищенности. Применение экспертных систем анализа.	4		
Самостоятельная работа	Практическая реализация систем протоколирования и анализа защищенности в современных программно-аппаратных средствах.			2
Практическая работа	Реализация на программном уровне сервисов шифрования и кодирования данных. Обзор и изучение программных криптографических систем.		2	
Тема 5.5. Криптографические средства и методы защиты информации	Определение понятий криптографии и шифрования информации. Связь криптографии и сервисов безопасности. Методы шифрования. Использование симметричных и асимметричных методов шифрования. Назначения открытого и секретного ключа. Контроль целостности информации криптографическими методами. Электронно-цифровая подпись. Цифровые сертификаты. Функции удостоверяющих центров сертификации.	4		
Самостоятельная работа	Классификация встроенных криптографических средств в современных информационных системах. Возможности за-			2

	щиты и контроля целости. Разновидности алгоритмов шифрования данных.			
Тема 5.6. Меры обеспечения контроля целостности, доступности, отказоустойчивости информационной системы	Основные понятия. Показатель «эффективность услуг». Показатель «время недоступности». Обеспечение мер высокой доступности, отказоустойчивости информационного сервиса. Отказоустойчивость и зона риска. Обеспечение обслуживаемости ИС.	4		
Самостоятельная работа	Расчет характеристик доступности, отказоустойчивости, обслуживаемости. Меры, направленные на обеспечение качества этих показателей.			2
Практическая работа	Оценка функциональности, настройка, принципы работы и управления.		2	
Тема 5.7. Проектирование и внедрение систем защиты информации предприятия	Процесс разработки систем защиты. Этапы создания СЗИ предприятия. Предпроектные работы. Проектирование СЗИ. Ввод в опытную и промышленную эксплуатацию.	2		
Самостоятельная работа	Нормативно-правовое обеспечение разрабатываемой системы защиты информации предприятия. Функции сторонних организации при создании системы.			2
	ИТОГО	**60**	**20**	**40**

МАТЕРИАЛЫ К ИТОГОВОМУ КОНТРОЛЮ

Вопросы к экзамену:

1. Понятия «информационная безопасность» и «защита информации».
2. Основные положения системы защиты информации.
3. Условия удовлетворяющие СЗИ.
4. Основные требования систем защиты информации
5. Концептуальная модель информационной безопасности.
6. Угрозы конфиденциальной информации.
7. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
8. Направления обеспечения информационной безопасности (правовая защита).
9. Страховая и лицензионная защита информации.
10. Направления обеспечения информационной безопасности (организационная защита).
11. Направления обеспечения информационной безопасности (инженерно-техническая защита).
12. Физические средства защиты информации.
13. Защита информации от утечки по техническим каналам.
14. Аппаратные средства защиты информации.
15. Архитектурная безопасность СВТ.
16. Технические средства несанкционированного доступа.
17. Программные средства защиты информации.
18. Основные направления использования программной защиты информации.
19. Защита информации от несанкционированного доступа.
20. Защита информации от копирования.
21. Защита информации от изменения и разрушения.
22. Криптографические средства защиты. Технологии шифрования.
23. Способы защиты информации.
24. Общая характеристика защитных действий.
25. Пресечение разглашения конфиденциальной информации.
26. Противодействие несанкционированному доступу к источникам конфиденциальной информации.
27. Способы несанкционированного доступа.
28. Возможности типичных систем управления безопасностью.
29. Нормативно-законодательная база в области информационной безопасности.
30. Стандарты в области информационной безопасности.

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

5.1 Самостоятельная работа студента

Основная работа по курсу выполняется студентами самостоятельно. Лекции и лабораторный практикум способны лишь более конкретно ориентировать студента, показать ключевые направления дисциплины, обеспечивать ознакомление с ключевыми понятиями, и магистральные пути развития знаний в области операционных систем.

Для закрепления теоретических знаний, ознакомления с литературой и приобретения навыков самостоятельного мышления в рамках самостоятельной работы предусматривается выполнение следующих видов заданий:

— Составление обзора публикаций по теме из предложенного преподавателем списка литературных источников.
— Подготовка каждым студентом устного сообщения или реферативного доклада на лабораторном занятии.

5.2 Оценочные средства для контроля успеваемости и результатов освоения учебной дисциплины

Итоговая оценка за дисциплину выставляется по результатам работы студента в течении семестра и результата сдачи экзамена. Допуск к экзамену осуществляется только после защиты отчетов по лабораторным работам. В экзаменационный билет входит два вопроса. При неполных ответах будут задаваться дополнительные вопросы.

Для получения отметки по экзамену необходимо полностью и без ошибок ответить на поставленные вопросы, уметь хорошо ориентироваться в предметной области, знать материал из основной и дополнительной литературы.

Экзамен ставится, если студент не полно отвечает на два вопроса, либо допускает небольшие неточности в ответе, однако хорошо ориентируется в материале.

Во всех остальных случаях «Не зачтено».

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Пермский кооперативный техникум (ПКТ) располагает материально-технической базой, соответствующей санитарно-техническим нормам и обеспечивающей проведение всех видов лабораторной, практической подготовки студентов, предусмотренных ГОС.

Аудиторный фонд техникума, оснащенный СВТ, включает 3 компьютерных классов ПК используются в режиме свободного доступа студентов. Все компьютеры объединены в единую локальную вычислительную сеть и имеют доступ в Интернет.

Лекционные занятия по дисциплине проводятся в аудиториях, оснащенных мультимедийным проекторами.

Лабораторные работы выполняются в стационарных классах.

В учебном процессе используется лицензионное программное обеспечение. На различных ПК установлено системное программное обеспечение Windows 7 Enterprise Service Pack 1, Windows 7 Professional Service Pack 1.

Для оформления отчетов по лабораторным работам, подготовки докладов и презентаций используется лицензионный пакет прикладных программ: Microsoft PowerPoint 2007, Microsoft PowerPoint 2007, Microsoft Word 2007, Microsoft Word 2007. Специализированное ПО представлено свободно распространяемыми и условно бесплатными (с ограниченным временем использования) продуктами. Также для самостоятельной работы студенты могут по своему усмотрению использовать дополнительно demo-версии. Для его хранения и инсталяции на каждом ПК есть доступ к специальному разделу 1 на файл-сервере с необходимыми правами доступа.

7. СПИСОК ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, ДРУГИЕ ИНФОРМАЦИОННЫЕ ИСТОЧНИКИ

Основная литература

1. Анин, Б.Ю. Защита компьютерной информации: учебник./ Б.Ю. Анин.-СПб: БХВ-Петербург, 2018 -384с.

2. Галатенко, В.А. Информационная безопасность: практический подход.: учебное пособие / В.А. Галатенко.- М.: Наука, 2017 – 358с..

3. Галатенко, В.А. Основы информационной безопасности: учебное пособие / В.А.Галатенко. – М.: Интернет-Университет информационных технологий, 2018 - 280с.

4. Галатенко, В.А. Стандарты информационной безопасности : учебное пособие / В.А. Галатенко. - М.: Интернет-Университет Информационных Технологий, 2018 - 264с.

5. Мельников, В.В. Защита информации в компьютерных системах / В.В. Мельников. - М.: Финансы и статистика, 2017 - 368с.

6. Мельников, В.П. Информационная безопасность и защита информации / В.П. Мельников, А.М. Петраков, С.А. Клейменов. - М.: ACADEMA, 2017 - 336с.

7. Мельников, Д.А. Информационные процессы в компьютерных сетях : Протоколы, стандарты, интерфейсы, модели / Д.А. Мельников. - М.: Кудиц-Образ, 2017 - 256с.

8. Трубачев, А.П. Оценка безопасности информационных технологий.: учебник /А.П.Трубачев; под общ. ред. В.А.Галатенко . - М.: СИП РИА, 2017 – 580с.

9. Ярочкин, В.И. Информационная безопасность: учебное пособие / В.И.Ярочкин. – М.: ООО «Академический проект», 2017 – 638с.

Дополнительная литература

1. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. – М., 2010.
2. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к ин формации. Показатели защищенности от НСД к информации. - М., 2010.
3. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. - М., 2010.
4. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. - М., 2010.
5. Гостехкомиссия России. Руководящий документ. Защита от несанк¬ционированного доступа к информации. Термины и определения. - М., 2012.
6. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.12.2020) "Об информации, информационных технологиях и о защите информации"

Базы данных, Интернет-ресурсы, информационно-справочные и поисковые системы

1. Барсуков, В.В., Защита компьютерных систем от силовых деструктивных воздействий [Электронный ресурс] / В.В.Барсуков. – М., 2000. – Режим доступа: http://www.jetinfo.ra/2000/2/2/article2.2.2000.html
2. Бабернов, В.В, Системы резервного копирования [Электронный ресурс] / В.В.Бабернов. – М., 2000. – Режим доступа: http://ww.jetinfo.ra/2000/12/l/articlel.l2.2000.html
3. Браунли, Н.П. Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21) [Электронный ресурс] / Н.П Браунли, Э.В.Гатмэн. – М., 2000. – Режим доступа: http://www.jetinfo.rU/2000/5/l/articlel.5.2000.html
4. Семенов, Г.Н. Не только шифрование, или Обзор криптотехнологий [Электронный ресурс] / Г.Н.Семенов. – М.,2000. – Режим доступа: http://www.jetinfo.ra/200 l/3/2/article2.3.2001 .html
5. Web-сервер Совета безопасности РФ [Электронный ресурс]. – Режим доступа: http://www.scrf.gov.ru/
6. Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.fagci.ru/
7. Порталы по информационной безопасности [Электронный ресурс]. – Режим доступа: http://infosecurity.report.ru/, http://www.void.ru/.
8. Российский криптографический портал [Электронный ресурс]. – Режим доступа: http://www.cryptography.ru/
9. Jet Info [Электронный ресурс]: информационный бюллетень с тематическим разделом по информационной безопасности. – Режим доступа: http://www.jetinfo.ru/

10. Открытые системы [Электронный ресурс]: журнал, регулярно публикующий статьи по информационной безопасности. – Режим доступа: http://www.osp.ra/os/
11. Сервер с информацией об аутентификации по биометрическим характеристикам (прежде всего - по отпечаткам пальцев) [Электронный ресурс]. – Режим доступа: http://biometrics.ra/
12. Сервер с новостной информацией по ИБ [Электронный ресурс]. – Режим доступа: http://www.infosecnews.com/
13. Сервер с реферативной информацией по ИБ [Электронный ресурс]. – Режим доступа: http://www.isr.net/
14. Информационная безопасность [Электронный ресурс]: журнал. – Режим доступа: http://www.securitymagazine.com/
15. Единое окно доступа к образовательным ресурсам. Электронная библиотека [Электронный ресурс]: инф. система. – М.: ФГАУ ГНИИ ИТТ "Информика", 2005-2012.- Режим доступа: http://window.edu.ru/