МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Заместитель директора по
учебно-методической работе
_____ Т.А. Харитонова

« 23 » июня 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: Информационная безопасность и защита информации
направление подготовки: 38.03.05 Бизнес – информатика
направленность (профиль): Информационные системы предприятия
форма обучения: очная

Рабочая программа разработана для обучающихся по направлениям подготовки 38.03.05 Бизнес – информатика.

Рабочая программа рассмотрена
на заседании кафедры бизнес – информатики и математики

Заведующий кафедрой _____ О.М. Барбаков
(подпись)

Рабочую программу разработал:

Величко А.Н., ст. преподаватель _____
(подпись)

1. Цели и задачи освоения дисциплины

Цель дисциплины заключается в овладении теоретическими знаниями и умениями, развитии навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности в условиях существования внутренних и внешних угроз безопасности информации.

Задачи дисциплины:

– изучение нормативных правовых и организационных основ обеспечения информационной безопасности;

– формирование умений выявления и формулирования требований к обеспечению информационной безопасности;

– формирование умений планирования, реализации, и контроля процесса управления информационной безопасностью;

– формирование навыков проведения работ по обеспечению информационной безопасности.

– развитие исследовательских и аналитических навыков, интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам обязательной части учебного плана.

Необходимыми условиями для освоения дисциплины являются:

знание:

– теоретических основ информационных и сетевых технологий;

умение:

– разрабатывать алгоритмы и реализовывать их с использованием языков программирования;

владение:

– навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины служит основой для прохождения технологической (проектно-технологической) практики, подготовки к выполнению выпускной квалификационной работы.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
УК – 2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК – 2.1 Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	Знать (З1) основные понятия в области информационной безопасности; основы планирования информационной безопасности организации.
		Уметь (У1) осуществлять планирование процессов управления информационной безопасностью с учетом правовых и организационно-технических ограничений.
		Владеть (В1) практическими навыками планирования процесса управления информационной безопасностью предприятия.

ОПК - 3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК – 3.2 Выбирает оптимальные языки программирования и успешно организует работу с базами данных, операционными системами и оболочками, современными программными средами разработки информационных систем и технологий	Знать (З2) стандарты информационной безопасности; методики управления процессом информационной безопасности.
		Уметь (У2) выявлять требования и потребности в области информационной безопасности; управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью; оптимизировать процесс управления информационной безопасностью.
		Владеть (В2) навыками формирования и согласования с заинтересованными лицами целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ; организации процесса управления информационной безопасностью ресурсов ИТ, вовлечения и привлечения необходимых ресурсов; согласования (отклонения) ключевых решений по информационной безопасности ресурсов ИТ; контроля изменений процесса управления информационной безопасностью ресурсов ИТ; формирования системы оценки процесса управления информационной безопасностью ресурсов ИТ, оценки процесса и выполнения управленческих действий по результатам оценки.
	ОПК – 3.3 Эффективно использует языки программирования, современные программные среды разработки информационных систем и технологий для автоматизации бизнес – процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ	Знать (З3) основные положения законодательства РФ в области информационной безопасности; общие принципы и механизмы обеспечения информационной безопасности организации.
		Уметь (У3) осуществлять поддержку бизнес-процессов с использованием механизмов обеспечения информационной безопасности.
		Владеть (В3) практическими навыками внедрения правовых и организационно-технических механизмов обеспечения информационной безопасности, администрирования (использования) средств защиты информации (в т.ч. СКЗИ).
	ОПК – 3.4 Использует основные методы программирования, отладки и тестирования прототипов программно – технических комплексов задач	Знать (З4) требования к защите информации в платежных системах
		Уметь (У4) определять порядок обеспечения защиты информации в платежной системе
		Владеть (В4) практическими навыками обеспечения защиты информации в информационных системах

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетных единицы, 108 часов.

Таблица 4.1

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	3/6	16	-	32	33	27	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины:

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Общие положения информационной безопасности	2	-	4	5	11	УК – 2.1 ОПК – 3.2 ОПК – 3.3 ОПК – 3.4	Задание для выполнения лабораторной работы, вопросы для защиты
2	2	Разработка системы управления информационной безопасностью организации	6	-	12	12	30		Задание для выполнения лабораторной работы, вопросы для защиты
3	3	Внедрение и обеспечение функционирования системы управления информационной безопасностью организации	2	-	4	4	10		Задание для выполнения лабораторной работы, вопросы для защиты
4	4	Проведение мониторинга и анализа системы управления информационной безопасностью организации	2	-	4	4	10		Задание для выполнения лабораторной работы, вопросы для защиты
5	5	Поддержка и улучшение системы управления информационной безопасностью организации	2	-	4	4	10		Задание для выполнения лабораторной работы, вопросы для защиты
6	6	Управление рисками информационной безопасности в платежных системах	2	-	4	4	10		Задание для выполнения лабораторной работы, вопросы для защиты
7	Экзамен		-	-	-	27	27	УК – 2.1 ОПК – 3.2 ОПК – 3.3 ОПК – 3.4	Экзаменационные вопросы и задания
Итого:			16	-	32	60	108	X	X

заочная форма обучения (ЗФО)

не реализуется

очно-заочная форма обучения (ОЗФО)

не реализуется

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. «Общие положения информационной безопасности». Основные понятия в области информационной безопасности. Нормативно-правовые акты, специальные нормативные документы и документы национальной (международной) системы стандартизации в области информационной безопасности. Система органов обеспечения информационной безопасности в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.

Раздел 2. «Разработка системы управления информационной безопасностью организации». Область и границы действия системы управления информационной безопасностью. Методика оценки угроз безопасности информации. Уязвимости. Оценка и варианты обработки рисков информационной безопасности. Выбор целей и мер управления для обработки рисков информационной безопасности, утверждение остаточных рисков информационной безопасности.

Раздел 3. «Внедрение и обеспечение функционирования системы управления информационной безопасностью организации». Разработка и реализация плана обработки рисков информационной безопасности. Внедрение мер управления безопасностью информации. Организационно-технические аспекты обеспечения информационной безопасности. Управление работой и ресурсами системы управления информационной безопасностью. Обнаружение событий информационной безопасности и реагирование на инциденты.

Раздел 4. «Проведение мониторинга и анализа системы управления информационной безопасностью организации». Процедуры мониторинга и анализа результативности системы управления информационной безопасностью. Внутренний аудит системы управления информационной безопасностью. Регистрация действий и событий информационной безопасности.

Раздел 5. «Поддержка и улучшение системы управления информационной безопасностью организации». Выявление возможности улучшения системы управления информационной безопасностью. Корректирующие и предупреждающие действия. Внедрение улучшений.

Раздел 6. «Управление рисками информационной безопасности в платежных системах». Требования, предъявляемые к защите информации в платежных системах. Порядок обеспечения защиты информации в платежной системе с использованием правовых, организационных и технических мер.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1.	1.	2	-	-	Общие положения информационной безопасности
2.	2.	6	-	-	Разработка системы управления информационной безопасностью организации
3.	3.	2	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью организации
4.	4.	2	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью организации
5.	5.	2	-	-	Поддержка и улучшение системы управления информационной безопасностью организации
6.	6.	2	-	-	Управление рисками информационной безопасности в платежных системах

Итого:	16	-	-	X

Практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лабораторной работы
		ОФО	ЗФО	ОЗФО	
1.	1.	4	-	-	Общие положения информационной безопасности
2.	2.	12	-	-	Разработка системы управления информационной безопасностью организации
3.	3.	4	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью организации
4.	4.	4	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью организации
5.	5.	4	-	-	Поддержка и улучшение системы управления информационной безопасностью организации
6.	6.	4	-	-	Управление рисками информационной безопасности в платежных системах
Итого:		32	-	-	X

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1.	1.	5	-	-	Общие положения информационной безопасности	Изучение теоретического материала для выполнения лабораторной работы, оформление отчетов
2.	2.	12	-	-	Разработка системы управления информационной безопасностью организации	Изучение теоретического материала для выполнения лабораторной работы, оформление отчетов
3.	3.	4	-	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью организации	Изучение теоретического материала для выполнения лабораторной работы, оформление отчетов
4.	4.	4	-	-	Проведение мониторинга и анализа системы управления информационной безопасностью организации	Изучение теоретического материала для выполнения лабораторной работы, оформление отчетов
5.	5.	4	-	-	Поддержка и улучшение системы управления информационной безопасностью организации	Изучение теоретического материала для выполнения лабораторной работы, оформление отчетов
6.	6.	4	-	-	Управление рисками информационной безопасности в платежных системах	Изучение теоретического материала для выполнения лабораторной работы, оформление отчетов
7.	1 – 6.	27	-	-	Все темы	Подготовка к экзамену
Итого:		60	-	-	X	X

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- информационно-телекоммуникационная (визуализация учебного материала в PowerPoint в диалоговом режиме);
- обучение в сотрудничестве (коллективная, групповая работа);
- индивидуальная, рейтинговая;
- технология проблемного обучения.

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

- заочная форма обучения (ЗФО): не реализуется;
- очно-заочная форма обучения (ОЗФО): не реализуется.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1.	Лабораторная работа № 1	0 – 15
2.	Лабораторная работа № 2	0 – 15
	ИТОГО за первую текущую аттестацию	0 – 30
2 текущая аттестация		
3.	Лабораторная работа № 3	0 – 15
4.	Лабораторная работа № 4	0 – 15
	ИТОГО за вторую текущую аттестацию	0 – 30
3 текущая аттестация		
5.	Лабораторная работа № 5	0 – 20
6.	Лабораторная работа № 6	0 – 20
	ИТОГО за третью текущую аттестацию	0 – 40
	ВСЕГО	**0 – 100**

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

– Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/;

– Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/;

– Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru;

– Электронно-библиотечная система «Лань» https://e.lanbook.com;

– Образовательная платформа ЮРАЙТ www.urait.ru;

– Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru;

– Национальная электронная библиотека (НЭБ);

– ЭКБСОН – информационная система доступа к электронным каталогам библиотек сферы образования и науки;

– Библиотеки нефтяных вузов России:

- Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/;
- Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/;
- Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books;
- Электронная справочная система нормативно-технической документации «Технорматив».

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- Nessus;
- Nmap;
- Wireshark;
- John the Ripper;
- Snort;
- Secret Net Studio;
- VipNet;
- OpenVPN;
- КриптоПро;
- Arp monitor;
- Intercepter-NG;
- Zone Alarm;
- GNS3;
- Event Log Explorer;
- nFront Weak Password Scanner;
- Cisco Packet Tracer;
- BMMeter;
- CPU-Z;
- SiSoftWare Sandra;
- 10-Страйк: Сканирование Сети;
- Algorius Net Viewer.

10. Материально-техническое обеспечение дисциплины/модуля

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4

1.	Информационная безопасность и защита информации	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 2 шт., микрофон - 1 шт., документ-камера - 1 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70, ауд. 508.
		Лабораторные занятия: Учебная аудитория для проведения занятий практического типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. ПЭВМ - 16 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 2 шт., микрофон - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70, ауд. 510.

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным работам.

Лабораторные работы способствуют углублённому изучению дисциплины и служат основной формой подведения итогов самостоятельной работы студентов. Цель лабораторных работ заключается в углублении и закреплении теоретических знаний, а также в формировании практических компетенций, необходимых будущим специалистам.

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении лабораторных работ необходимо отрабатывать задания, учитывающие специфику будущих функциональных обязанностей обучающихся, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Студенту рекомендуется следующая схема подготовки к занятию:

- проработать конспект лекций;
- изучить рекомендованную литературу;
- при затруднениях сформулировать вопросы к преподавателю;
- после выполнения лабораторной работы оформить отчет и подготовиться к защите.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы

регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, подготовка мультимедиа-сообщений/докладов, подготовка реферата, тестирование, решение заданий по образцу, решение вариативных задач, выполнение чертежей, схем, расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и, собственно, конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию, поскольку в первые минуты лекции объявляется тема лекции, формулируется ее основная цель. Без этого дальнейшее восприятие лекции становится сложным. Важно научиться слушать преподавателя во время лекции. Здесь не следует путать такие понятия как слышать и слушать. Слушание лекции состоит из нескольких этапов, начиная от слышания (первый шаг в процессе осмысленного слушания) и заканчивая оценкой сказанного.

Чтобы процесс слушания стал более эффективным, нужно разделять качество общения с лектором, научиться поддерживать непрерывное внимание к выступающему. Для оптимизации процесса слушания следует:

1. Научиться выделять основные положения. Нельзя понять и запомнить все, что говорит выступающий, однако можно выделить основные моменты. Для этого необходимо обращать внимание на вводные слова, словосочетания, фразы, которые используются, как правило, для перехода к новым положениям, выводам и обобщениям;

2. Во время лекции осуществлять поэтапный анализ и обобщение, услышанного. Необходимо постоянно анализировать и обобщать положения, раскрываемые в речи говорящего. Стараясь представить материал обобщенно, мы готовим надежную базу для экономной, свернутой его записи. Делать это лучше всего по этапам, ориентируясь на момент логического завершения одного вопроса (подвопроса, тезиса и т.д.) и перехода к другому;

3. Готовность слушать выступление лектора до конца.

Слушание является лишь одним из элементов хорошего усвоения лекционного материала.

Поток информации, который сообщается во время лекции необходимо фиксировать, записывать – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции.

Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции

одну или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.

Главным отличием конспекта лекции от текста является свертывание текста. При ведении конспекта удаляются отдельные слова или части текста, которые не выражают значимую информацию, а развернутые обороты речи заменяют более лаконичными или же синонимичными словосочетаниями. При конспектировании основную информацию следует записывать подробно, а дополнительные и вспомогательные сведения, примеры – очень кратко. Особенно важные моменты лекции, на которые следует обратить особое внимание лектор, как правило, читает в замедленном темпе, что позволяет сделать их запись дословной. Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: **Информационная безопасность и защита информации**
Код, направление подготовки: **38.03.05 Бизнес – информатика**
Направленность (профиль): **Информационный системы предприятия**

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1 – 2	3	4	5
УК – 2	УК – 2.1 Проводит анализ поставленной цели и формулирует совокупность взаимосвязанных задач, которые необходимо решить для ее достижения	Знать (З1) основные понятия в области информационной безопасности; основы планирования информационной безопасности организации	Не знает основные понятия в области информационной безопасности; основы планирования информационной безопасности организации	Демонстрирует знание некоторых понятий в области информационной безопасности; отдельных аспектов планирования информационной безопасности организации	Демонстрирует достаточные знания об основных понятиях в области информационной безопасности; об основах планирования информационной безопасности организации	Демонстрирует исчерпывающие знания об основных понятиях в области информационной безопасности; об основах планирования информационной безопасности организации
		Уметь (У1) осуществлять планирование процессов управления информационной безопасностью с учетом правовых и организационно-технических ограничений	Не умеет осуществлять планирование процессов управления информационной безопасностью с учетом правовых и организационно-технических ограничений	Демонстрирует отдельные умения осуществлять планирование процессов управления информационной безопасностью с учетом правовых и организационно-технических ограничений	Демонстрирует достаточные умения осуществлять планирование процессов управления информационной безопасностью с учетом правовых и организационно-технических ограничений	Демонстрирует исчерпывающие умения осуществлять планирование процессов управления информационной безопасностью с учетом правовых и организационно-технических ограничений
		Владеть (В1) практическими навыками планирования процесса управления информационной безопасностью предприятия	Не владеет практическими навыками планирования процесса управления информационной безопасностью предприятия	Демонстрирует отдельные практические навыки планирования процесса управления информационной безопасностью предприятия	Демонстрирует достаточные практические навыки планирования процесса управления информационной безопасностью предприятия	Демонстрирует исчерпывающие практические навыки планирования процесса управления информационной безопасностью предприятия
ОПК – 3	ОПК – 3.2	Знать (З2)	Не знает	Демонстрируе	Демонстрируе	Демонстрируе

	Выбирает оптимальные языки программирования и успешно организует работу с базами данных, операционными системами и оболочками, современными программными средами разработки информационных систем и технологий	стандарты информационной безопасности; методики управления процессом информационной безопасности	стандарты информационной безопасности; методики управления процессом информационной безопасности	т знание некоторых стандартов информационной безопасности; методик управления процессом информационной безопасности	т достаточные знания стандартов информационной безопасности; методик управления процессом информационной безопасности	т исчерпывающие знания стандартов информационной безопасности; методик управления процессом информационной безопасности
		Уметь (У2) выявлять требования и потребности в области информационной безопасности; управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью; оптимизировать процесс управления информационной безопасностью	Не умеет выявлять требования и потребности в области информационной безопасности; управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью; оптимизировать процесс управления информационной безопасностью.	Демонстрирует отдельные умения выявлять требования и потребности в области информационной безопасности; управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью; оптимизировать процесс управления информационной безопасностью.	Демонстрирует достаточные умения выявлять требования и потребности в области информационной безопасности; управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью; оптимизировать процесс управления информационной безопасностью	Демонстрирует исчерпывающие умения выявлять требования и потребности в области информационной безопасности; управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью; оптимизировать процесс управления информационной безопасностью
		Владеть (У2) навыками формирования и согласования с заинтересованными лицами целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ; организации процесса управления информационной	Не владеет навыками формирования и согласования с заинтересованными лицами целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ; организации процесса управления информационной	Демонстрирует отдельные навыки формирования и согласования с заинтересованными лицами целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ; организации процесса управления информационн	Демонстрирует достаточные навыки формирования и согласования с заинтересованными лицами целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ; организации процесса управления информационн	Демонстрирует исчерпывающие навыки формирования и согласования с заинтересованными лицами целей, требований и приоритетов управления информационной безопасностью ресурсов ИТ; организации процесса управления

		безопасностью ресурсов ИТ, вовлечения и привлечения необходимых ресурсов; согласования (отклонения) ключевых решений по информационной безопасности ресурсов ИТ; контроля изменений процесса управления информационной безопасностью ресурсов ИТ; формирования системы оценки процесса управления информационной безопасностью ресурсов ИТ, оценки процесса и выполнения управленческих действий по результатам оценки	безопасностью ресурсов ИТ, вовлечения и привлечения необходимых ресурсов; согласования (отклонения) ключевых решений по информационной безопасности ресурсов ИТ; контроля изменений процесса управления информационной безопасностью ресурсов ИТ; формирования системы оценки процесса управления информационной безопасностью ресурсов ИТ, оценки процесса и выполнения управленческих действий по результатам оценки	ой безопасностью ресурсов ИТ, вовлечения и привлечения необходимых ресурсов; согласования (отклонения) ключевых решений по информационной безопасности ресурсов ИТ; контроля изменений процесса управления информационной безопасностью ресурсов ИТ; формирования системы оценки процесса управления информационной безопасностью ресурсов ИТ, оценки процесса и выполнения управленческих действий по результатам оценки	ой безопасностью ресурсов ИТ, вовлечения и привлечения необходимых ресурсов; согласования (отклонения) ключевых решений по информационной безопасности ресурсов ИТ; контроля изменений процесса управления информационной безопасностью ресурсов ИТ; формирования системы оценки процесса управления информационной безопасностью ресурсов ИТ, оценки процесса и выполнения управленческих действий по результатам оценки	информационной безопасностью ресурсов ИТ, вовлечения и привлечения необходимых ресурсов; согласования (отклонения) ключевых решений по информационной безопасности ресурсов ИТ; контроля изменений процесса управления информационной безопасностью ресурсов ИТ; формирования системы оценки процесса управления информационной безопасностью ресурсов ИТ, оценки процесса и выполнения управленческих действий по результатам оценки
	ОПК – 3.3 Эффективно использует языки программирования, современные программные среды разработки информационных систем и технологий для автоматизации бизнес – процессов, решения прикладных задач различных	Знать (З3) основные положения законодательства РФ в области информационной безопасности; общие принципы и механизмы обеспечения информационной безопасности организации	Не знает основные положения законодательства РФ в области информационной безопасности; общие принципы и механизмы обеспечения информационной безопасности организации	Демонстрирует знание некоторых основных положений законодательства РФ в области информационной безопасности; общих принципов и механизмов обеспечения информационной безопасности организации	Демонстрирует достаточные знания основных положений законодательства РФ в области информационной безопасности; общих принципов и механизмов обеспечения информационной безопасности организации	Демонстрирует исчерпывающие знания основных положений законодательства РФ в области информационной безопасности; общих принципов и механизмов обеспечения информационной безопасности организации
		Уметь (У3)	Не умеет	Демонстрируе	Демонстрируе	Демонстрируе

	классов, ведения баз данных и информационных хранилищ	осуществлять поддержку бизнес-процессов с использованием механизмов обеспечения информационной безопасности	осуществлять поддержку бизнес-процессов с использованием механизмов обеспечения информационной безопасности	т отдельные умения осуществлять поддержку бизнес-процессов с использованием механизмов обеспечения информационной безопасности	т достаточные умения осуществлять поддержку бизнес-процессов с использованием механизмов обеспечения информационной безопасности	т исчерпывающие умения осуществлять поддержку бизнес-процессов с использованием механизмов обеспечения информационной безопасности
		Владеть (В3) практическими навыками внедрения правовых и организационно-технических механизмов обеспечения информационной безопасности, администрирования (использования) средств защиты информации (в т.ч. СКЗИ)	Не владеет практическими навыками внедрения правовых и организационно-технических механизмов обеспечения информационной безопасности, администрирования (использования) средств защиты информации (в т.ч. СКЗИ)	Демонстрирует отдельные практические навыки внедрения правовых и организационно-технических механизмов обеспечения информационной безопасности, администрирования (использования) средств защиты информации (в т.ч. СКЗИ)	Демонстрирует достаточные практические навыки внедрения правовых и организационно-технических механизмов обеспечения информационной безопасности, администрирования (использования) средств защиты информации (в т.ч. СКЗИ)	Демонстрирует исчерпывающие практические навыки внедрения правовых и организационно-технических механизмов обеспечения информационной безопасности, администрирования (использования) средств защиты информации (в т.ч. СКЗИ)
	ОПК – 3.4 Использует основные методы программирования, отладки и тестирования прототипов программно–технических комплексов задач	Знать (З4) требования к защите информации в платежных системах	Не знает требования к защите информации в платежных системах	Демонстрирует знание некоторых требований к защите информации в платежных системах	Демонстрирует достаточные знания требований к защите информации в платежных системах	Демонстрирует исчерпывающие знания о требованиях к защите информации в платежных системах
		Уметь (У4) определять порядок обеспечения защиты информации в платежной системе	Не умеет определять порядок обеспечения защиты информации в платежной системе	Демонстрирует отдельные умения определять порядок обеспечения защиты информации в платежной системе	Демонстрирует достаточные умения определять порядок обеспечения защиты информации в платежной системе	Демонстрирует исчерпывающие умения определять порядок обеспечения защиты информации в платежной системе
		Владеть (В4) практическими навыками обеспечения защиты информации в	Не владеет практическими навыками обеспечения защиты информации в	Демонстрирует отдельные практические навыки обеспечения защиты	Демонстрирует достаточные практические навыки обеспечения защиты	Демонстрирует исчерпывающие практические навыки

		информационных система	информационных системах	информации в информационных системах	информации в информационных системах	обеспечения защиты информации в информационных системах

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: **Информационная безопасность и защита информации**
Код, направление подготовки: **38.03.05 Бизнес-информатика**
Направленность (профиль): **Информационный системы предприятия**

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Щеглов, Андрей Юрьевич. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2021. - 309 с. - (Бакалавр и магистр. Академический курс). - https://urait.ru/bcode/469866.	ЭР	30	100	+
2	Защита информации: учебное пособие для вузов / А. А. Внуков. - 3-е изд., пер. и доп. - Москва: Издательство Юрайт, 2021. - 161 с. - (Высшее образование). - ЭБС "Юрайт". https://urait.ru/bcode/4701311	ЭР	30	100	+
3	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020. - 312 с. - (Высшее образование). - ЭБС "Юрайт". – https://urait.ru/bcode/452368	ЭР	30	100	+
4	Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. - Санкт-Петербург : Лань, 2021. - 324 с. - https://e.lanbook.com/book/165837 .	ЭР	30	100	+
5	Информационная безопасность и защита информации: практикум / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. - Дубна: Государственный университет «Дубна», 2020. - 85 с. - ЭБС "Лань". https://e.lanbook.com/book/154490	ЭР	30	100	+
6	Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020. - 220 с. - (Высшее образование). - ЭБС "Юрайт". - https://urait.ru/bcode/452871	ЭР	30	100	+
7	Управление информационной безопасностью: Учебное пособие / А. К. Шилов. - Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. - 120 с. - http://www.iprbookshop.ru/87643.html	ЭР	30	100	+

8	Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Лань, 2019. - 344 с. - ЭБС Лань. - https://e.lanbook.com/book/125739	ЭР	30	100	+
9	Информационная безопасность и защита информации / В. Ф. Шаньгин. - Саратов: Профобразование, 2019. - 702 с. - ЭБС "IPR BOOKS" http://www.iprbookshop.ru/87995.html	ЭР	30	100	+
10	Основы информационной безопасности: учебное пособие / В. А. Галатенко. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Эр Медиа, 2020. - 266 с. http://www.iprbookshop.ru/97562.html	ЭР	30	100	+

ЭР – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/