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

Комплексное обеспечение информационной безопасности

09.04.01 «Информатика и вычислительная техника»
(направленность (профиль): «Программная инженерия»)

Квалификация выпускника
Магистр

Форма обучения
Очная форма

Срок обучения: 2 года

Год начала подготовки 2025

Новокузнецк
2025

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: daba56d7b892efca3bf5c04ed0251c98b19b099c
Владелец: Директор ИИТиАС Зимин Алексей Валерьевич
Действителен: с 15 января 2025 г. по 10 апреля 2026 г.
Дата и время: 22-04-2025 14:43:51 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации в организации.

Задачами учебной дисциплины являются:

– изучить основные задачи в рамках общей проблемы обеспечения информационной безопасности в организации, решаемых организационно-правовыми, техническими и программно-аппаратными средствами защиты информации;
– обеспечить знание обучающимися принципов и методов применения технических и программно-аппаратных средств защиты информации в информационно-телекоммуникационных системах;
– научиться использовать современные пакеты прикладных программ для решения типовых задач, связанных с анализом и синтезом элементов защищенных телекоммуникационных систем;
– научиться практически решать задачи защиты данных;
– выработать навыки работы с современными техническими и программно-аппаратными средствами защиты информации;
– научиться применять системный подход к обеспечению информационной безопасности телекоммуникационных систем.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам части, формируемой участниками образовательных отношений **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.04.01 «Информатика и вычислительная техника».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Механизмы управления организационными системами;
– Разработка и реализация проектов 1;
– Облачные технологии;
– Гибкие методологии управления проектами.

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

– Управление разработкой программного обеспечения;
– Механизмы управления организационными системами;
– Методы и инструменты цифровой трансформации;
– Стандартизация и сертификация программных продуктов;
– Разработка и реализация проектов 2;
– Преддипломная практика.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Профессиональные компетенции

Наименование категории (группы) ПК	Код и наименование ПК	Код и наименование индикатора достижения ПК	Планируемые результаты обучения
	ПК-1: Способен участвовать в управлении проектированием компьютерного программного обеспечения	ПК-1.1 Анализирует архитектуру компьютерного программного обеспечения	– знать: архитектурные принципы разработки программного обеспечения. – уметь: определять объекты защиты данных, анализировать возможности осуществления атак.
		ПК-1.3 Проектирует компьютерное программное обеспечение и оценивает его качество	– знать: принципы и сервисы информационной безопасности программные средства информационной защиты. – уметь: использовать методы разработки защищённых компьютерных систем, создавать программные средства для разграничения доступа к информационной системе.

4 Объем и содержание учебной дисциплины

Учебные занятия по учебной дисциплине проводятся в форме контактной работы и в форме самостоятельной работы обучающихся.

Контактная работа включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия, практикумы), промежуточную аттестацию обучающихся и иные формы взаимодействия обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации ООП на иных условиях, в том числе при проведении промежуточной аттестации обучающихся. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Объем учебной дисциплины

Семестр / курс		***ИТОГО***	***4 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость	*академ. час.*	***216***	*216*
	зачетных единиц	***6***	*6*
Лекции, *академ. час.*		***16***	*16*
в форме практической подготовки		***0***	*0*
Лабораторные работы, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Практические занятия, *академ. час.*		***24***	*24*
в форме практической подготовки		***0***	*0*
Курсовая работа / проект, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Консультации, *академ. час.*		***0***	*0*
в форме практической подготовки		***0***	*0*
Самостоятельная работа, *академ. час.*		***149***	*149*
в форме практической подготовки		***0***	*0*
Контроль, *академ. час.*		***27***	*27*
в форме практической подготовки		***0***	*0*

Содержание учебной дисциплины

Раздел 1 Методологические основы обеспечения информационной безопасности;

Тема 1.1 Проблемы обеспечения информационной безопасности и пути их решения (Особенности обеспечения информационной безопасности в различных сферах жизнедеятельности общества и государства. Основные направления обеспечения информационной безопасности);

Тема 1.2 Основные угрозы информационной безопасности и оценка вероятности их реализации (Объекты, угрозы и источники угроз информационной безопасности. Возможные последствия угроз информационной безопасности. Методы и средства предотвращения и нейтрализации угроз информационной безопасности. Кибератаки.);

Тема 1.3 Основные свойства и показатели эффективности системы защиты информации (Обеспечение защиты информации на практике. Факторы, влияющие на уровень защиты информации);

Раздел 2 Комплексный подход к обеспечению информационной безопасности объекта;

Тема 2.1 Место киберкультуры в бизнесе (Системный подход к информационной безопасности. Эшелонированная защита от внутренних угроз. Анализ способов нарушений информационной безопасности);

Тема 2.2 Управление информационной безопасностью (Система управления информационной безопасностью. Типовые подсистемы и решения обеспечения информационной безопасности. ITIL и COBIT.).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1.	Методологические основы обеспечения информационной безопасности	8	
Раздел 2.	Комплексный подход к обеспечению информационной безопасности объекта	8	
Итого:		**16**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, *академ.час*	
		всего	**в форме практической подготовки**
Раздел 1; Тема 1.1; Тема 1.2; Тема 1.3.	Определение способов защиты информации: составление списка возможных атак и стратегий осуществления этих атак	8	
Раздел 2; Тема 2.1.	Анализ таксономии причин нарушений безопасности	8	
Раздел 2; Тема 2.2.	Использование методов разработки защищенных компьютерных систем	8	
Итого:		**24**	**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; 3. Прохождение тестирования.	74	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	75	
Контроль	*Подготовка к экзамену*	27	
Итого:		**176**	**0**

10 Матрица компетентностных задач по учебной дисциплине

Контролируемые разделы (темы) дисциплины	Контролируемые компетенции	Оценочные средства
Раздел 1.	ПК-1	1. Наблюдение за работой на практическом занятии; 2. Тестовые задания
Раздел 2.	ПК-1	1. Наблюдение за работой на практическом занятии; 2. Тестовые задания
Экзамен.	ПК-1	1. Экзамен на основе результатов текущего контроля

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 ВО.

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 «Moodle».

Формы проведения текущего контроля – наблюдение за работой на практическом занятии; тестовые задания.

12.2 Описание оценочных средств

Шкалы оценивания (методики оценки)

12.2.1 Рекомендации по оцениванию результатов тестирования обучающихся

Тестирование проводится по изученным разделам (темам) учебной дисциплины для выявления уровня знаний и умений обучающегося, мотивирования обучающегося к активизации самостоятельной работы по усвоению учебного материала, выявления и устранения пробелов в знаниях, повышения дисциплины и организации учебной деятельности обучающегося.

Тестирование проводится в СУО «Moodle» в рамках часов, отведенных на самостоятельную работу обучающихся. Для тестирования используется 20 вопросов из базы типовых тестовых заданий по изученным разделам (темам) учебной дисциплины. Обучающийся выбирает один ответ из предложенных вариантов ответа. В случае выбора неправильного ответа обучающийся получает за данный вопрос 0 баллов; в случае правильного ответа – 1 балл.

Оценка формируется в соответствии с критериями таблицы:

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.

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 текущего контроля.

13.2 Оценивание обучающегося на экзамене

Оценка	Требования к знаниям
отлично	Оценка «отлично» выставляется обучающемуся, если он получил среднюю оценку «отлично» по 2-м результатам тестирования в период текущих аттестаций в семестре, выполнил правильно и полно все практические задания и самостоятельную работу.
хорошо	Оценка «хорошо» выставляется обучающемуся, если он получил среднюю оценку «хорошо» по 2-м результатам тестирования в период текущих аттестаций в семестре, выполнил правильно и полно все практические задания.
удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, если он получил среднюю оценку «удовлетворительно» по 2-м результатам тестирования в период текущих аттестаций в семестре, выполнил правильно и полно все практические задания практические задания и самостоятельную работу.
неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, если он получил среднюю оценку «неудовлетворительно» по 2-м результатам тестирования в период текущих аттестаций в семестре или не выполнил все практические задания практические задания и самостоятельную работу.

Задания и вопросы для промежуточной аттестации обучающихся приведены в приложении.

14 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – 2-е изд. – Москва : Издательство Юрайт, 2020. – 473 с. – ISBN 978-5-534-12474-3. – URL: https://urait.ru/bcode/450277 (дата обращения: 17.04.2025);

2 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. – Москва : Издательство Юрайт, 2020. – 349 с. – URL: https://urait.ru/bcode/450998 (дата обращения: 17.04.2025);

3 Информационное право. Практикум : учебное пособие для вузов / Н. Н. Ковалева, Н. А. Жирнова, Ю. М. Тугушева, Е. В. Холодная ; под редакцией Н. Н. Ковалевой. – Москва : Издательство Юрайт, 2020. – 159 с. – ISBN 978-5-534-12442-2. – URL: https://urait.ru/bcode/449378 (дата обращения: 17.04.2025);

4 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва : Издательство Юрайт, 2020. – 325 с. – ISBN 978-5-534-03600-8. – URL: https://urait.ru/bcode/450371 (дата обращения: 17.04.2025);

5 Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. – Москва : Издательство Юрайт, 2020. – 220 с. – ISBN 978-5-9916-9244-1. – URL: https://urait.ru/bcode/452871 (дата обращения: 17.04.2025);

6 Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва : Издательство Юрайт, 2020. – 342 с. – ISBN 978-5-534-05142-1. – URL: https://urait.ru/bcode/454453 (дата обращения: 17.04.2025);

7 Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. – Москва : ЮФУ, 2018. – 120 с. – ISBN 978-5-9275-2742-7. – URL: https://www.studentlibrary.ru/book/ISBN9785927527427.html (дата обращения: 17.04.2025);

8 Ярочкин, В.И. Информационная безопасность : учебник для вузов / Ярочкин В. И. – Москва : Академический Проект, 2020. – 544 с. – ISBN 978-5-8291-3031-2. – URL: https://www.studentlibrary.ru/book/ISBN9785829130312.html (дата обращения: 17.04.2025);

9 Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В.Я. Ищейнов. – Москва : Берлин : Директ-Медиа, 2020. – 271 с. – ISBN 978-5-4499-0496-6. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 17.04.2025).

б) 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 : [коллекция «Единая профессиональная база знаний для технических вузов - Издательство Лань" ЭБС»] / 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. – URL: http://www.biblioclub.ru;

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.

в) лицензионное и свободно распространяемое программное обеспечение:

– Astra Linux Special Edition;
– LibreOffice;
– Microsoft Office;
– Microsoft Windows;
– Р7-Офис.

г) 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, оснащенные оборудованием, компьютерной техникой, и техническими средствами обучения, в том числе:

- учебную аудиторию для проведения занятий лекционного типа, оборудованную учебной доской, экраном и мультимедийным проектором;

- учебную аудиторию для проведения занятий семинарского типа (практических занятий);
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, научно-техническую библиотеку СибГИУ.
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.04.01 «Информатика и вычислительная техника».

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

1 Вопросы для входного контроля знаний обучающихся

1. Что такое «персональные данные»?
2. Номер телефона – это персональные данные?
3. Что нужно сделать организации, чтобы использовать такие общие персональные данные, как данные паспорта?
4. Где можно найти специальные персональные данные?
5. Выберите персональные данные, которые относятся к классу общих персональных данных.
6. Назовите основные информационные категории, предназначенные для защиты.

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

2 Тестирование по результатам освоения лекционного материала и самостоятельной работы

Тестирование проводится для определения степени усвоения материалов лекций, а также выполнения самостоятельной работы в рамках часов, отведенных на самостоятельную работу обучающихся, в СУО «Moodle».

Перечень вопросов для тестирования:

Раздел 1. Методологические основы обеспечения информационной безопасности.

1. Выберите основные информационные категории, предназначенные для защиты.

а) целостность
б) актуальность
в) конфиденциальность
г) доступность

2. Средства контроля какого вида целостности применяются при анализе потока финансовых сообщений для выявления кражи, переупорядочения или дублирования отдельных сообщений?

а) средства контроля статической целостности
б) средства контроля структурной целостности
в) средства контроля динамической целостности

г) средства контроля логической целостности

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

а) конфиденциальность
б) доступность
в) целостность

4. Как называются попытки реализации угрозы?
а) атаки
б) риски
в) опасности
г) агрессия

5. Какие угрозы доступности являются самыми частыми опасными с точки зрения размера ущерба?

а) непреднамеренные ошибки штатных пользователей
б) стихийные бедствия (пожары, наводнения, землетрясения и т.д.)
в) внутренний отказ информационной системы
г) отказ поддерживающей инфраструктуры

6. 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

7. Выберите правильное высказывание.

а) для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель)
б) для большинства уязвимых мест окно опасности существует сравнительно недолго (несколько минут, иногда - часов)
в) для большинства уязвимых мест окно опасности существует всегда
г) для большинства уязвимых мест окно опасности существует совсем недолго (несколько секунд, иногда - минут)

8. Какие методы осуществления угроз информационной безопасности относятся к «хакерским»?

а) DOS-атаки

б) несанкционированное проникновение в компьютерные сети
в) порча оборудования
г) разрушение инфраструктуры системы

9. Выберите существующее название угрозы конфиденциальности.

а) «маскарад»
б) «карнавал»
в) «хоровод»
г) «спектакль»
д) «цирк»

10. К угрозе чего относится «перехват данных»?

а) к угрозе конфиденциальности
б) к угрозе доступности
в) к угрозе целостности
г) к угрозе достоверности

11. Какие сведения содержит тема «Законопослушность» в Политике безопасности?

а) сведения о том, где, когда, как, по отношению к кому и чему применяется политика безопасности
б) информация о должностных лицах, ответственных за реализацию политики безопасности
в) сведения о том, куда следует обращаться за разъяснениями, помощью и дополнительной информацией
г) общее описание запрещенных действий и наказаний за них

12. Сколько уровней может содержать программа реализации политики безопасности в простейшем случае?

а) три – по количеству уровней управления организацией
б) два – верхний (центральный) и нижний (служебный)
в) достаточно одного центрального, охватывающего всю организацию

13. Что представляет наибольшую опасность на этапе эксплуатации информационного сервиса?

а) резкие изменения в конфигурации сервиса
б) значительные изменения в конфигурации сервиса
в) незначительные изменения в конфигурации сервиса

г) существенные изменения в поведении пользователей и администраторов

Раздел 2. Комплексный подход к обеспечению информационной безопасности объекта.

1. К какому уровню безопасности относится управление персоналом?

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

2. «Непрерывность защиты в пространстве и времени» – это основной принцип:

а) программной защиты
б) физической защиты
в) поддержания работоспособности
г) архитектурной безопасности

3. Выберите, почему необходима минимизация объёма защитных средств, выносимых на клиентские системы?

а) это просто слишком дорого
б) конфигурацию клиентских систем трудно или невозможно контролировать
в) распределенные по клиентским системам средства не смогут нормально взаимодействовать друг с другом

4. В чем заключается задача логического управления доступом?

а) оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на неё
б) для каждой пары «субъект-объект» определить множество допустимых операций и контролировать выполнение установленного порядка
в) назначить разграничения доступа клиентов из одного множества ИС к серверам из другого множества

5. Что такое «матрица доступа»?

а) каталог с криптографическими ключами пользователей
б) таблица отношений «субъекты-объекты»
в) последовательность символов, характеризующих пользователя

6. Что служит основой мандатного управления доступом?

а) матрица доступа
б) метки безопасности
в) списки доступа

6. В чём заключается суть ограничивающего интерфейса?

а) пользователь видит все варианты выбора, но доступ к каждому из них получает после дополнительной аутентификации
б) пользователь видит все варианты выбора, но доступ получает только к активным элементам
в) пользователь видит лишь те варианты выбора, к которым имеет доступ

7. В чём состоит суть протоколирования?

а) удостоверение подлинности сведений
б) анализ накопленной информации
в) сбор и накопление информации

8. Какие виды ключей применяются в асимметричных методах шифрования?
а) секретный ключ для шифрования
б) секретный ключ для расшифрования
в) не секретный ключ для шифрования
г) не секретный ключ для расшифрования

9. Какими средствами чаще всего реализуется хэш-преобразование?

а) средствами симметричного шифрования со связыванием блоков
б) средствами асимметричного шифрования без связывания блоков
в) средствами симметричного шифрования без связывания блоков
г) средствами асимметричного шифрования со связыванием блоков

10. Что такое «дайджест»?

а) результат применения хэш-функции к исходным данным
б) цикл применения хэш-функции к исходным данным
в) ошибка, возникающая при применении хэш-функции

11. Что называется «коллизией»?

а) совпадение результатов хэширования для различных данных
б) допустимая погрешность хэширования данных
в) ошибка, возникающая при хэшировании данных

12. Почему за приемлемое время специально организовать коллизию невозможно?

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

2 Выполнение практических работ

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