Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный индустриальный университет»

Кафедра прикладных информационных технологий и программирования

УТВЕРЖДАЮ
Директор института
информационных технологий и
автоматизированных систем
_____ А.В. Зимин
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

09.02.11 «Разработка и управление программным обеспечением»
(направленность (профиль): «Разработка и управление программным обеспечением»)

Квалификация выпускника
Программист

Форма обучения
Очная форма

Срок обучения: 3 года 10 месяцев

Год начала подготовки 2026

Новокузнецк
2026

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: e95695aa2c5fd4a2ad858d663abfeefbdf88f7d3
Владелец: Директор ИИТиАС Зимин Алексей Валерьевич
Действителен: с 2 апреля 2026 г. по 26 июня 2027 г.
Дата и время: 08-05-2026 11:45:02 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование представлений области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

Задачами учебной дисциплины являются:

– сформировать у обучающихся компетенции по классификации уровней секретности информации;
– научить обучающихся определять угрозы информационной безопасности и применять соответствующие меры по их устранению.

2 Место учебной дисциплины в структуре ООП по специальности

Учебная дисциплина относится к учебным дисциплинам общепрофессионального цикла ООП по специальности 09.02.11 «Разработка и управление программным обеспечением».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Проектная деятельность 1;
– Информатика;
– Основы безопасности и защиты Родины.

Учебная дисциплина дополняет умения и знания, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Защита дипломного проекта (работы);
– Проектирование и разработка баз данных;
– Проектирование и разработка веб-приложений;
– Операционные системы и среды;
– Архитектура аппаратных средств;
– Компьютерные сети;
– Основы работы с информацией;
– Проектная деятельность 2;
– Проектная деятельность 3;
– Проектная деятельность 4;
– Основы применения искусственного интеллекта и нейронных сетей в профессиональной деятельности.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

Общие компетенции

– ОК 01.: Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

– ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности

– ОК 09.: Пользоваться профессиональной документацией на государственном и иностранном языках

В результате освоения учебной дисциплины обучающийся должен уметь, знать:

Код ОК, ПК	Уметь	Знать
ОК 01. ОК 02. ОК 09.	классифицировать защищаемую информацию по видам тайны и степеням секретности, классифицировать основные угрозы безопасности информации	сущность и понятие информационной безопасности, характеристику ее составляющих место информационной безопасности в системе национальной безопасности страны виды, источники и носители защищаемой информации источники угроз безопасности информации и меры по их предотвращению факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи современные средства и способы обеспечения информационной безопасности основные методики анализа угроз и рисков

		информационной безопасности

4 Объем и содержание учебной дисциплины

Учебная деятельность обучающихся предусматривает учебные занятия (лекция, практическое занятие, консультация), самостоятельную работу, а также другие виды учебной деятельности, определенные учебным планом и календарным планом воспитательной работы.

Объем учебной дисциплины

Семестр / курс	***ИТОГО***	***3 семестр***
Форма промежуточной аттестации		*экзамен*
Трудоёмкость, *академ. час.*	***72***	*72*
Лекции, *академ. час.*	***8***	*8*
в форме практической подготовки	***0***	*0*
Лабораторные работы, *академ. час.*	***0***	*0*
в форме практической подготовки	***0***	*0*
Практические занятия, *академ. час.*	***32***	*32*
в форме практической подготовки	***0***	*0*
Курсовая работа / проект, *академ. час.*	***0***	*0*
в форме практической подготовки	***0***	*0*
Консультации, *академ. час.*	***1***	*1*
в форме практической подготовки	***0***	*0*
Самостоятельная работа, *академ. час.*	***25***	*25*
в форме практической	***0***	*0*

подготовки		
Контроль, *академ. час.*	***6***	*6*
в форме практической подготовки	***0***	*0*

Содержание учебной дисциплины

Раздел 1 Теоретические основы информационной безопасности;

Тема 1.1 Основные понятия и задачи информационной безопасности (Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.);

Тема 1.2 Основы защиты информации (Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.);

Тема 1.3 Угрозы безопасности защищаемой информации (Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к уязвимости информации. Методы оценки уязвимости информации.);

Раздел 2 Методология защиты информации;

Тема 2.1 Методологические подходы к защите информации (Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.);

Тема 2.2 Нормативно правовое регулирование защиты информации (Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.);

Тема 2.3 Защита информации в автоматизированных (информационных) системах (Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Теоретические основы информационной безопасности		
Тема 1.1.	Основные понятия и задачи информационной безопасности	1	
Тема 1.2.	Основы защиты информации	1	
Тема 1.3.	Угрозы безопасности защищаемой информации	2	
Раздел 2.	Методология защиты информации		
Тема 2.1.	Методологические подходы к защите информации	1	
Тема 2.2.	Нормативно правовое регулирование защиты информации	1	
Тема 2.3.	Защита информации в автоматизированных (информационных) системах	2	
Итого:		**8**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Теоретические основы информационной безопасности		
Тема 1.1.	Определение объектов защиты на типовом объекте информатизации	4	

Тема 1.2.	Классификация защищаемой информации по видам тайны и степеням конфиденциальности	4	
Тема 1.3.	Определение угроз объекта информатизации и их классификация	8	
Раздел 2.	Методология защиты информации		
Тема 2.1.	Основные принципы построения систем защиты информации	2	
Тема 2.2.	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	4	
Тема 2.3.	Выбор мер защиты информации для автоматизированного рабочего места	10	
Итого:		**32**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	**Темы лабораторных работ**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	**Темы курсовых работ (проектов)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	**Виды самостоятельной работы**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию.	12	

Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию.	13	
	Консультации	1	
Контроль	*Подготовка к экзамену*	6	
Итого:		**32**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые разделы (темы) дисциплины	**Контролируемые компетенции**	**Оценочные средства**
Раздел 1.	ОК 01.; ОК 02.; ОК 09.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии
Раздел 2.	ОК 01.; ОК 02.; ОК 09.	1. Вопросы для устного обсуждения (опроса); 2. Наблюдение за работой на практическом занятии
Экзамен.	ОК 01.; ОК 02.; ОК 09.	1. Экзамен на основе результатов компьютерного тестирования

11 Входной контроль

11.1 Цель входного контроля – определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания обучающегося используются как начальные значения в индивидуальном профиле академической успешности обучающегося.

11.2 Описание оценочных средств

Форма проведения входного контроля – индивидуальный или фронтальный устный опрос. В ходе проведения входного контроля обучающимся предлагается ответить на вопросы по материалу, изученному в процессе освоения ООП СПО.

Шкала оценивания устных ответов обучающихся

Критерии оценки:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– сознательность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– сопровождение ответа примерами (учитывается умение грамотно и с пользой применять фактический материал для подкрепления теоретического при устном ответе);

– рациональность использования времени, отведенного на ответ (не одобряется затянутость выполнения задания, устного ответа во времени).

Оценку «зачтено» получает обучающийся, если он при собеседовании обнаруживает знание и понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, в том числе и самостоятельно составленные; при ответе на вопросы излагает материал последовательно и правильно, полно и аргументировано отвечает по содержанию задания; рационально использует время, отведенное на ответ.

Оценку «не зачтено» получает обучающийся, который не рационально использует время, отведенное на ответ; обнаруживает незнание ответа на соответствующий вопрос; допускает ошибки в формулировке определений и правил, искажающие их смысл; беспорядочно и неуверенно излагает материал. Оценка «не зачтено» отмечает такие недостатки в подготовке обучающегося, которые требуют проведения дополнительных индивидуальных консультаций.

Вопросы для входного контроля знаний обучающихся приведены в приложении.

12 Текущий контроль

12.1 Текущий контроль знаний используется для оперативного и регулярного управления учебной деятельностью (в том числе самостоятельной) обучающихся. Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению учебной дисциплины и позволяет оценить степень освоения изученного материала.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы по индивидуальной инициативе педагогического работника, в том числе посредством использования СУО СибГИУ.

Формы проведения текущего контроля – вопросы для устного обсуждения (опроса); наблюдение за работой на практическом занятии.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию устных ответов обучающихся

С целью контроля и подготовки обучающихся к изучению новой темы в начале лекции педагогическим работником проводится индивидуальный или фронтальный устный опрос по выполненным заданиям предыдущего раздела (темы).

Критерии оценки:

– правильность ответа по содержанию задания (учитывается количество и характер ошибок при ответе);

– полнота и глубина ответа (учитывается количество усвоенных фактов, понятий и т.п.);

– сознательность ответа (учитывается понимание излагаемого материала);

– логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией);

– рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели);

– своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается умение грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе);

– использование дополнительного материала (обязательное условие);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени).

Оценка «отлично» ставится, если обучающийся:

– полно и аргументировано отвечает по содержанию задания;

– обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, в том числе самостоятельно составленные;

– излагает материал последовательно и правильно.

Оценка «хорошо» ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1 – 2 ошибки, которые сам же исправляет.

Оценка «удовлетворительно» ставится, если обучающийся обнаруживает знание и понимание основных положений данного задания, но:

– излагает материал неполно и допускает неточности в определении понятий или формулировке правил;

– не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры;

– излагает материал непоследовательно и допускает ошибки.

Оценка «неудовлетворительно» ставится, если обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. Оценка «неудовлетворительно» отмечает такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному освоению последующего материала.

12.2.2 Рекомендации по оцениванию в процессе наблюдения за работой на практическом занятии

Наблюдение за работой на практическом занятии – важнейший компонент контроля деятельности обучающихся и качества их обучения.

Критерии оценки в процессе наблюдения за работой на практическом занятии:

– самостоятельность выполнения задания и работы с методическими указаниями (учитывается работа в течение занятия, быстрота и способность нахождения в методических указаниях нужной информации);

– правильность выполнения работы (учитывается последовательность выполняемых действий, умение работать с инструментами и/или средствами вычислительной техники);

– рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения работы с учетом индивидуальных особенностей обучающихся);

– активность обучающегося при выполнении практической работы (учитывается индивидуальная работа и работа в группе).

Критерии оценки по результатам наблюдения за работой на практическом занятии

Наименование параметра оценки	Максимальное количество баллов
Самостоятельно выполняет задания; умеет работать с методическими указаниями.	2,5
Указанные в методических указаниях действия выполняет в правильной последовательности; умеет работать с инструментами и/или средствами вычислительной техники.	1,25
Рационально использует время, отведенное на задание; проявляет активность при выполнении практической работы.	1,25
Итого	**5**

Максимальное количество – 5 баллов соответствует оценке «отлично», 4 балла – «хорошо», 3 балла – «удовлетворительно», 2 балла – «неудовлетворительно».

Задания и вопросы для текущего контроля знаний обучающихся по разделам (темам) учебной дисциплины приведены в приложении.

13 Промежуточная аттестация

13.1 Оценочные материалы для промежуточной аттестации обучающихся по учебной дисциплине предназначены для оценки степени достижения запланированных результатов обучения по завершению изучения учебной дисциплины в установленной учебным планом форме и позволяют определить качество усвоения изученного материала.

Итоговой формой контроля сформированности компетенций у обучающихся по учебной дисциплине является: экзамен.

Оценочные материалы для промежуточной аттестации обучающихся включают: экзамен на основе результатов компьютерного тестирования.

13.2 Оценивание обучающегося на экзамене

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он ответил правильно на 80% - 100% тестовых заданий.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он ответил правильно на 70% - 79% тестовых заданий.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он ответил правильно на 60% - 69 %тестовых заданий.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, если он ответил правильно менее чем на 60% тестовых заданий.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) основная литература:

1 Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 161 с. – URL: https://urait.ru/bcode/542340 (дата обращения: 12.04.2026);

2 Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва: Издательство Юрайт, 2025. — 352 с. – URL: https://urait.ru/bcode/580668 (дата обращения: 04.05.2026);

3 Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. – URL: https://urait.ru/bcode/584372 (дата обращения: 04.05.2026);

4 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, 2026. — 312 с. – URL: https://urait.ru/bcode/588246 (дата обращения: 04.05.2026).

б) дополнительная литература:

1 Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. – URL: https://urait.ru/bcode/590435 (дата обращения: 12.04.2026);

2 Козырь, Н. С. Аудит информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. – URL: https://urait.ru/bcode/590434 (дата обращения: 12.04.2026);

в) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru. – URL: https://libr.sibsiu.ru;

2 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для авторизир. пользователей. – URL: https://library.sibsiu.ru/LibrELibraryFullText.asp;

3 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, [200 –]. – URL: http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

4 ЛАНЬ : электронно-библиотечная система : [Единая профессиональная база знаний издательства Лань для СПО - Издательство Лань (СПО)] / ООО «Издательство ЛАНЬ». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

5 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

6 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: https://biblioclub.ru. – Режим доступа: для авторизир. пользователей;

7 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

8 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: http://eivis.ru. – Режим доступа: по подписке.

г) лицензионное и свободно распространяемое программное обеспечение:

– 7-Zip;
– Adobe Acrobat Reader;
– Astra Linux Special Edition;
– Kaspersky Endpoint Security;
– Microsoft Office;
– Microsoft Windows;
– OnlyOffice;
– Р7-Офис.

д) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

15 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории для проведения занятий всех видов, предусмотренных учебным планом, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов, научно-техническую библиотеку СибГИУ:

- автоматизированное место преподавателя;
- автоматизированные места обучающихся;
- рабочее место преподавателя;
- посадочные места по количеству обучающихся;
- программные и программно-аппаратные средства защиты информации;
- программные средства криптографической защиты информации:
- доска маркерная или интерактивная;

- сервер;
- антивирусные программные комплексы.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС СПО по направлению подготовки (специальности) 09.02.11 «Разработка и управление программным обеспечением».

Составитель(и):

доцент Пермякова Елена Павловна (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Согласован:

Генеральный директор

ООО «Агит-плюс»  Рыжих А.Ю.

Приложение

Вопросы для входного контроля знаний обучающихся

1. Что такое многосвязный интерфейс?
2. Что называется каналом связи?
3. Как называется путь, соединяющий два смежных узла сети?
4. Какая из перечисленных топологий в основном применяется в глобальных сетях?
5. Какой тип сетевого кабеля является наиболее помехозащищённым?
6. Какой тип интерфейса использует операционная система Windows?
7. Из каких частей состоит диалог между пользователем и приложением?
8. Какие составляющие включает пользовательский интерфейс?

Задания и вопросы для текущего контроля знаний обучающихся по разделам учебной дисциплины

Тема 1.1. Основные понятия и задачи информационной безопасности

Устный опрос по теме:

1. Что входит в понятие «персональные данные»?

2. Что относится к специальным персональным данным?

2. Что такое целостность информации?

3. Как вы понимаете термин «информационная безопасность»?

4. Объясните понятие «защищённость информации».

Тема 1.2. Основы защиты информации

1. Что такое угроза информационной безопасности?

2. Чем характеризуется вредоносное программное обеспечение?

3. Что такое «фишинг»?

4. Что входит в понятие «модель защиты информации»?

5. Как называется попытка реализации угрозы ИБ?

Тема 1.3. Угрозы безопасности защищаемой информации

1. Что такое «источник угрозы»? Какими бывают источники?

2. Приведите примеры угроз конфиденциальности.

3. На что направлены угрозы целостности?

4. Какие виды угроз безопасности стоят на первом месте по опросам пользователей? Почему?

5. Что такое «канал утечки информации»?

Тема 2.1 Методологические подходы к защите информации

1. Какой документ в организации является основополагающим документом по защите информации?

2. Какие требования предъявляются в защите информации?

3. Что такое «сервисы безопасности»? Назовите основные.

4. Перечислите методы защиты от вредоносного ПО.

5. Назовите инфраструктурные способы защиты информации.

Тема 2.2 Нормативно правовое регулирование защиты информации

1. В каких основных нормативных актах РФ заложены принципы ИБ?

2. Какие международные стандарты в области ИБ вы знаете?

3. Назовите первый стандарт по ИБ, от которого произошли все остальные?

4. Назовите основные особенности стандарта COBIT.

5. Какой из законов РФ регулирует работу с персональными данными?

Тема 2.3 Защита информации в автоматизированных (информационных) системах

1. Назовите основные механизмы защиты данных.

2. Какие механизмы осуществляют контроль целостности данных?

3. Какое второе называние получили криптографические средства защиты информации?

4. На каких методах шифрования строится электронная подпись?

5. Назовите особенности биометрической аутентификации.

1 Выполнение практических работ

Задания для практических работ, теоретический и методический материал для самостоятельного изучения представлены в методических указаниях к практическим занятиям.

Примеры заданий на практические работы.

Раздел 1 Теоретические основы информационной безопасности

1. Определение объектов защиты на типовом объекте информатизации.

По описанию объекта информатизации определить: компоненты информационной системы, характеристики аппаратного обеспечения, характеристики программного обеспечения, перечень защищаемых ресурсов. Результаты представить в виде таблиц.

2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.

На рассматриваемом объекте информатизации определить: виды защищаемой информации (открытая, специализированная, коммерческая тайна, государственная тайна и др.), категории лиц, имеющих к ним доступ. Составить таблицу результатов.

3. Определение угроз объекта информатизации и их классификация.

Для рассматриваемого объекта определить список возможных угроз информационной безопасности, последствия от их реализации и каналы утечки информации.

Раздел 2 Методология защиты информации

1. Основные принципы построения систем защиты информации.

Для рассматриваемого объекта постройте модель нарушителя, модель угроз, модель защиты. Модели представить в графическом виде.

2. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

Определите основные законы РФ в области информационной безопасности и другие нормативные акты, которые вы будете использовать для выбора мер защиты.

3. Выбор мер защиты информации для автоматизированного рабочего места:

– разработайте проект подсистемы защиты информации для автоматизированного рабочего места (АРМ);

– создайте подсистему опознания и разграничения доступа для АРМ;

– создайте матрицу разграничения полномочий;

– создайте журнал входа-выхода в/из системы для регистрации событий;

– проанализируйте материал по выбору механизмов и средств обеспечения безопасности информации;

– выберите методы защиты.

3. Оценивание обучающегося на экзамене

Тестовые задания по разделам (фрагменты).

Раздел 1 Теоретические основы информационной безопасности

1. Какая из категорий является важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию»?

а) конфиденциальность
б) доступность
в) целостность

2. Следствием чего в большинстве случаев является угроза?

а) следствием наличия уязвимых мест
б) следствием наличия злоумышленников
в) следствием наличия окон опасности
г) следствием наличия источников угроз

3. Какие из вредоносных программ способны самостоятельно распространять свои копии?

а) вирусы
б) черви
в) спам
г) рекламные программы
д) программы дозвона

4. Для чего обычно предназначена «логическая бомба»?

а) для удаления вредоносного ПО из системы
б) для внедрения вредоносной программы
в) для контроля над атакуемой системой

г) для агрессивного потребления ресурсов
д) для предотвращения заражения компьютера вредоносным ПО

5. Мероприятия по защите чего вы будете разрабатывать при переупорядочении, краже, дублировании данных, возникших в вашей системе?

а) динамической целостности
б) статической целостности
в) прямой доступности
г) структурной целостности
д) достоверности данных

6. При защите чего вы примените помехоподавляющие фильтры?

а) сетей питания и каналов связи для безопасности передаваемых сигналов
б) персональных компьютеров для безопасности персональных ресурсов
в) корпоративных компьютеров для безопасности корпоративной информации

7. В вашей системе зафиксировано выполнение действий под видом лица, обладающего полномочиями, для доступа к данным? Вы предпримите ответные действия как на:

а) маскарад
б) злоупотребление полномочиями
в) подмену ролей
г) фальсификацию

Раздел 3 Методология защиты информации

1. К какому уровню безопасности относится управление персоналом?

а) к административному
б) к процедурному
в) к программно-техническому

2. В группу каких сервисов попадает большинство сервисов безопасности?

а) локализующие
б) превентивные

в) меры обнаружения нарушений
г) меры по выявлению нарушителя

3. Словосочетание «проверка подлинности» используется как синоним?

а) идентификации
б) аутентификации
в) псевдонимности
г) аудита

4. Какой из видов аутентификации является самым слабым средством проверки подлинности?

а) биометрическая аутентификация
б) парольная аутентификация
в) SMS-аутентификация
г) аутентификация по электронной подписи

5. Почему за приемлемое время специально организовать так называемую «коллизию» при хэшировании невозможно?

а) потому что хэш-функция – односторонняя
б) потому что хэш-функция – двусторонняя
в) потому что хэш-функция – обратимая

6. Вы – администратор сети. Как при ролевом управлении доступом вы определите роль пользователя в системе?

а) в соответствии с технической структурой организации
б) в соответствии с функциональной структурой организации
в) в соответствии с организационной структурой организации

7. Выберите, что как системный администратор вы должны осуществлять в рамках такого направления поддержания работоспособности, как «поддержка программного обеспечения»?

а) контроль за тем, какое программное обеспечение установлено
б) контроль за изменениями, вносимыми в программную конфигурацию
в) контроль за физическими носителями информации (флэшками, HDD-дисками и др.)
г) контроль за отсутствием неавторизованного изменения программ и прав доступа к ним