



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники



Декан

Буднев Н.М.

«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.ДВ.05.01 Управление рисками
информационной безопасности**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

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 № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

**Рекомендовано кафедрой радиофизики и
радиоэлектроники:**

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

	стр.
1. Цели и задачи дисциплины (модуля)	3
2. Место дисциплины в структуре ОПОП.....	3
3. Требования к результатам освоения дисциплины (модуля)	4
4. Объем дисциплины (модуля) и виды учебной работы	5
5. Содержание дисциплины (модуля).....	5
5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются	6
5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами	6
5.3. Разделы и темы дисциплин (модулей) и виды занятий	7
6. Перечень семинарских, практических занятий и лабораторных работ	8
6.1. План самостоятельной работы студентов	8
6.2. Методические указания по организации самостоятельной работы студентов.....	9
7. Примерная тематика курсовых работ (проектов).....	9
8. Учебно-методическое и информационное обеспечение дисциплины (модуля):	9
а) основная литература.....	10
б) дополнительная литература.....	10
в) программное обеспечение	10
г) базы данных, информационно-справочные и поисковые системы	10
9. Материально-техническое обеспечение дисциплины (модуля)	10
10. Образовательные технологии.....	10
11. Оценочные средства (ОС):	11
11.1. Оценочные средства для входного контроля.....	12
11.2. Оценочные средства текущего контроля.....	12
11.3. Оценочные средства для промежуточной аттестации	12

Цели и задачи дисциплины:

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) **«Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»**, а также изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем управления информационной безопасностью и защитой информации

Задачи:

- направленность на многоуровневую систему образования и непрерывность профессионального развития;
- обеспечение обучающимися выбора индивидуальной образовательной траектории;
- 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;
 - определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Управление рисками информационной безопасности»: Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

«История», «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»,

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: «Комплексная система защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Государственная итоговая аттестация».

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций: ОК-7; ПК-8; ПК-10

ОК-7; способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности

В результате изучения дисциплины студент должен:

Знать: коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности

Уметь: использовать коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности

Владеть: навыками по применению коммуникаций в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в ; сфере профессиональной деятельности

ПК-8; способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

В результате изучения дисциплины студент должен:

Знать: рабочую техническую документацию с учетом действующих нормативных и методических документов

Уметь: использовать рабочую техническую документацию с учетом действующих нормативных и методических документов

Владеть: навыками по применению рабочей технической документации с учетом действующих нормативных и методических документов

ПК-10; способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

В результате изучения дисциплины студент должен:

Знать: рабочую техническую документацию по анализу информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Уметь: использовать рабочую техническую документацию по анализу информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Владеть: навыками по применению рабочей технической документации по анализу информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		7			
Аудиторные занятия (всего)	144/4	144/4			
В том числе:	-	-	-	-	-
Лекции	44/1,33	44/1,33			
Практические занятия (ПЗ)	22/0,61	22/0,61			
Семинары (С)					
Лабораторные работы (ЛР)					
КСР	12/0,33	12/0,33			
Самостоятельная работа (всего)	66/0,83	66/0,83			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
<i>Другие виды самостоятельной работы</i>					
Вид промежуточной аттестации (<i>зачет, экзамен</i>)	зачет	зачет			
Контактная работа (всего)					
Общая трудоемкость	часы	144	144		
	зачетные единицы	4	4		

5. Содержание дисциплины (модуля)

Раздел 1.

Тема1 Теоретические подходы к анализу информационных рисков

Понятие информационных рисков. Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия. /Лек/

Проработка лекционного материала Понятие информационных рисков. Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия. /Пр/

Тема2 Подготовка к практической работе по теме «Роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия» /Ср/

Методические подходы и инструментарий в оценке информационных рисков. /Лек/

Тема3 Аудит информационной безопасности /Лек/

Подготовка к семинарским занятиям; «Аудит информационной безопасности» /Ср/

Организация обеспечения информационной безопасности автоматизированных систем /Пр/

Тема4 Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем» /Ср/

Раздел 2.

Тема5 Управление комплексной системой защиты информации

Назначение, структура и содержание управления комплексной системой защиты информации /Лек/

Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации /Ср/

Тема6 Принципы и методы планирования комплексной системы защиты информации /Пр/

Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы защиты информации» /Ср/

Сущность и содержание контроля функционирования комплексной системы защиты информации /Лек/

Проработка лекционного материала «Сущность и содержание контроля функционирования комплексной системы защиты информации» /Ср/

Тема7 Общая характеристика подходов к оценке эффективности систем защиты информации /Пр/

Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/

Методы и модели оценки эффективности комплексной системы защиты информации /Лек/

Методы и модели оценки эффективности комплексной системы защиты информации /Ср/

Раздел 3. Контроль знаний

Подготовка к промежуточной аттестации (зачет)

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Техническая защита информации	1-7
2	Радиотехнические цепи и сигналы	1-7
3	Защита информации от несанкционированного доступа	1-7
4	Электроника и схемотехника	1-7
5	Операционные системы	1-7
6	Базы данных	1-7
7	Электротехника	1-7
8	Основы построения и функционирования специальных технических средств	1-7
9	Безопасность компьютерных сетей	1-7
10	Практика по получению первичных профессиональных умений и навыков	1-7
11	Эксплуатационная практика	1-7
12	Проектно-технологическая практика	1-7

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					Всего
			Лекц.	Практ. зан.	Семина	Лаб. зан.	СРС	
1.	Раздел 1	Тема 1	6	3			4	13
2.	Раздел 1	Тема 2	6	3			4	13
3.	Раздел 1	Тема 3	6	3			4	13
4.	Раздел 1	Тема 4	6	3			4	13
5.	Раздел 2	Тема 5	6	3			4	13
6.	Раздел 2	Тема 7	6	3			4	13
7.	Раздел 2	Тема 8	4	2			2	8
8.	Раздел 2	Тема 9	4	2			2	8

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	2	3	4	5	6
1.	<i>Раздел 1</i>	Практич. Занятие№1	2	Тестовый контроль по теме	ПК-7
2.	<i>Раздел 1</i>	Практич. Занятие№2	6	Тестовый контроль по теме	ПК-7
3.	<i>Раздел 2</i>	Практич. Занятие№3	2	Тестовый контроль по теме	ПК-8
4.	<i>Раздел 2</i>	Практич. Занятие№4	4	Тестовый контроль по теме	ПК-8
5.	<i>Раздел 2</i>	Практич. Занятие№5	4	Тестовый контроль по теме	ПК-10
6.	<i>Раздел 2</i>	Практич.№6	4	Тестовый контроль по теме	ПК-10

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	1-3	Подготовка к практич. работе №1	№1	Учебный сайт	36
8		Практическая работа №1.		Учебный сайт	
9		Подведение итогов по практич. работе №1. Работа над ошибками по контрольной работе №1.		Учебный сайт	
10-16	4-7	Подготовка итоговой экзаменационной работы	№2	Учебный сайт	30
17		Подготовка доклада с презентацией		Учебный сайт	

18		Подведение итогов		Учебный сайт	
----	--	-------------------	--	--------------	--

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Управление рисками информационной безопасности». Нормативные документы технической защиты информации», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Управление рисками информационной безопасности». направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1 Краковский Ю. М Информационная безопасность и защита информации: учебное пособие Иркутск: ИрГУПС, 2016 50

2. Прохорова О.В. Информационная безопасность и защита информации: Учебник [Электронный ресурс]

//biblioclub.ru/index.php?page=book&id=438331 Самара: СГА-СУ, 2014 100%

Онлайн

б) дополнительная литература

1. Нортон, П. Персональный компьютер [Текст]. Кн. 1. Аппаратно-программная организация ; Кн. 2. Модернизация и ремонт / П. Нортон, Дж. Гудман. - СПб. : BNY, 1999. - 848 ил
2. Попов, В. Б. Основы информационных и телекоммуникационных технологий [Текст] : учеб. пособие. Ч. 1. Программно-аппаратное обеспечение / В.Б. Попов. - М. : Финансы и статистика, 2005. - 144 с.

в) программное обеспечение

Система тестирования и анализа аппаратной платформы ЭВМ.

г) базы данных, информационно-справочные и поисковые системы

1. Учебный сайт Лаборатории ТЗИ Физического факультета ИГУ – Режим доступа: <https://sites.google.com/view/ltzi/>, свободный.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Управление рисками информационной безопасности», используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль (25 вариантов, 7-й семестр), представляет собой перечень из 10-15 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (10 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

11.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

Тестовые работы (10 комплектов по 3-5 вариантов). Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

доцент



Н.И.Глухов

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой



Колесник С.Н.

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.