МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан физического факультета
_____ / Н.М. Буднев
«31» 08 2021 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.21 Компьютерная защита информации от несанкционированного доступа**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК:
физического факультета
Протокол № 30 от «31» августа 2021 г.

Председатель: д.ф.-м.н., профессор
_____ Н.М. Буднев

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 1 от «30» августа 2021 г.

И.о.зав.кафедрой _____ Колесник С.Н.

Иркутск 2021 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели:

1. Изучение каналов утечки информации за счет несанкционированного доступа, методов и способов технической защиты информации.

2. Формирование профессиональных знаний о проведении организационно-технических и технических мероприятий по защите информации, организации контроля эффективности создаваемых систем защиты.

Задачи:

- анализ и оценка угроз информационной безопасности объекта информатизации;
- изучение отечественных и зарубежных стандартов в области информационной безопасности;
- изучение нормативных документов по защите информации;
- применение на практике методов анализа угроз информационной безопасности от несанкционированного доступа.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б1.О.21 Компьютерная защита информации от несанкционированного доступа относится к обязательной части программы. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Б1.О.23 Сети и системы передачи информации, Б1.О.26 Программирование на языках высокого уровня, Б1.О.27 Безопасность операционных систем, Б1.О.31 Аппаратные средства вычислительной техники.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б1.О.39 Технико-экономическое обоснование и управление проектами.

При подготовке специалистов по разработке и эксплуатации современных комплексов технической защиты информации, необходимо уделять особое внимание рассмотрению вопросов взаимовлияния радиоэлектронных средств. Этой цели служит курс "Компьютерная защита информации от несанкционированного доступа".

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-3.4. Способен проводить контроль защищенности информации от несанкционированного доступа	ИДК$_{ОПК3.4.1.}$ Проводит контроль эффективности защиты информации от несанкционированного доступа;	Знать: основные угрозы защищенности объектов информатизации от несанкционированного доступа; Уметь: проводить оценку защищенности и эффективности защиты информации от

		несанкционированного доступа; Владеть: навыками оценки защищенности и эффективности защиты информации от несанкционированного доступа.

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет __2___ зачетных единиц, ___72___часов,
в том числе ___0____ зачетных единиц, __0___часов на зачет

Форма промежуточной аттестации: Зачет

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

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Защита конфиденциальной информации от несанкционированного доступа	6	15,2	8	4	8	0,2	3	Устный опрос, письменный опрос на практических занятиях
2	Защита ИСПДн от несанкционированного доступа	6	16,3	8	4	8	0,3	4	Устный опрос, письменный опрос на практических занятиях

3	Защита государственных информационных систем от несанкционированного доступа	6	16,2	8	4	8	0,2	4	Устный опрос, письменный опрос на практических занятиях
4	Защита критических информационных инфраструктур от несанкционированного доступа	6	16,3	8	4	8	0,3	4	Устный опрос, письменный опрос на практических занятиях

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
1	Защита конфиденциальной информации от несанкционированного доступа	Работа с учебником, справочной литературой, первоисточниками, конспектом	1-ая неделя	3	Устный опрос, письменный опрос на практических занятиях	Источники из основной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
2	Защита ИСПДн от несанкционированного доступа	Работа с учебником, справочной литературой, первоисточниками, конспектом	5-ая неделя	4	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
3	Защита государственных информационных систем от несанкционированного доступа	Работа с учебником, справочной литературой, первоисточниками, конспектом	9-ая неделя	4	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
4	Защита критических информационных инфраструктур от несанкционированного доступа	Работа с учебником, справочной литературой, первоисточниками, конспектом	13-ая неделя	12	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
Общий объем самостоятельной работы по дисциплине (час)				**15**		

4.3. Содержание учебного материала

Тема 1. Защита конфиденциальной информации от несанкционированного доступа

Введение. Требования руководящих документов к защите конфиденциальной информации от несанкционированного доступа. Требования к настройке систем защиты информации от несанкционированного доступа.

Тема 2. Защита ИСПДн от несанкционированного доступа

Введение. Требования руководящих документов к защите ИСПДн от несанкционированного доступа. Требования к настройке систем защиты информации от несанкционированного доступа.

Тема 3. Защита государственных информационных систем от несанкционированного доступа

Введение. Требования руководящих документов к защите ГИС от несанкционированного доступа. Требования к настройке систем защиты информации от несанкционированного доступа.

Тема 4. Защита критических информационных инфраструктур от несанкционированного доступа

Введение. Требования руководящих документов к защите КИИ от несанкционированного доступа. Требования к настройке систем защиты информации от несанкционированного доступа.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	1	ПР1. Защита конфиденциальной информации от несанкционированного доступа	8	8	Защита лабораторной работы	ОПК-3.4.
2	2	ПР2. Защита ИСПДн от несанкционированного доступа	8	8	Защита лабораторной работы	ОПК-3.4.
3	3	ПР3. Защита государственных информационных систем от несанкционированного доступа	8	8	Защита лабораторной работы	ОПК-3.4.
4	4	ПР4. Защита критических информационных инфраструктур от несанкционированного доступа	8	8	Защита лабораторной работы	ОПК-3.4.

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

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	2	3	4	5
1	ПР1. Защита конфиденциальной информации от несанкционированного доступа	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-3.4.	ОПК3.4.1.
2	ПР2. Защита ИСПДн от несанкционированного доступа	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-3.4.	ОПК3.4.1.
3	ПР3. Защита государственных информационных систем от несанкционированного доступа	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-3.4.	ОПК3.4.1.
4	ПР4. Защита критических информационных инфраструктур от несанкционированного доступа	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	ОПК-3.4.	ОПК3.4.1.

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе которой студент активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. В процессе проведения самостоятельной работы формируется компетенция ПК-1.

На самостоятельную работу выносятся следующие вопросы по темам дисциплины:

Тема 1. Защита конфиденциальной информации от несанкционированного доступа. Проработка лекционного материала и материала практического занятия (3ч).

Тема 2. Защита ИСПДн от несанкционированного доступа. Проработка лекционного материала и материала практического занятия (4ч).

Тема 3. Защита государственных информационных систем от несанкционированного доступа. Проработка лекционного материала и материала практического занятия (4ч).

Тема 4. Защита критических информационных инфраструктур от несанкционированного доступа. Проработка лекционного материала и материала практического занятия (4ч).

Контроль самостоятельной работы проводится на практических занятиях.

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Технические средства и методы защиты информации [Текст] : учеб. пособие / А. П. Зайцев [и др.] ; ред.: А. П. Зайцев, А. А. Шелупанов. - 4-е изд., испр. и доп. - М. : Горячая линия — Телеком, 2009. - 615 с. ; 21 см. - (Учебное пособие для вузов). - Библиогр.: с. 608-609. - ISBN 978-5-9912-0084-4

2. Защита объектов и информации от технических средств разведки [Текст] : учеб. пособие / Ю. К. Меньшаков ; Рос. гос. гуманит. ун-т. - М. : Изд-во РГГУ, 2002. - 400 с. : ил. ; 21 см. - Библиогр.: с. 396-399. - ISBN 5-7281-0487-8

3. Физические основы технических средств обеспечения информационной безопасности [Текст] : учеб. пособие для студ. вузов / А. Н. Соболев, В. М. Кириллов. - М. : Гелиос АРВ, 2004. - 223 с. : граф., рис. ; 20 см. - ISBN 5-85438-084-6

4. Защита конфиденциальной информации [Текст] : учеб. пособие для студ. вузов / В. Я. Ищейнов, М. В. Мецатунян. - М. : Форум, 2011. - 254 с. : ил. ; 22 см. - (Высшее образование). - Библиогр.: с. 249-252. - ISBN 978-5-91134-336-1

б) базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex.
2. Электронные ресурсы доступные по логину и паролю, предоставляемые Научной библиотекой ИГУ.

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Чтение лекций сопровождается демонстрацией информации (мультимедийный проектор, офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материалов).

6.2. Программное обеспечение:

1. Microsoft PowerPoint
2. Microsoft Windows.

6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Наименование тем занятий с указанием форм/ методов/ технологий обучения:

№ п/п	Тема занятия	Вид занятия	Форма / Методы//технологии дистанционного, интерактивного обучения	Количество часов
1	**2**	**3**	**4**	**5**
1	ПР1. Защита конфиденциальной информации от несанкционированного доступа	Практическое занятие	Групповая дискуссия	5
2	ПР2. Защита ИСПДн от несанкционированного доступа	Практическое занятие	Групповая дискуссия	5
3	ПР3. Защита государственных информационных систем от несанкционированного доступа	Практическое занятие	Групповая дискуссия	5
4	ПР4. Защита критических информационных инфраструктур от несанкционированного доступа	Практическое занятие	Групповая дискуссия	4,2
Итого часов:				**19,2**

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные материалы (ОМ)

8.1.1. Оценочные материалы для входного контроля

Не предусмотрено

8.1.2 Оценочные материалы текущего контроля

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ4. Текущий контроль направлен на выявление сформированности компетенций ОПК-3.4..

Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

Усвоение студентом изучаемой дисциплины максимально оценивается 100 баллами. Максимальное количество баллов за текущую работу в семестре ограничивается 60-ю баллами, на оценку экзамена максимально предусмотрено 30 баллов. Возможны «премиальные» баллы (от 0 до 10), которые могут быть добавлены студенту за активные формы работы, высокое качество выполненных практических работ и т.д.

За посещение одного вида занятия дается 1.1 балла (24 занятия (Л+Пз) * 1.1 балл = 26.4 балла), максимальное количество баллов за письменный контроль на Пз – 2.1 балла (8 занятий (ПЗ)*2.1 балл = 16,8 балла).

Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ6.

Критерии оценки	Оценка / баллы			
	Отлично 2.1 балла.	Хорошо 1.4 балла	Удовлетв. 0.7 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок.

Вопросы для письменного текущего контроля приведены ниже:

1. Требования руководящих документов к защите конфиденциальной информации от несанкционированного доступа.
2. Требования к настройке систем защиты информации от несанкционированного доступа.
3. Требования руководящих документов к защите ИСПДн от несанкционированного доступа.
4. Требования к настройке систем защиты информации от несанкционированного доступа.
5. Требования руководящих документов к защите ГИС от несанкционированного доступа.
6. Требования к настройке систем защиты информации от несанкционированного доступа.
7. Требования руководящих документов к защите КИИ от несанкционированного доступа.
8. Требования к настройке систем защиты информации от несанкционированного доступа.

Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ4.

Критерии оценки	Оценка / баллы			
	Отлично/ 2.1 балла.	Хорошо/ 1.4 балла	Удовлетв. / 0.7 балла.	Неудовл. / 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок.

8.1.3 Оценочные материалы для промежуточной аттестации

Промежуточная аттестация проводится в форме зачета. Форма проведения зачета – устный по билетам или письменный по билетам. Зачет проводится во время зачетной недели в соответствии с расписанием.

Зачетный билет состоит из двух теоретических вопросов. Зачетные задания (билеты) выполнены многовариантными, чтобы исключить возможность списывания и обмена информацией в ходе зачета. Вопросы для самостоятельной подготовки студентов к зачету приведены в приложении 1.

Студент допускается к зачету в том случае, если в течение семестра защищены все лабораторные работы. Во время зачета студент может набрать до 30 баллов. Если на зачете ответ студента оценивается менее чем 16-ю баллами, то зачет считается не сданным, студенту выставляется 0 баллов, а в ведомость выставляется оценка «не зачтено».

Если на зачете студент набирает 16 и более баллов, то зачет считается сданным, в ведомость выставляется оценка «зачтено».

Критерии	Оценка			
	Зачтено		Не зачтено	
Знание	Всесторонние глубокие знания **(10 -11 баллов)**	Знание материала в пределах программы **(7 -9 баллов)**	Отмечены пробелы в усвоении программного материала **(4 -6 баллов)**	Не знает основное содержание дисциплины **(0-3 балла)**
Понимание	Полное понимание материала, приводит примеры, дополнительные вопросы не требуются **(8 -10 баллов)**	Понимает материал, приводит примеры, но испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы **(6 -8 баллов)**	Суждения поверхностны, содержат ошибки, примеры не приводит, ответы на дополнительные вопросы неуверенные **(4 -6 баллов)**	С трудом формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы **(0-3 балла)**
Применение проф. терминологии	Дает емкие определения основных понятий, корректно использует профессиональную терминологию**(3-5 баллов)**	Допускает неточности в определении понятий, не в полном объеме использует профессиональную терминологию **(2-3 балла)**	Путает понятия, редко использует профессиональную терминологию **(1-2 балла)**	Затрудняется в определении основных понятий дисциплины, некорректно использует профессиональную терминологию (**0-2 балла**)
Соблюдение норм литературного языка	Соблюдает нормы литературного языка, преобладает научный стиль изложения **(3-4 балла)**	Соблюдает нормы литературного языка, допускает единичные ошибки **(2- 3 балла)**	Допускает множественные речевые ошибки при изложении материала **(1-2 балл)**	Косноязычная речь искажает смысл ответа (**0-1 балл**)

№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	**2**	**3**	**4**
1	Тест	Темы 1-4	ОПК-3.4.
2	Промежуточная аттестация – экзамен	Темы 1-4	ОПК-3.4.

Демонстрационный вариант теста №1

1. На каком этапе создания системы защиты персональных данных разрабатывается частная модель угроз?
1) предпроектная стадия
2) стадия проектирования
3) ввод в действие
4) эксплуатация

2.Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?
1) конфиденциальность
2) доступность
3) целостность
4) аутентичность

3.Обработка персональных данных считается неавтоматизированной, если осуществляется:
1) без использования ЭВМ
2) без использования сети Интернет
3) при непосредственном участии человека
4) без использования средств защиты информации

4.Основные принципы и правила обеспечения безопасности персональных данных при обработке в информационных системах регулируются:
1) Федеральным законом “О персональных данных”
2) Федеральным законом “Об информации, информационных технологиях и о защите информации”
3) Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных
4) Конституцией РФ

5.От чего должны быть защищены персональные данные при их обработке в ИСПД?
1) от утечки по техническим каналам утечки
2) от стихийных бедствий
3) от несанкционированного доступа, в том числе случайного
4) от передачи по сети Интернет
5) от передачи на носителях, открытых на запись

6.Результатом предпроектного этапа построения системы защиты персональных данных является:
1) аттестация ИСПД
2) сертификация средств защиты
3) разработка частного технического задания СЗПД
4) уведомление Роскомнадзора о намерении обрабатывать персональные данные

7.Какая подсистема в рамках СЗПД предназначена для защиты ПД при передаче по открытым каналам связи или в несегментированной сети?
1) подсистема антивирусной защиты
2) подсистема анализа защищенности
3) подсистема обнаружения вторжений
4) подсистема управления доступом, регистрации и учета
5) подсистема обеспечения целостности
6) подсистема безопасности межсетевого взаимодействия
7) подсистема криптографической защиты информации

8.Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?
1) атака
2) угроза

3) уязвимость
4) слабое место системы
9.Ситуация, когда работник оператора сохранил персональные данные в виде файла на компьютере, считается:
1) автоматизированной обработкой персональных данных
2) неавтоматизированной обработкой персональных данных
3) запрещенной обработкой персональных данных в соответствии с ФЗ “О персональных данных”
4) неавтоматизированной обработкой, если работник не знал, что это персональные данные
10.На каком этапе построения системы защиты персональных данных происходит выявление технических каналов утечки информации?
1) оценка обстановки
2) разработка замысла защиты
3) реализация замысла защиты
4) решение вопросов управления защитой
11.Как называется воздействие на защищаемую информацию с нарушением установленных прав и или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации?
1) случайный несанкционированный доступ
2) несанкционированный доступ
3) неправомерный доступ
4) утечка по техническому каналу утечки информации
12.На каком этапе создания СЗПД разрабатывается задание и проект проведения работ?
1) предпроектная стадия
2) стадия проектирования
3) ввод в действие
4) эксплуатация
13.Какая подсистема в рамках СЗПД предназначена для защиты информационной системы от вредоносных программ?
1) подсистема антивирусной защиты
2) подсистема анализа защищенности
3) подсистема обнаружения вторжений
4) подсистема безопасности межсетевого взаимодействия
14.Какой уровень защиты информации состоит из мер, реализуемых людьми?
1) законодательный
2) процедурный
3) программно-технический
4) административный
15.Сколько классов защищенности от несанкционированного доступа устанавливается для автоматизированных систем обработки информации?
1) 3
2) 5
3) 9
4) 10
16.Какие виды ущерба выделяют в зависимости от объекта, которому наносится ущерб?
1) персональный ущерб
2) опосредованный ущерб
3) косвенный ущерб
4) непосредственный ущерб
5) коллективный ущерб

17.Для какого класса ИСПД меры и способы защиты определяет оператор персональных данных?
1) 1
2) 2
3) 3
4) 4
18.На каком этапе создания СЗПД производится опытная эксплуатация средств защиты?
1) предпроектная стадия
2) стадия проектирования
3) ввод в действие
4) эксплуатация
19.При использовании антивируса, использующего сигнатурный метод для обнаружения вируса, необходимо:
1) регулярно изучать информацию о новых вирусах в сети
2) регулярно обновлять антивирусную базу
3) подключить к антивирусу системные журналы
4) регулярно обмениваться с друзьями антивирусными базами
20.Какой федеральный закон является базовым в Российском законодательстве в области информационных отношений и информационной безопасности?
1) о персональных данных
2) о техническом регулировании
3) об информации, информационных технологиях и о защите информации
4) о лицензировании отдельных видов деятельности
21.К каким классам защищенности должны быть отнесены автоматизированные системы обработки персональных данных?
1) 1 В
2) 2 В
3) 3 В
4) 2 Б
5) 3 Б
6) не ниже 1Д
22.Если злоумышленник получил доступ к реквизитам банковской карты человека и украл 1000 рублей, то о каком виде ущерба идет речь?
1) явный ущерб
2) опосредованный ущерб
3) непосредственный ущерб
4) ущерб в особо крупном размере
23.Требования по защите от НСД каких классов ИСПД в однопользовательском режиме совпадают?
1) 1 и 3 классов
2) 1 и 2 классов
3) 2 и 3 классов
4) 3 и 4 классов
24.К организационным мерам по защите персональных данных можно отнести:
1) выбор адекватных и достаточных технических средств защиты информации
2) уведомление уполномоченного органа о намерении обрабатывать ПД
3) определение должностных лиц, которые будут работать с ПД
4) применение межсетевых экранов на границе локальной сети и Интернета
5) обучение персонала
6) опытная эксплуатация средств защиты информации
7) получение письменного согласия на обработку ПД от субъектов ПД

25.Как называется метод нахождения вирусов, представляющий собой совокупность приблизительных методов, основанных на тех или иных предположениях?
1) сравнительный
2) сигнатурный
3) приблизительный
4) эвристический
26.Совокупность содержащихся в базах данных информации, обеспечивающих ее обработку информационных технологий и технических средств, называется:
1) система защиты информации
2) автоматизированная система
3) информационная система
4) система обработки персональных данных
27.В случае обеспечения безопасности в локальных вычислительных сетях без использования внутренних межсетевых экранов средства защиты должны использоваться:
1) во всех узлах сети, где обрабатывается конфиденциальная информация
2) во всех узлах сети, независимо от того, обрабатывают они конфиденциальную информацию или нет
3) на серверах сети
4) на пользовательских ЭВМ
28.Если в результате атаки отказ в обслуживании на медицинское учреждение база данных пациентов стала недоступна, о каком виде ущерба идет речь?
1) нематериальный ущерб
2) неявный ущерб
3) непосредственный ущерб
4) опосредованный ущерб
29.Анализ защищенности информационных систем проводится с помощью:
1) межсетевых экранов
2) сканеров безопасности
3) браузеров
4) команды ping
30.Какой уполномоченный орган должен уведомить оператор о своем намерении обрабатывать ПД?
1) ФСБ России
2) ФСТЭК России
3) Роскомнадзор
4) Роспотребнадзор

Примерный перечень вопросов и заданий к экзамену

1. Электронный документ (ЭД). Понятие ЭД. Типы ЭД.
2. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
3. Понятие несанкционированного доступа (НСД), классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.
4. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
5. Политика безопасности в компьютерных системах. Оценка защищенности.
6. Способы защиты конфиденциальности, целостности и доступности в КС.
7. Руководящие документы ФСТЭК по оценке защищенности от НСД.
8. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация (понятие, способы хранения, связь с ключевыми системами).

9. Основные подходы к защите данных от НСД. Шифрование. Контроль доступа. Разграничение доступа.
10. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
11. Организация доступа к файлам. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
12. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
13. Способы фиксации факторов доступа. Журналы доступа и критерии их информативности.
14. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
15. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).
16. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
17. Защита массивов информации от изменения (имитозащита). Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения.
18. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
19. Построение программно-аппаратных комплексов шифрования.
20. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.
21. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
22. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.
23. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
24. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств.
25. Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования.
26. Надежность средств защиты компонент. Понятие временной и гарантированной надежности.
27. Несанкционированное копирование программ. Юридические аспекты несанкционированного копирования программ. Несанкционированное копирование программ как тип НСД.
28. Защита программ от несанкционированного копирования (общее понятие защиты от копирования). Разновидности задач защиты от копирования.
29. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.
30. Способы создания некопируемых меток. Точное измерение характеристик форматирования дорожки. Технология «слабых битов».
31. Физические метки и технология работы с ними.
32. Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ.

33. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».
34. Хранение ключей информации.
35. Секретная информация, используемая для контроля доступа: ключи и пароли.
36. Классификация средств хранения ключей и идентифицирующей информации.
37. Организация хранения ключей (с примерами реализации).
38. Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО.
39. Способы изучения ПО: статистическое и динамическое изучение. Роль программной и аппаратной среды.
40. Временная надежность (невозможность обеспечения гарантированной надежности).
41. Задачи защиты от изучения и способы их решения.
42. Защита от отладки: итеративный программный замок.
43. Защита от отладки: принцип ловушек и избыточного кода.
44. Защита от дизассемблирования. Принцип внешней загрузки файлов.
45. Динамическая модификация программы. Защита от трассировки по прерываниям.
46. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки.
47. Программно-аппаратные средства реализации блочных шифров с секретным ключом в различных режимах функционирования: базовые режимы простой замены, электронной кодовой книги, режимы гаммирования, сцепления блоков.
48. Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности.
49. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

Разработчики:

доцент Марков В.П.

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «30» августа 2021 г. Протокол № 1

И.О. зав. кафедрой  Колесник С.Н.