МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»
Колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	***10.02.05 Обеспечение информационной безопасности автоматизированных систем***
Обучение:	по программе базовой подготовке
Уровень образования, на базе которого осваивается ППССЗ:	основное общее образование
Квалификация:	техник по защите информации
Форма обучения:	очная

Махачкала – 2022

Рабочая программа дисциплины «Основы информационной безопасности» разработана на основе требований Федерального государственного образовательного стандарта (далее ФГОС) для среднего профессионального образования (СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Организация-разработчик: Колледж федерального государственного бюджетного образовательного учреждения высшего образования «Дагестанский государственный университет».

Разработчики:
Магомедова П. Р.- к.ю.н., доцент, зав кафедрой общепрофессиональных дисциплин Колледжа ДГУ.
Джафарова З. К. – к.э.н., доцент, преподаватель кафедры общепрофессиональных дисциплин Колледжа ДГУ.

Рецензент:

Исмиханов З.Н.- к.э.н., доцент, зав. кафедрой информационных систем и технологий программирования факультета ИИТ ДГУ.

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании кафедры общепрофессиональных дисциплин Колледжа ДГУ.

Протокол №_7_ от «_31_» _марта_ 2022 г.

Зав. кафедры _____/Магомедова П.Р.
подпись *Фамилия И.О.*

Утверждена на заседании учебно-методического совета колледжа ДГУ

Ст. методист _____/Шамсутдинова У.А.
подпись *Фамилия И.О.*

Рабочая программа дисциплины согласована с учебно-методическим управлением

«_31_» _05_ 20_22_ г. _____
подпись

СОДЕРЖАНИЕ

1. Паспорт программы учебной дисциплины
2. Структура и содержание дисциплины
3. Условия реализации дисциплины
4. Контроль и оценка результатов освоения дисциплины

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «Основы информационной безопасности»

1.1. Область применения программы

Рабочая программа дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных информационных систем» для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.

Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровью, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждается в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Основы информационной безопасности» относится к *общепрофессиональным дисциплинам профессионального цикла* ПССЗ.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

Содержание программы учебной дисциплины «Основы информационной безопасности» направлено на достижение следующих целей:

- изучение моделей структур данных;
- понимание способов классификации СУБД в зависимости от реализуемых моделей данных и способов их использования;
- изучение способов хранения данных на физическом уровне, типы и способы организации файловых систем;
- подробное изучение реляционной модели данных и СУБД, реализующих эту модель, языка запросов SQL;
- понимание проблем и основных способов их решения при коллективном доступе к данным;
- изучение возможностей СУБД, поддерживающих различные модели организации данных, преимущества и недостатки этих СУБД при реализации различных структур данных, средствами этих СУБД

Освоение содержания учебной дисциплины «Основы информационной безопасности» обеспечивает достижение студентами следующих результатов:

Общие компетенции:

ОК – 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК – 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК – 09. Использовать информационные технологии в профессиональной деятельности.

ОК – 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

Профессиональные компетенции:

ПК – 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В результате освоения дисциплины обучающийся должен уметь:

- строить модели программных проектов и программных продуктов
- работать с системами конфигурационного управления;

- выполнять процедуру восстановления базы данных и вести мониторинг выполнения этой процедуры;
- обеспечивать информационную безопасность на уровне базы данных;
- выбирать и анализировать показатели качества и критерии оценки систем защиты информации;
- подбирать информацию и пользоваться современной научно-технической литературой для решения задач защиты информации.

В результате освоения дисциплины обучающийся должен знать:
- фундаментальные концепции процесса разработки программного обеспечения,
- архитектуры программного обеспечения, управления требованиями,
- конфигурационного управления, тестирования и документирования программного обеспечения;
- основы лицензирования программного обеспечения
- основные виды тестирования программного обеспечения;
- основные методологии разработки программного обеспечения.
- роль специалиста по защите информации;
- место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства;
- содержание информационной войны, методы и средства ее ведения;
- виды информации ограниченного доступа, в соответствии с требованиями Российского законодательства;
- основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации;
- методы и средства и обеспечения информационной безопасности компьютерных систем, механизмы защиты информации;
- критерии оценки защищенности автоматизированных систем и современные методы обеспечения их информационной безопасности;
- особенности обеспечения информационной безопасности автоматизированных систем при обработке информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	88
Обязательная аудиторная учебная нагрузка (всего)	78
в том числе:	
теоретическое обучение	40
лабораторные работы	
практические занятия	38
контрольные работы	
консультации	
курсовой проект	
Самостоятельная работа обучающегося (всего)	
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	10
Промежуточная аттестация в форме *экзамена*	

2.2. Тематический план и содержание дисциплины ОП.01 «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала лабораторные и практические самостоятельная работа обучающихся, работа (проект) лекций,занятия, курсовая		*Объем часов*	*Формы и методы контроля и оценки результатов обучения*
1	2		3	
Раздел 1	Информационная безопасность в системе национальной безопасности Российской Федерации			
Тема 1.1.	**Лекция – Национальная безопасность Российской Федерации**		**4**	
	1	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства.	*2*	
	2	Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы.	*1*	
	3	Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.	*1*	
	Практические занятия		4	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра.
	1	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства.	*2*	
	2	Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы.	*1*	
	3	Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.	*1*	
	Самостоятельная работа обучающихся: - темы рефератов, эссе - ***Виды безопасности в различных сферах жизнедеятельности личности, общества и государства;*** - перечень вопросов для самостоятельного изучения: 1. Проблемы региональной информационной безопасности; 2. Основные понятия информационной безопасности		1	тестирование, коллоквиум
Тема 1.2	Лекция – Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.		4	
	1	Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации.	*1*	
	2	Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере.	*1*	
	3	Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз.	*1*	
	4	Направления обеспечения информационной безопасности государства. Проблемы региональной	*1*	

		информационной безопасности.		
	Практические занятия		4	
	1	Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра.
	2	Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере.	*1*	
	3	Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз.	*1*	
	4	Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.	*1*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе - ***Угрозы информационной безопасности Российской Федерации в различных сферах;*** - перечень вопросов для самостоятельного изучения: 1. Виды защищаемой информации и защита интеллектуальной собственности; 2. Компьютерная система как объект информационной войны		1	тестирование, коллоквиум
Тема 1.3.	**Лекция – Основные понятия и принципы теории информационной безопасности.**		**4**	
	1	Источники понятий в области информационной безопасности.	*1*	
	2	Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации.	*2*	
	3	Принципы теории информационной безопасности.	*1*	
	Практические занятия		4	
	1	Источники понятий в области информационной безопасности.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра.
	2	Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации.	*1*	
	3	Принципы теории информационной безопасности.	*2*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – ***Механизмы защиты информации компьютерных систем;*** - перечень вопросов для самостоятельного изучения: 1. Проблемы информационной безопасности в государственных структурах; 2. Информационная безопасность в сфере бизнеса		1	тестирование, коллоквиум
Тема 1.4.	**Лекция – Понятие и виды защищаемой информации.**		**4**	
	1. Понятие и сущность защищаемой информации. Права и обязанности обладателя информации.		*1*	
	2. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна,		*1*	

	коммерческая тайна, персональные данные.		
	3. Перечень сведений конфиденциального характера.	*1*	
	4. Понятие интеллектуальной собственности и особенности ее защиты.	*1*	
	Практические занятия	4	
	1. Понятие и сущность защищаемой информации. Права и обязанности обладателя информации.	1	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные.	1	
	3. Перечень сведений конфиденциального характера.	1	
	4. Понятие интеллектуальной собственности и особенности ее защиты.	1	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – ***Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства)***. - перечень вопросов для самостоятельного изучения: 1. Влияние процессов информатизации общества на составляющие информационной безопасности. 2. Состав и содержание направлений информационной безопасности.	2	тестирование, коллоквиум
Итого по разделу 1 :		***34***	
Раздел II	Информационная война, методы и средства ее ведения		
Тема 2.1.	**Лекция – Понятие и виды угроз информационной безопасности.**	**4**	
	1. Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию.	*1*	
	2. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности.	*1*	
	3. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа.	*1*	
	4. Основные элементы канала реализации угрозы безопасности информации.	*1*	
	Практические занятия	4	
	1. Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности.	*1*	
	3. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа.	*1*	
	4. Основные элементы канала реализации угрозы безопасности информации.	*1*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – ***Государственная информационная политика. История, становление, сущность и содержание, основные направления***; - перечень вопросов для самостоятельного изучения: 1. Виды информации с точки зрения информационной безопасности. 2. Виды защищаемой информации	1	тестирование, коллоквиум

Тема 2.2.	**Лекция – Информационная безопасность и информационное противоборство.**	**4**	
	1. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства.	*2*	
	2. Информационное оружие, его классификация и возможности.	*2*	
	Практические занятия	4	
	1. Субъекты информационного противоборства.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Цели информационного противоборства.	*1*	
	3. Составные части и методы информационного противоборства.	*1*	
	4. Информационное оружие, его классификация и возможности.	*1*	
	Самостоятельная работа обучающихся: - темы рефератов, эссе – ***Угрозы информационной безопасности и факторы, воздействующие на информацию;*** - перечень вопросов для самостоятельного изучения: 1. Причины, виды, каналы утечки и искажение информации. 2. Информационное оружие, его классификация и возможности	1	тестирование, коллоквиум
Тема 2.3.	**Лекция – Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны..**	**4**	
	1. Методы нарушения конфиденциальности, целостности и доступности информации.	*1*	
	2. Причины, виды, каналы утечки и искажения информации.	*1*	
	3. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.	*1*	
	4. Компьютерная система как объект информационной войны.	*1*	
	Практические занятия	4	
	1. Методы нарушения конфиденциальности, целостности и доступности информации.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Причины, виды, каналы утечки и искажения информации.	*1*	
	3. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.	*1*	
	4. Компьютерная система как объект информационной войны.	*1*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – ***Методы нарушения конфиденциальности (целостности, доступности) информации ;*** - перечень вопросов для самостоятельного изучения: 1. Национальные интересы РФ и угрозы национальной безопасности. 2. Угрозы информационной безопасности Российской Федерации.	2	тестирование, коллоквиум

Итого по разделу 11:		***26***	
Раздел III	Обеспечения информационной безопасности компьютерных систем		
Тема 3.1.	**Лекция – Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.**	***4***	
	1. Методы и средства обеспечения информационной безопасности компьютерных систем.	1	
	2. Компьютерная система как объект информационной безопасности.	1	
	3. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации.	1	
	4. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.	1	
	Практические занятия	4	
	1. Методы и средства обеспечения информационной безопасности компьютерных систем.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Компьютерная система как объект информационной безопасности.	*1*	
	3. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации.	*1*	
	4. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.	*1*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – ***Политика информационной безопасности предприятия и организации***; - перечень вопросов для самостоятельного изучения: 1. Организация физической защиты информации. 2. Организация работы с персоналом в системе информационной безопасности.	1	тестирование, коллоквиум
Тема 3.2.	**Лекция – Механизмы защиты информации в автоматизированных системах.**	**4**	
	1. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит.	*2*	
	2. Криптография для сервисов безопасности: шифрование и контроль целостности.	*1*	
	3. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.	*1*	
	Практические занятия	4	
	1. Содержание сервисов безопасности программно-технического уровня..	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит	*1*	
	3. Криптография для сервисов безопасности: шифрование и контроль целостности.	*1*	
	4. Экранирование. Анализ защищенности.		
	5. Обеспечение доступности. Туннелирование. Управление.	*1*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – Актуальные проблемы безопасности компьютерных систем. Актуальные проблемы информационной безопасности при	1	тестирование, коллоквиум

	использовании мобильных средств связи; - перечень вопросов для самостоятельного изучения: 1. Актуальные проблемы информационной безопасности в социальных сетях. 2. Актуальные проблемы информационной безопасности критически важных объектов. 3. Компьютерная система как объект информационного воздействия		
Тема 3.3.	**Лекция – Методы и критерии оценки защищенности компьютерных систем.**	**4**	
	1. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	*1*	
	2. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий.	*1*	
	3. Защита информации, обрабатываемой в автоматизированных системах от технических разведок.	*1*	
	4. Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем.	*1*	
	Практические занятия	4	
	1. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	*1*	Устный опрос, фронтальный опрос, коллоквиум, тестирование, решение ситуационных задач, деловая игра
	2. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий.	*1*	
	3. Защита информации, обрабатываемой в автоматизированных системах от технических разведок.	*1*	
	4. Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем.	*1*	
	Самостоятельная работа обучающихся: * - темы рефератов, эссе – Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Современные методы и средства защиты информации. Отечественные и зарубежные стандарты в области информационной безопасности.; - перечень вопросов для самостоятельного изучения: 1. Криптология и основные этапы ее становления и развития. 2. Комплексный подход к обеспечению информационной безопасности. 3. Основные механизмы и сервисы защиты информации. 4. Правовое обеспечение информационной безопасности.	2	тестирование, коллоквиум
Итого по разделу 1 :		***28***	
Итого по дисциплине :		**88**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- автоматизированные рабочие места обучающихся;
- автоматизированное рабочее место преподавателя;
- комплект учебно-наглядных пособий «Технология разработки и защиты баз данных».

Технические средства обучения: компьютеры с лицензионным программным обеспечением общего и профессионального назначения, мультимедиа проектор, принтер.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — URL : https://urait.ru/bcode/476997
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — URL : https://urait.ru/bcode/475889
3. Черткова, Е. А. Программная инженерия. Визуальное моделирование программных систем : учебник для среднего профессионального образования / Е. А. Черткова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 147 с. — (Профессиональное образование). — ISBN 978-5-534-09823-5. — URL : https://urait.ru/bcode/473307
4. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497642.

Дополнительная литература

1. Белов, П. Г. Системный анализ и программно-целевой менеджмент рисков : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2021. — 289 с. — (Высшее образование). — ISBN 978-5-534-04690-8. — URL : https://urait.ru/bcode/473132
2. Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю.

Федоров. — Москва : Издательство Юрайт, 2021. — 235 с. — (Профессиональное образование). — ISBN 978-5-534-05047-9. — URL : https://urait.ru/bcode/472502

3. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — URL : https://urait.ru/bcode/471382
4. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2021. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — URL : https://urait.ru/bcode/471910

Электронные ресурсы:

1. Открытые системы.- URL: http://biblioclub.ru/index.php?page=journal&jid=436083
2. Информатика в школе .- URL: http://dlib.eastview.com/browse/publication/18988
3. Программные продукты и системы.- URL: http://dlib.eastview.com/browse/publication/64086
4. Информатика и образование.- URL: http://dlib.eastview.com/browse/publication/18946
5. Системный администратор.- URL: http://dlib.eastview.com/browse/publication/66751
6. Computerword Россия.- URL: http://dlib.eastview.com/browse/publication/64081
7. Мир ПК.- URL: http://dlib.eastview.com/browse/publication/64067
8. Информационно-управляющие системы.- URL: http://dlib.eastview.com/browse/publication/71235
9. Журнал сетевых решений LAN.- URL: http://dlib.eastview.com/browse/publication/64078
10. Информатика и образование.- URL: http://dlib.eastview.com/browse/publication/1894624
11. Прикладная информатика.- URL: http://elibrary.ru/title_about.asp?id=25599

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. ЭБС «Университетская библиотека ONLINE». – URL: www.biblioclub.ru
2. ЭБС издательства «Лань». – URL: https://e.lanbook.com
3. ЭБС «ZNANIUM.COM» www.znanium.com
4. Электронный каталог Научной библиотеки КубГУ. – URL:http://212.192.134.46/MegaPro/Catalog/Home/Index
5. Электронная библиотека «Издательского дома «Гребенников» - URL:www.grebennikon.ru
6. Научная электронная библиотека (НЭБ) «eLibrary.ru». - URL:http://www.elibrary.ru
7. Базы данных компании «Ист Вью». - URL:http://dlib.eastview.com
8. Лекториум ТВ». - URL: http://www.lektorium.tv/
9. Национальная электронная библиотека «НЭБ». - URL:http://нэб.рф/ 10.КиберЛенинка: научная электронная библиотека. – URL: http://cyberleninka.ru/
10. Единое окно доступа к образовательным ресурсам : федеральная ИС свободного доступа. – URL: http://window.edu.ru.
11. Справочно-правовая система «Консультант Плюс» - URL http://www.consultant.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
В результате освоения дисциплины обучающийся должен **уметь:** - строить модели программных проектов и программных продуктов - работать с системами конфигурационного управления; - выполнять процедуру восстановления базы данных и вести мониторинг выполнения этой процедуры; - обеспечивать информационную безопасность на уровне базы данных; - выбирать и анализировать показатели качества и критерии оценки систем защиты информации; - подбирать информацию и пользоваться современной научно-технической литературой для решения задач защиты информации.	Текущий контроль: - тестирование; - практические работы; - письменные работы. - самостоятельная работа.
В результате освоения дисциплины обучающийся должен **знать:** - фундаментальные концепции процесса разработки программного обеспечения, - архитектуры программного обеспечения, управления требованиями, - конфигурационного управления, тестирования и документирования программного обеспечения; - основы лицензирования программного обеспечения - основные виды тестирования программного обеспечения; - основные методологии разработки программного обеспечения. - роль специалиста по защите информации; - место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства; - содержание информационной войны, методы и средства ее ведения; - виды информации ограниченного доступа, в соответствии с требованиями Российского законодательства; - основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации; - методы и средства и обеспечения информационной безопасности компьютерных систем, механизмы защиты информации; - критерии оценки защищенности автоматизированных систем и современные методы обеспечения их информационной безопасности; - особенности обеспечения информационной безопасности автоматизированных систем при обработке информации.	Текущий контроль: - устный опрос, - тестирование, - практические работы, - самостоятельная работа

Перечень экзаменационных вопросов:

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Виды угроз информационной безопасности Российской Федерации.
8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации
10. Источники понятий в области информационной безопасности.
11. Основные понятия информационной безопасности.
12. Общеметодологические принципы теории информационной безопасности.
13. Понятие и сущность защищаемой информации.
14. Права и обязанности обладателя информации.
15. Виды защищаемой информации.
16. Перечень сведений конфиденциального характера.
17. Понятие интеллектуальной собственности и особенности ее защиты.
18. Понятие угрозы информационной безопасности.
19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
20. Классификация и виды угроз информационной безопасности.
21. Внутренние и внешние источники угроз информационной безопасности.
22. Угрозы утечки информации и угрозы несанкционированного доступа.
23. Основные элементы канала реализации угрозы безопасности информации.
24. Субъекты и цели информационного противоборства.
25. Составные части и методы информационного противоборства.
26. Информационное оружие, его классификация и возможности.
27. Методы нарушения конфиденциальности, целостности и доступности информации.
28. Информационная война как способ воздействия на информационные системы.
29. Информационная безопасность критически важных объектов.
30. Обеспечение безопасности объектов информационной сферы государства в информационной войне.
31. Компьютерная система как объект информационной безопасности.
32. Основные способы защиты информации.
33. Понятие и классификация средств защиты информации.
34. Характеристика средств защиты информации.
35. Уровни информационной безопасности и их характеристика.
36. Сервисы безопасности программно-технического уровня.
37. Идентификация и аутентификация как сервисы безопасности.
38. Управление доступом и его виды.
39. Авторизация как сервис безопасности.
40. Протоколирование и аудит как сервисы безопасности.
41. Криптографические сервисы безопасности.
42. Экранирование как сервис безопасности.
43. Анализ защищенности как сервис безопасности.
44. Туннелирование как сервис безопасности.
45. Управление как сервис безопасности.
46. Назначение формальных моделей безопасности. Политика безопасности.

47. Понятие ролевого управления доступом.
48. Модели, стратегии и системы обеспечения информационной безопасности.
49. Критерии безопасности компьютерных систем «Оранжевая книга».
50. Общие критерии безопасности информационных технологий.
51. Стандарты по управлению информационной безопасностью
52. Классификация и возможности технических разведок.
53. Компьютерная разведка.
54. Технические каналы утечки информации при эксплуатации автоматизированных систем.
55. Электромагнитное воздействие и эффекты его воздействия.
56. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.