МИНОБРНАУКИ РОССИИ

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

УТВЕРЖДАЮ:
Декан _____ Буднев Н.М.
«06» мая 2022 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.33 Модели информационной безопасности**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Техническая защита информации**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №32 от «23» марта 2022 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 6 от «01» марта 2022 г.

И.О. зав. кафедрой _____ Колесник С.Н.

Иркутск 2022 г

Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ…….3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО……....3
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ……..3
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ…….5
4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов…….5
4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине…….6
4.3. Содержание учебного материала ……...8
4.3.1. Перечень семинарских, практических занятий и лабораторных работ.....9
4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)…….10
4.4. Методические указания по организации самостоятельной работы студентов…...12
4.5. Примерная тематика курсовых работ……..12
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ ……13
а) основная литература……..13
б) дополнительная литература……..13
в) базы данных, информационно-справочные и поисковые системы……..13
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ……13
6.1. Учебно-лабораторное оборудование……..13
6.2. Программное обеспечение……13
6.3. Технические и электронные средства…….13
7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ…….13
8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ……...14

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели и задачи дисциплины «Модели информационной безопасности»

Цели: Главной целью дисциплины является формирования у обучающихся универсальных, общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 **«Информационная безопасность»** направленность (профиль) «**Техническая защита информации»,** а также изучение теоретических, методологических и практических проблем методики формализации политики информационной безопасности, моделирования управления потоками информации, разграничением доступа.

Задачи:

– практико-ориентированное обучение, позволяющее сочетать фундаментальные знания с практическими навыками по направлению подготовки 10.03.01 Информационная безопасности, учитывающие требования предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями и иных источников;

– формирование готовности выпускников Университета к активной профессиональной и социальной деятельности

- раскрытие места информационной безопасности и защиты информации в системе информационных отношений;

- раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации;

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина «**Модели информационной безопасности»** относится к обязательной части программы

Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*:*
«Психология социального взаимодействия, саморазвития и самоорганизации», «Документоведение. Нормативные документы в сфере информационной безопасности». «Защита и обработка конфиденциальных документов», «Основы построения и функционирования технических средств защиты информации», «Компьютерная защита информации от несанкционированного доступа», «Управление проектами», «Защита информации от утечки по техническим каналам», «Организационное и правовое обеспечение информационной безопасности»

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: «Техническая защита персональных данных», «Техническая защита объектов критической информационной инфраструктуры», «Государственная итоговая аттестация».

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

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

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защит	ИДК$_{ОПК10.2.}$ Организовывает, поддерживает и управляет выполнением комплекса мер по обеспечению информационной безопасности	**Знать:** методику создания организационно-распорядительных документов по защите информации. **Уметь:** применять методику создания организационно-распорядительных документов по защите информации. **Владеть:** навыками по применению методики создания организационно-распорядительных документов по защите информации.

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 5 зачетных единиц, 180 часов,

Из них реализуется с использованием электронного обучения и дистанционных образовательных технологий 26 часов

Форма промежуточной аттестации: экзамен

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/ Форма промежуточной аттестации (по семестрам)
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Тема 1. Основные понятия и определения моделей информационной безопасности	5	20		6	6	0,2	10	Устный опрос, решение практических задач
2	Тема 2. Модель дискреционного доступа (DAC)	5	30		7	7	0,2	20	Устный опрос, решение

									практических задач
3	Тема 3. Модель безопасности белла-ЛаПадулы	5	30		7	7	0,2	20	Устный опрос, решение практических задач
4	Тема 4. Ролевая модель контроля доступа (RBAC)	5	26		7	7	0,2	20	Устный опрос, решение практических задач
5	Тема 5. Системы разграничения доступа	5	25		7	7	0,2	14	Устный опрос, решение практических задач
					34	**34**		**84**	

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.)		
5	Тема 1. Основные понятия и определения моделей информационной безопасности	внеаудиторная	1-4неделя	10	Выполнение заданий по семинарским работам	Источники 1,2 из основной литературы и 1 из дополнительной
5	Тема 2. Модель дискреционного доступа (DAC)			20		

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
5	Тема 3. Модель безопасности белла-ЛаПадулы	внеаудиторная	5-9 неделя	20	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
5	Тема 4. Ролевая модель контроля доступа (RBAC)	внеаудиторная	10-13 неделя	20	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
5	Тема 5. Системы разграничения доступа	внеаудиторная	14-16 неделя	14	Выполнение заданий по семинарским работам	Источники 1,3 из основной литературы и 2 из дополнительной
Общий объем самостоятельной работы по дисциплине (час)				**84**		
Из них объем самостоятельной работы **с использованием электронного обучения и дистанционных образовательных технологий (час)**				**20**		

4.3.Содержание учебного материала

Тема 1. Основные понятия и определения моделей информационной безопасности

Цель моделирования информационной безопасности. Определение потоков информации, разрешений, правил управления доступом.

Тема 2. Модель дискреционного доступа (DAC)

Объект и субъект модели. Информационные ресурсы. Система запросов доступа к объекту. Преимущества и недостатки модели дискреционного доступа, при реализации на различных информационных платформах, для различных классов защищаемых информационных систем. Автоматизация реализации модели дискреционного доступа.

Тема 3. Модель безопасности белла-ЛаПадулы

Понятие мандатного управления доступом. Определение субъекта и объекта операции доступа. Свойства простой безопасности. Правила разграничения доступа в системе с управляемыми уровнями секретности информации. Математическая формализация модели. Преимущества и недостатки реализации модели Ла-Падулы на различных операционных системах.

Тема 4. Ролевая модель контроля доступа (RBAC)

Ролевой метод управления доступом. Понятия и определения ролевой модели. Математическая формализация. Средства и способы выполнения ролей в информационных системах различного уровня защиты. Достоинства и недостатки ролевой модели контроля доступа.

Тема 5. Системы разграничения доступа

Основные требования к реализации диспетчера доступа. Принципы и концепции воплощения систем разграничения доступа к данным. Особенности реализации и формализации СРД в различных информационных системах, и платформах ОС.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

4.3.5 Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы) *
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	1	Тема 1. Основные понятия и определения моделей информационной безопасности	6		Выполнение заданий по вопросам семинара	$ИДК_{ОПК10.2}$
2	2	Тема 2. Модель дискреционного доступа (DAC)	7		Выполнение заданий по вопросам семинара	$ИДК_{ОПК10.2}$

3	3	Тема 3. Модель безопасности белла-ЛаПадулы	7		Выполнение заданий по вопросам семинара	ИДК$_{ОПК10.2}$
4	4	Тема 4. Ролевая модель контроля доступа (RBAC)	7		Выполнение заданий по вопросам семинара	ИДК$_{ОПК10.2}$
5	5	Тема 5. Системы разграничения доступа	7		Выполнение заданий по вопросам семинара	ИДК$_{ОПК10.2}$

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	Тема 1. Основные понятия и определения моделей информационной безопасности	Подготовка по вопросам семинара	ОПК-10	ИДК$_{ОПК10.2}$
2	Тема 2. Модель дискреционного доступа (DAC)	Подготовка по вопросам семинара	ОПК-10	ИДК$_{ОПК10.2}$
3	Тема 3. Модель безопасности белла-ЛаПадулы	Подготовка по вопросам семинара	ОПК-10	ИДК$_{ОПК10.2}$
4	Тема 4. Ролевая модель контроля доступа (RBAC)	Подготовка по вопросам семинара	ОПК-10	ИДК$_{ОПК10.2}$
5	Тема 5. Системы разграничения доступа	Подготовка по вопросам семинара	ОПК-10	ИДК$_{ОПК10.2}$

4.4. Методические указания по организации самостоятельной работы студентов

а) Методические рекомендации по изучению теоретической части учебного модуля

Теоретические занятия дисциплины представлены в виде лекций.

Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом дисциплины.

Задачи лекционных занятий – дать связанное, последовательное изложение материала, сообщить студентам основное содержание предмета в целостном, систематизированном виде.

Структура и содержание основных разделов **(**приведена в рабочей программе учебной дисциплины, раздел 4.1)

Методы и средства проведения теоретических занятий

При изучении учебного модуля студенты должны посещать лекционные занятия, вести конспекты и самостоятельно прорабатывать по учебникам вопросы, указанные преподавателем. (Список основной литературы приведен разделе 5).

Отличительной особенностью данной дисциплины является ее практическая направленность. В ходе лекций предполагается рассматривать только основные теоретические вопросы защиты информации, а подробное изучение теоретических положений и практических приложений теории, а также получение навыков работы в современных информационных системах защиты информации на языке программирования высокого уровня должно проводиться в часы семинарских занятий, а также внеаудиторной СРС. Для этого преподаватель выдает студентам задания по вопросам на семинарских занятиях.

б) Методические рекомендации по самостоятельной работе студентов

Аудиторная самостоятельная работа студентов заключается в выполнении одной контрольной реферативной работы в середине семестра и сдаче итогового экзаменационного теста для получения оценки. Внеаудиторная самостоятельная работа студентов заключается в подготовке к лекционным занятиям, подготовке к выполнению семинарских заданий. Самостоятельная работа подразумевает систематический подход к обучению, в соответствии с предложенным в разделе 4.2 графиком, что, в свою очередь, способствует успешной подготовке к зачету.

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

5 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ				
5.1 Учебная литература				
5.1.1 Основная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л1.1	В.Я.Ищейнов.	Защита конфиденциальной информации: учебное пособие	Изд. Фррум,М 2015. – 146 с.	25
Л1.2	М. В. Гришина	Комплексная система защиты информации на предприятии: учебное пособие	Изд. Фррум,М 2009. - 2009	18
Л1.3	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% Онлайн
Л14	М.А. Лапина, А.Г. Ревин, В.И. Лапин	Информационное право : учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% Онлайн
5.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие	М. ; Берлин : Директ-Медиа, 2015	100% онлайн

		//biblioclub.ru/index.php?page=book&id=276557		
Л2.2	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% онлайн
Л2.3	Коваленко, Ю.И	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/5163	М. : Горячая линия-Телеком, 2012	100% Онлайн
5.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	- Иркутск: ИрГУПС, 2013	55
5.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Глухов Н.И.	Материалы для самостоятельной работы студентов	Личный кабинет студента	100% онлайн
5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Линия защиты «Сюртель» www.suritel.ru			
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
5.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем				
5.3.1 Перечень базового программного обеспечения				
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд		
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org		
5.3.2 Перечень специализированного программного обеспечения				
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.			
5.3.3 Перечень информационных справочных систем				
6.3.3.1	«Консультант +» http://www.consultant.ru/			
6.3.3.2	«Техэксперт» http://www.cntd.ru/			
5.4 Перечень правовых и нормативных документов				
6.4.1	Не предусмотрено			

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материала.

6.2. Программное обеспечение:

Интегрированная среда разработки ПО Microsoft Visual Studio (2019 Community).

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

Чтение лекций по темам предполагает разбор конкретных ситуаций в качестве примеров, подкрепляющих теоретический материал.

При проведении лабораторных занятий студентам (в отдельных случая – группам студентов) предлагается выполнение разнообразных творческих заданий по текущей теме.

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Материалы для проведения текущего и промежуточного контроля знаний студентов:

Для оценки достижений студентов в процессе изучения дисциплины; управления процессом приобретения студентами необходимых знаний, умений, навыков и формирования компетенций; оценки способностей студента к творческой деятельности, обеспечивающей решения новых задач; обеспечения соответствия результатов обучения задачам будущей профессиональной деятельности осуществляется поэтапный контроль степени освоения компетенций. В таблице приведены этапы освоения компетенций и виды оценочных средств, предназначенных для оценивания компетенций на разных стадиях обучения студентов.

№ п/п	Модуль, раздел (в соответствии с РП)	Контролируемые компетенции (или их части)	Вид оценочного средства
1	Раздел 1	ПК-3	Зачет по теме
2	Раздел 2	ПК-3	Зачет по теме
3	Раздел 3	ПК-3	Зачет по теме
4	Раздел 4	ПК-3	Тестирование
5	Раздел 5	ПК-3	Тестирование

Контроль качества освоения студентами дисциплины осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС). Индикатором сформированности компетенции является начисление студенту баллов за

выполнение задания семинаров, контрольных работ в виде теста, получения премиальных баллов и /или выполнения итогового теста.

Назначение оценочных средств текущего контроля – выявить сформированность компетенций (ПК-3).

Промежуточная аттестация проводится в форме защиты реферата. Студент допускается к итоговой аттестации - экзамену в том случае, если он защитит реферат, выполнит все семинарские задания и получит более 42 баллов, а также сдаст на положительную оценку контрольные работы в виде тестов. Если студент набрал необходимое количество баллов, предлагается итоговый тест – экзамен.

Темы рфератов:

1. Классификация систем моделирования информационной безопасности
2. Понятия «хорошей» и «плохой» моделях безопасности. Критерии определения.
3. Классификация субъекта и объекта в модели дискреционного доступа
4. Разрешающие и запрещающие операции обеспечения доступа к ресурсам в модели дискреционного доступа.
5. Математический аппарат формализации модели Ла-Падулла
6. Секретности информации. Меры и степени секретности в модели Ла-Падулла и их классификация.
7. Реализация уровней доступа к данным в формальных моделях безопасности.
8. Электронная почта. Применимость формальных моделей безопасности к управлению доступом к данным в почтовых протоколах.
9. Принципы и особенности реализации формальных моделей в операционных системах Linux.
10. Ролевые модели. Их особенности и применимость в различных ИС,
11. Математические принципы моделирования ролевых моделей.

Параметры оценочного средства

Предел длительности контроля	45 мин
Последовательность выборки вопросов из разделов (по всему курсу дисциплины)	случайная
Критерии оценки:	
«5», если	45 – 50 правильных ответов (добавляется 17 - 20 баллов в рейтинг студента)
«4», если	39 - 44 правильный ответ (добавляется 13 - 16 баллов в рейтинг студента)
«3», если	33 - 38 правильных ответов (добавляется 10 - 12 баллов в рейтинг студента)

Итоговый рейтинг студента формируется следующим образом:

№ п/п	Вид учебной деятельности	баллы	Максимально за 1 семестр
1.	Ведение конспекта лекций (за лекцию)	0.5	9
2	Выполнение семинарских заданий (см. перечень заданий в прил. 1)	2	28
3	Премиальные баллы за интерес к изучению курса (за семестр):	10	10

	Зачет в сессию	8	8

Разработчик:

доцент Глухов Н. И.

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

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «01» марта 2022 г. Протокол № 6

И.о.зав. кафедрой  Колесник С.Н.