МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ИГУ»)

Институт математики и информационных технологий

Кафедра вычислительной математики и оптимизации

«УТВЕРЖДАЮ»
Директор ИМИТ ИГУ
_____ М. В. Фалалеев
«11» апреля 2025 г.

Рабочая программа дисциплины (модуля)

Б1.О.34 Основы информационной безопасности

Направление подготовки	01.03.02 Прикладная математика и информатика
Направленность (профиль) подготовки	Системная и бизнес-аналитика
Квалификация выпускника	бакалавр
Форма обучения	очная

Иркутск 2025 г.

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи: формирование представлений, знаний, умений и навыков осуществления деятельности в области информационных технологий с учетом требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б1.О.35 Основы информационной безопасности относится к обязательной части Блока 1 образовательной программы.
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Б1.О.11 Физика, Б1.О.34 Программные средства защиты информации.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б2.О.01(Пд) Преддипломная практика, Б3.01 (Д) Выполнение и защита выпускной
квалификационной работы.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки 01.03.02 Прикладная математика и информатика:
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен
знать: основные понятия и направления в защите компьютерной информации, принципы защиты информации, принципы классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, основные концепции и инструменты обеспечения безопасности в информационных системах;
уметь: настраивать средства защиты информации в соответствии с политиками разграничения доступа, осуществлять мероприятия по контролю защищенности информационных систем, определять защищаемые информационные ресурсы, планировать мероприятия по защите информации;
владеть: навыками применения средств защиты информации; приемами анализа и классификации угроз информационной безопасности.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных ед., 108 час.

Форма промежуточной аттестации: зачет.

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

Раздел дисциплины / тема	Сем.	Виды учебной работы				Формы текущего контроля; Формы промежут. аттестации
		Контактная работа преподавателя с обучающимися			Самост. работа	
		Лекции	Лаб. занятия	Практ. занятия		
Тема 1. Факторы, воздействующие на информацию.		2			4	Опрос, Проверка домашней работы
Тема 2. Система защиты информации в Российской Федерации		2	2		4	Опрос, Проверка домашней работы
Тема 3. Система защиты информации ведущих зарубежных стран		2			4	Опрос, Проверка домашней работы
Тема 4. Управление рисками		2	4		4	Опрос, Проверка домашней работы
Тема 5. Формальные модели безопасности		2	4		4	Опрос, Проверка домашней работы
Тема 6. Опасные информативные сигналы в компьютерных системах		4	10		4	Опрос, Проверка домашней работы
Тема 7. Методы защиты информации в компьютерных системах		4	4		4	Опрос, Проверка домашней работы
Тема 8. Организация защиты информации на предприятии		4	2		4	Опрос, Проверка домашней работы
Тема 9. Инженерно-техническая укреплённость		4	2		4	Опрос, Проверка домашней работы
Тема 10. Аудит безопасности		4	2		4	Опрос, Проверка домашней работы
Итого (7 семестр):		30	30		40	зач.

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Раздел дисциплины / тема	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самост. работы
	Вид самост. работы	Сроки выполнения	Затраты времени		
Тема 1. Факторы, воздействующие на информацию.	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	2 неделя	4	Опрос	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 2. Система защиты информации в Российской Федерации	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	4 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 3. Система защиты информации ведущих зарубежных стран	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	6 неделя	4	опрос	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 4. Управление рисками	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	7 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 5. Формальные модели безопасности	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	8 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 6. Опасные информативные сигналы в компьютерных системах	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	9 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru

Тема 7. Методы защиты информации в компьютерных системах	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	10 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 8. Организация защиты информации на предприятии	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	12 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 9. Инженерно-техническая укреплённость	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	14 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Тема 10. Аудит безопасности	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации	16 неделя	4	Опрос, лабораторная работа	Основная и дополнительная литература согласно раздела 5 РПД, методические материалы в ЭОР на educa.isu.ru
Общая трудоемкость самостоятельной работы (час.)			40		
Из них с использованием электронного обучения и дистанционных образовательных технологий (час.)					

4.3. Содержание учебного материала

Тема 1. Факторы, воздействующие на информацию.
Классификация факторов, воздействующих на информацию. Условия возникновения угроз информационной безопасности. Конфиденциальность, целостность и доступность. Понятие «вектор атаки».
Тема 2. Система защиты информации в Российской Федерации. Силы и средства государственной системы защиты информации. Вопросы органов исполнительной власти, составляющих систему.
Тема 3. Система защиты информации ведущих зарубежных стран. Силы и средства систем защиты информации США, Германии, Великобритании. Стандарт «Оранжевая книга». Стандарт BSI/IT. Законодательство Великобритании в области защиты информации.
Тема 4. Управление рисками. Стандарты менеджмента информационной безопасности. Оценка рисков.
Тема 5. Формальные модели безопасности. Модель Бибба. Модель Белла – Лаппаддулы. Модель Харрисона – Руззо – Ульмана.

Тема 6. Опасные информативные сигналы в компьютерных системах. Физическая природа возникновения опасных информативных сигналов. Меры противодействия распространению опасных информативных сигналов.
Тема 7. Методы защиты информации в компьютерных системах. Защита оперативной памяти. Защита данных кэша. Типовые модели разграничения доступа к ресурсам. Политики разграничения доступа.
Тема 8. Организация защиты информации на предприятии. Состав и функции сил и средств обеспечения безопасности информации. Защита информации в делопроизводстве. Режим коммерческой тайны. Режим секретности.
Тема 9. Инженерно-техническая укреплённость. Категории объектов защиты. Ограждающие конструкции. Сейфы и сейфовые комнаты. Классы взломостойкости и огнестойкости. Охранно-пожарная сигнализация.
Тема 10. Аудит безопасности. Стандарты аудита информационной безопасности. Виды аудита. Инструментальные средства аудита.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

Тема занятия	Всего часов	Оценочные средства	Формируемые компетенции
Тема 2	2	ЛР «Изучение системы защиты информации в России»	ОПК-4
Тема 4	2	Лабораторная работа «Расчёт рисков»	ОПК-4
	2	Лабораторная работа «Применение метода согласованных экспертных оценок»	ОПК-4
Тема 5	4	Лабораторная работа «Реализация дискреционных и мандатных моделей разграничения доступа»	ОПК-4
Тема 6	5	Лабораторная работа «Изучение наводок сигналов в проводных линиях»	ОПК-4
	5	Лабораторная работа «Экранирование технических средств»	ОПК-4
Тема 7	4	Лабораторная работа «Анализ защищенности с помощью средств обнаружения уязвимостей»	ОПК-4
Тема 8	2	Лабораторная работа «Анализ политики безопасности с помощью Microsoft Security Assessment Tool»	ОПК-4

Тема 9	2	Лабораторная работа «Категорирование объекта и определение требований к инженерно-технической укреплённости»	ОПК-4
Тема 10	2	Лабораторная работа «Применение средств аудита безопасности компьютерных систем»	ОПК-4

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы

Тема	Задание	Формируемые компетенции
Тема 1	Форматы представления векторов атаки	ОПК-4
Тема 3	Вклад международных организаций в информационную безопасность. Международное право в области ИБ	ОПК-4
Тема 8	Защита информации в делопроизводстве. Штатное расписание. Учет документов.	ОПК-4
Тема 10	Ассортимент средств аудита информационной безопасности	ОПК-4

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов всех форм и видов обучения является одним из обязательных видов образовательной деятельности, обеспечивающей реализацию требований Федеральных государственных стандартов высшего образования. Согласно требованиям нормативных документов самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов. Самостоятельная работа студентов представляет собой совокупность аудиторных и внеаудиторных занятий и работ. Самостоятельная работа в рамках образовательного процесса в вузе решает следующие задачи:
– закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий, превращение их в стереотипы умственной и физической деятельности;
– приобретение дополнительных знаний и навыков по дисциплинам учебного плана;
– формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;
– развитие ориентации и установки на качественное освоение образовательной программы;
– развитие навыков самоорганизации;
– формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;

– выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Подготовка к лекции. Качество освоения содержания конкретной дисциплины прямо зависит от того, насколько студент сам, без внешнего принуждения формирует у себя установку на получение на лекциях новых знаний, дополняющих уже имеющиеся по данной дисциплине. Время на подготовку студентов к двухчасовой лекции по нормативам составляет не менее 0,2 часа.

Подготовка к практическому занятию. Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии. Подготовка к практическому занятию нередко требует подбора материала, данных и специальных источников, с которыми предстоит учебная работа. Студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы доказательства авторами научных работ ценности того, чем они занимаются. В ходе самого практического занятия студенты сначала представляют найденные ими варианты формулировки актуальности исследования, обсуждают их и обосновывают свое мнение о наилучшем варианте. Время на подготовку к практическому занятию по нормативам составляет не менее 0,2 часа.

Подготовка к семинарскому занятию. Самостоятельная подготовка к семинару направлена: на развитие способности к чтению научной и иной литературы; на поиск дополнительной информации, позволяющей глубже разобраться в некоторых вопросах; на выделение при работе с разными источниками необходимой информации, которая требуется для полного ответа на вопросы плана семинарского занятия; на выработку умения правильно выписывать высказывания авторов из имеющихся источников информации, оформлять их по библиографическим нормам; на развитие умения осуществлять анализ выбранных источников информации; на подготовку собственного выступления по обсуждаемым вопросам; на формирование навыка оперативного реагирования на разные мнения, которые могут возникать при обсуждении тех или иных научных проблем. Время на подготовку к семинару по нормативам составляет не менее 0,2 часа.

Подготовка к коллоквиуму. Коллоквиум представляет собой коллективное обсуждение раздела дисциплины на основе самостоятельного изучения этого раздела студентами. Подготовка к данному виду учебных занятий осуществляется в следующем порядке. Преподаватель дает список вопросов, ответы на которые следует получить при изучении определенного перечня научных источников. Студентам во внеаудиторное время необходимо прочитать специальную литературу, выписать из нее ответы на вопросы, которые будут обсуждаться на коллоквиуме, мысленно сформулировать свое мнение по каждому из вопросов, которое они выскажут на занятии. Время на подготовку к коллоквиуму по нормативам составляет не менее 0,2 часа.

Подготовка к контрольной работе. Контрольная работа назначается после изучения определенного раздела (разделов) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они заранее получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя: — изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой; повторение учебного материала, полученного

при подготовке к семинарским, практическим занятиям и во время их проведения; изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний; составление в мысленной форме ответов на поставленные в контрольной работе вопросы; формирование психологической установки на успешное выполнение всех заданий. Время на подготовку к контрольной работе по нормативам составляет 2 часа.

Подготовка к зачету. Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра. Подготовка включает следующие действия: перечитать все лекции, а также материалы, которые готовились к семинарским и практическим занятиям в течение семестра, соотнести эту информацию с вопросами, которые даны к зачету, если информации недостаточно, ответы находят в предложенной преподавателем литературе. Рекомендуется делать краткие записи. Время на подготовку к зачету по нормативам составляет не менее 4 часов.

Подготовка к экзамену. Самостоятельная подготовка к экзамену схожа с подготовкой к зачету, особенно если он дифференцированный. Но объем учебного материала, который нужно восстановить в памяти к экзамену, вновь осмыслить и понять, значительно больше, поэтому требуется больше времени и умственных усилий. Важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. Необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к экзамену. Время на подготовку к экзамену по нормативам составляет 36 часов для бакалавров.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением о самостоятельной работе студентов, принятым Ученым советом ИГУ 22 июня 2012 г.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература:

1. Введение в криптографию / ред. В. В. Ященко. – М.: Изд-во МЦНМО, 2012. – 347 с. – ISBN: 978-5-4439-0026-1 (26 экз.)
2. Рябец Л.В. Задачник-практикум по криптографии: учеб. пособие / Л.В. Рябец. – Иркутск: Изд-во Вост-Сиб. гос. акад. образ., 2013. – 76 с. – ISBN: 978-5-85827-864-1 (30 экз.)
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК-Пресс. – 2010. – 542 с. – ISBN: 978-5-94074-518-1 (25 экз.)
4. Келлеров А. С., Корольков Ю. Д. Основы информационной безопасности : учеб. пособие. – Иркутск: Изд-во ИГУ, 2013. – 113 с. . – ISBN: 978-5-9624-0791-3 (30 экз.)

б) дополнительная литература:

1. Герман О.Н. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования / О.Н. Герман. – М.: Академия. – 2012. – 257 с. – ISBN: 978-5-7695-6786-5. Режим доступа: ЭЧЗ «Библиотех». – Неогранич. доступ.
2. Конеев И. Р. Информационная безопасность предприятия: научное издание / И. Р. Конеев, А. В. Беляев. – СПб.: БХВ-Петербург, 2003. – 733 с. – ISBN 5-94157-280-8 (99 экз).

3. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учеб. пособие / А. В. Бабаш. – М.: КноРус, 2013. – 131 с. – ISBN 978-5-406-02760-8 (50 экз.).
4. Смарт Н. Криптография: учебное пособие / Н. Смарт – М.: Техносфера, 2005. – 525 с. – ISBN 5-94836-043-1 (5 экз.)
5. Нечаев, В.И. Элементы криптографии: основы теории защиты информации: Учеб.пособие для ун-тов и пед.вузов / В.И. Нечаев. – М.: Высш. шк., 1999. – 109 с. – ISBN 5060036448 (17 экз.).
6. Чмора А. Л. Современная прикладная криптография: учеб.пособие / А.Л. Чмора – М.: Гелиос АРВ, 2001. – 244 с. – ISBN 5854380374 (51экз.)
7. Глухов М.М. Введение в теоретико-числовые методы криптографии / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. – СПб.: Лань. – 2011. – 400 с. – ISBN: 978-5-8114-1116-0. Режим доступа: ЭБС «Лань». – Неогранич. доступ.

в) базы данных, информационно-справочные и поисковые системы:

1. Банк данных угроз информационной безопасности ФСТЭК bdu.fstec.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование

ЭТОТ РАЗДЕЛ НЕ ЗАПОЛНЯТЬ

6.2. Программное обеспечение

1. LTSpice (https://www.analog.com/ru/design-center/design-tools-and-calculators/ltspice-simulator.html) (возможна замена Multisim Online Circuit Simulator (https://www.multisim.com/) или любым другим SPICE-симулятором с аналогичными возможностями моделирования электрических и логических цепей);
2. Lasarus IDE (https://www.lazarus-ide.org/);
3. Astra Linux;
4. Scan-OVAL (https://bdu.fstec.ru/scanovalforlinux);
5. Kali Linux (https://www.kali.org/).

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Оценочные средства текущего контроля

Вид контроля	Контролируемые темы	Контролируемые компетенции
опрос	1 - 10	ОПК-4
Защита отчета о лабораторной работе	2, 4 - 10	ОПК-4

Примеры оценочных средств текущего контроля

Опрос к теме 10.
Описать принцип работы и привести примеры средств активного аудита:

1. сетевой сканер;
2. сканер паролей;
3. средство поиска активности пользователя компьютерной системы;
4. тестовая вредоносная программа для проверки работоспособности САВЗ.

7.2. Оценочные средства для промежуточной аттестации

Список вопросов для промежуточной аттестации:

1. Субъективные и объективные факторы. Риск и угроза.
2. Уязвимости. Вектор атаки.
3. Применение банка данных угроз информационной безопасности.
4. Система защиты информации в РФ. Силы и средства, функции.
5. Иностранные практики защиты информации.
6. Менеджмент информационной безопасности. Методики оценки рисков. CRAMM, RiskWatch.
7. Рекомендации по стандартизации Банка России ИББС.
8. Процедуры реагирования на инциденты ИБ.
9. Модель Бибба. Краткая характеристика, преимущества и недостатки.
10. Модель Белла – Лаппадулы. Краткая характеристика, преимущества и недостатки.
11. Модель Харрисона – Руззо – Ульмана. Краткая характеристика, преимущества и недостатки.
12. Опасные информативные сигналы. Способы противодействия распространению.
13. Виды экранов. Материалы, применяемые в экранировании.
14. Условия появления наводок в проводных линиях связи.
15. Архитектурные особенности компьютерных систем, обеспечивающие защиту информации.
16. Состав и функции сил и средств обеспечения безопасности информации на предприятии.
17. Защита информации в делопроизводстве. Режим коммерческой тайны. Режим секретности.
18. Стандарты и руководящие документы в области инженерно-технической укрепленности.
19. Классы взломостойкости и огнестойкости.
20. Средства охранно-пожарной сигнализации.
21. Внутренний и внешний аудит. Цели и объекты аудита ИБ.

Примеры оценочных средств для промежуточной аттестации:

Пример тестового задания:
№1
Фактор, воздействующий на информацию - это...
а) явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней
б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
в) субъект, случайно или преднамеренно совершивший действие, следствием которого является возникновение и/или реализация угроз нарушения безопасности информации

№2
Какая из этих методик оценки рисков опирается на представление доступа к объекту в виде графа?
а) CRAMM
б) RiskWatch
в) OCTAVE

№3
Перехват сигнала в линии электропитания невозможен с "внешней" линии, входящей в трансформаторную подстанцию, потому что:
а) на подстанции объединяются фазы многих потребителей, помехи в которых зашумляют опасный информативный сигнал
б) опасный информативный сигнал не доходит до трансформаторной подстанции из-за затухания в кабеле электропитания
в) опасный информативный сигнал снимается с цепей электропитания через цепь заземления трансформаторной подстанции

№4
Какие из перечисленных экранов нуждаются в дополнительном заземлении:
а) электростатические
б) магнитостатические
в) звукопоглощающие

№5
Величина относительной магнитной проницаемости для ферромагнитных материалов:
а) стремится к 1
б) зависит от частоты сигнала
в) зависит от плотности материала

№6
Основным недостатком подавителей диктофонов является:
а) малая площадь покрытия
б) шум в звуковом диапазоне, вызывающий дискомфорт у людей
в) большие габариты

№7
Прорези трубчатого микрофона обеспечивают:
а) прием звуковой волны, приходящей с осевого направления
б) прием звуковой волны, приходящей с боковых направлений
в) прием звуковой волны, приходящей со всех направлений

№8
Для обнаружения опасного информативного сигнала в проводной линии можно воспользоваться:
а) локатором нелинейностей
б) комплексом радиомониторинга или поисковым прибором с зондами-"иглами"
в) интерцептором

№9
Контрольные мероприятия по технической защите информации, включающие поиск каналов утечки и закладных устройств, проводятся:

а) в рабочее время в повседневном режиме
б) в нерабочее время или с соблюдением конспирации
в) единственный раз перед вводом объекта информатизации в эксплуатацию

№10
Одно из основных назначений грифа "коммерческая тайна" это
а) обозначение сроков рассекречивания
б) уведомление о том, что содержимое носителя конфиденциально
в) идентификация носителя защищаемой информации

№11
Наименее защищены от вскрытия:
а) реечные замки
б) цилиндрические замки
в) кодовые замки

№12
К субъективным внутренним факторам, воздействующим на защищаемую информацию, относятся:
а) разглашение защищаемой информации лицами, имеющими к ней право доступа
б) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации
в) акустоэлектрические преобразования в ТСОИ

Разработчик: Муценек В.Е., старший преподаватель кафедры Информационных технологий