ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 26.09.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.26 Управление информационной безопасностью
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 26.09.2021

А. Н. Соколов

Разработчик программы,
д.пед.н., проф., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Астахова Л. В.
Пользователь: astakhovalv
Дата подписания: 24.09.2021

Л. В. Астахова

Челябинск

1. Цели и задачи дисциплины

Дисциплина имеет целью изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии. Задачами дисциплины являются: - приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность; - формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

Краткое содержание дисциплины

Изучение дисциплины "Управление информационной безопасностью" является одной из завершающих стадий прикладной подготовки специалистов в области обеспечения информационной безопасности автоматизированных систем. Ее освоение должно обеспечить интеграцию полученных ранее знаний в области методов и средств защиты информации с материалами по правовым и организационно-управленческим аспектам информационной безопасности, способность обучаемых применить приобретенные умения и навыки в профессиональной деятельности.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать:основные угрозы безопасности информации и модели нарушителя в информационных системах (ПК-11); принципы формирования политики информационной безопасности в информационных системах (ПК-11, 21, 22);
	Уметь:определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите (ПК-11); разрабатывать модели угроз и нарушителей информационной безопасности информационных систем (ПК-11); разрабатывать частные политики информационной безопасности информационных систем (ПК-11, 22);
	Владеть:навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности (ПК-11)
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Знать:основные методы управления информационной безопасностью (ПК-28);
	Уметь:разрабатывать предложения по совершенствованию системы управления информационной безопасностью

	информационных систем (ПК-21, 28);
	Владеть:методами управления информационной безопасностью информационных систем (ПК-28);
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Знать:принципы формирования политики информационной безопасности в информационных системах (ПК-11, 21, 22);
	Уметь:разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем (ПК-21, 28);
	Владеть:
ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знать:отечественные и зарубежные стандарты в области информационной безопасности (ПК-12);
	Уметь:составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем (ПК-12); оценивать информационные риски в информационных системах (ПК-12);
	Владеть:навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности (ПК-11);
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Знать:принципы формирования политики информационной безопасности в информационных системах (ПК-11, 21, 22); критерии эффективности функционирования защищенных автоматизированных информационных систем (ПК-22);
	Уметь:разрабатывать частные политики информационной безопасности информационных систем (ПК-11, 22); контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем (ПК-22);
	Владеть:методами организации и управления деятельностью служб защиты информации на предприятии (ПК-22); навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем (ПК-22);

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.27 Безопасность сетей электронных вычислительных машин, В.1.02 Экономика и управление на предприятии, Б.1.32 Метрология, стандартизация и сертификация	Б.1.43 Аудит информационной безопасности

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.27 Безопасность сетей электронных вычислительных машин	Знать, уметь и владеть навыками обеспечения безопасности информационных систем и сетей
В.1.02 Экономика и управление на предприятии	Знать, уметь и владеть навыками управления организацией
Б.1.32 Метрология, стандартизация и сертификация	Знать основы стандартизации и сертификации в области информационной безопасности

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	80	80
МОДЕЛИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СВЯЗАННОЙ С ПЕРСОНАЛОМ ОРГАНИЗАЦИИ	80	80
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Базовые понятия и подходы к управлению информационной безопасностью	4	2	2	0
2	Международные и российские стандарты по УИБ	12	6	6	0
3	Политика ИБ организации	8	6	2	0
4	Система управления информационной безопасностью организации (СУИБ)	12	6	6	0
5	Ресурсное обеспечение СУИБ	12	6	6	0
6	Контроль и проверка процессов УИБ	12	6	6	0
7	Документационное обеспечение СУИБ	4	0	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Базовые понятия и подходы к управлению информационной безопасностью	2
2	2	Стандарты ИСО серии 27000	4
3	2	Отраслевые стандарты по ИБ	2
4	3	Политика ИБ организации	4
5	3	Организационные основы политики ИБ	2
6	4	Управление рисками ИБ	4
7	4	Управление инцидентами ИБ	2
8	5	Техническое обеспечение УИБ	2
9	5	Организационное и кадровое обеспечение СУИБ	4
10	6	Контроль и проверка процессов УИБ	4
11	6	Инструментальные средства проверки СУИБ	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Базовые понятия и подходы к управлению информационной безопасностью	2
2	2	Международные и российские стандарты по УИБ	6
3	3	Политика ИБ организации	2
4	4	Система управления информационной безопасностью организации (СУИБ)	6
5	5	Ресурсное обеспечение СУИБ	6
6	6	Контроль и проверка процессов УИБ	6
7	7	Документационное обеспечение СУИБ	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
МОДЕЛИРОВАНИЕ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СВЯЗАННОЙ С ПЕРСОНАЛОМ ОРГАНИЗАЦИИ	а) стандарты: 1. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Сист. емы менеджмента информационной безопасности. Общий обзор и терминология, ГОСТ Р от 15 ноября 2012 года №ИСО/МЭК 27000-2012. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 2. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и	80

	средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности, ГОСТ Р от 24 сентября 2012 года №ИСО/МЭК 27002-2012. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 4. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности, ГОСТ Р от 15 ноября 2012 года №ИСО/МЭК 27003-2012. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 5. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения, ГОСТ Р от 01 декабря 2011 года №ИСО/МЭК 27004-2011. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 6. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности, ГОСТ Р от 30 ноября 2010 года №ИСО/МЭК 27005-2010. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 7. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности, ГОСТ Р от 11 июня 2014 года №ИСО/МЭК 27007-2014. – URL: http://docs.cntd.ru (дата обращения: 10.01. 2020). 8. СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М., 2014. 9. СТО БР ИББС-1.1-2007. «Аудит информационной безопасности». 10. СТО БР ИББС-1.2-2014. Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.- 2014. – М., 2014. (4 редакция) 11. СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной	

	безопасности при осуществлении переводов денежных средств». 12. СТО БР ИББС-1.4-2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском информационной безопасности при аутсорсинге». 13. РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0». 14. РС БР ИББС-2.1-2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. 15. РС БР ИББС-2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. – М., 2009. – 23с. 16. РС БР ИББС-2.5-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности. 17. РС БР ИББС-2.6-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем». 18. РС БР ИББС-2.7-2015. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности. 19. РС БР ИББС-2.8-2015. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации. 20. РС БР ИББС-2.9-2016. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации. – М., 2016. - 25 с.	

	б)основная литература: 1. Николаев Н.С. Управление информационной безопасностью. Учебник. – М: Общество с ограниченной ответственностью "Издательство "КноРус", 2021. 190с. 2. Абденов, А. Ж. Современные системы управления информационной безопасностью : учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск : НГТУ, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118224 (дата обращения: 24.09.2021). — Режим доступа: для авториз. пользователей. 3. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : СКФУ, 2017. — 86 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155146 (дата обращения: 24.09.2021). — Режим доступа: для авториз. пользователей. Дополнительная литература: 1. Основы управления информационной безопасностью Текст учеб. пособие для вузов по направлениям (специальностям) 090000 "Информ. безопасность" / А. П. Курило и др. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2016. - 243 с. ил. 2. Милославская, Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью Текст учеб. пособие для вузов по направлению 090900 "Информ. безопасность" Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2016. - 165 с. ил. 3. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью Текст учеб. пособие для вузов по направлению 090900 "Информ. безопасность" (бакалавр/магистр) Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2016. - 214 с. ил. 4. Милославская, Н. Г. Управление рисками информационной безопасности Текст учеб. пособие для вузов по направлению 090900 "Информ. безопасность" (уровень	

	- магистр) Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2014. - 130 с. 5. Милославская, Н. Г. Управления инцидентами информационной безопасности и непрерывностью бизнеса Текст учеб. пособие для вузов по направлению 090900 "Информ. безопасность" (уровень - магистр) Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2014. - 168 с. ил. 6. Астахова Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2013. – Т. 13, № 1. – С. 79-83. 7. Астахова Л.В. Требования «мягкой силы» в управлении информационной безопасностью / Л.В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2016.№ 8. С. 9-12. 8. Астахова Л.В. УПРАВЛЕНЧЕСКАЯ КОМПЕТЕНЦИЯ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ: монография / Министерство образования и науки Российской Федерации, Южно-Уральский государственный университет. Челябинск, 2014. 99с. 9. Лукацкий А.В. Как оценить программу повышения осведомленности? – URL: http://lukatsky.blogspot.ru/2011/08/blog-post_19.html - (свободный, Загл. с экрана). 10. Прозоров А. Человеческий фактор в стандартах ИБ – URL: http://www.slideshare.net/AndreyProzorov/ss-27026263 (свободный, Загл. с экрана).	

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Инновационные технологии построения системы СУРИБ в организациях	Практические занятия и семинары	Моделирование системы СУРИБ	12
Интерактивные формы проведения занятий	Лекции		20
Активные и интерактивные формы проведения занятий	Практические занятия и семинары	Моделирование систем СУРИБ	12

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Проектное обучение	Использование теории управления проектами при моделировании подсистем СУИБ отдельной организации

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Базовые понятия и подходы к управлению информационной безопасностью	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Защита отчета по практической работе	Часть 1
Международные и российские стандарты по УИБ	ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Защита отчета по практической работе	Часть 2
Политика ИБ организации	ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Защита отчета по практической работе	Часть3
Система управления информационной безопасностью организации (СУИБ)	ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Защита отчета по практической работе	Часть 3
Ресурсное обеспечение СУИБ	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Защита отчета по практической работе	Часть 6
Контроль и проверка процессов УИБ	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Защита отчета по практической работе	Часть 7
Все разделы	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Письменный опрос или тест	1-7
Все разделы	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Экзамен	1-7
Все разделы	ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Посещаемость занятий	1-7

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Письменный опрос или тест	Письменный опрос осуществляется на последнем занятии изучаемого раздела. Студенту задаются 5 вопросов из списка контрольных вопросов. Время, отведенное на опрос -20 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Правильный ответ на вопрос соответствует 2 баллам. Частично правильный ответ соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов. Вместо письменного опроса может проводиться тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов – 10. Весовой коэффициент мероприятия (за каждый письменный опрос) – 0,05.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.
Защита отчета по практической работе	Защита практической работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, своевременность выполнения работы и ответы на вопросы (задаются 2-3 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Общий балл при оценке определяется на основе следующих показателей (за каждое практическое задание): - правильность оформления отчета, если отчет оформлен с недочетами из оценки вычитается 1 балл; - своевременность сдачи отчета, за каждую неделю просрочки отчета из оценки вычитается 0,5 балла; - ответы на вопросы, оценка снижается на 1 балл за каждый неправильный ответ на вопрос. Максимальное количество баллов за одну работу – 10. Весовой коэффициент мероприятия (за каждую работу) – 0,05.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %
Экзамен	На экзамене происходит оценивание	Отлично: 85…100 % Оценка «Отлично»

	учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Отлично: Величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: Величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 % Если рейтинг обучающегося по дисциплине ниже 60%, то он сдает экзамен с целью возможного повышения рейтинга. По результатам сдачи экзамена выставляется оценка, которая учитывается при определении рейтинга.	выставляется за ответ, который полностью раскрывает поставленный вопрос. Студент показывает глубокое знание вопросов темы, свободно оперирует терминами предметной области и легко отвечает на поставленные вопросы. Хорошо: 75…84 % Оценка «Хорошо» выставляется за ответ, который полностью соответствует поставленному вопросу. Ответ демонстрирует хорошее владение материалом и наличие навыков решения поставленных задач. Ответ содержит последовательное изложение материала с соответствующими выводами, однако, положения ответа не всегда достаточной степени обоснованы, а используемая терминология не всегда корректна. Удовлетворительно: 60…74 % Оценка «Удовлетворительно» выставляется за ответ, который не полностью соответствует поставленному вопросу, содержит незначительные пробелы в излагаемом материале. Студент в недостаточной степени владеет общепринятой терминологией, а также слабыми навыками решения прикладных задач. Неудовлетворительно: 0…59 % Оценка «Неудовлетворительно» выставляется за ответ, который не соответствует поставленному вопросу. Студент демонстрирует существенные пробелы в знаниях и недостаточный уровень навыков при решении практических задач. В ответе допускаются существенные ошибки.
Посещаемость занятий	Отмечается присутствие студента на занятиях. За каждое посещение прибавляется 0,4 балла. Максимальное количество баллов за 1-й семестр равно 25,6	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Письменный опрос или тест	УИБ_Тест_Часть 4.docx; УИБ_Тест_Часть 5.docx; УИБ_Тест_Часть 2.docx; УИБ_Тест_Часть1.docx; УИБ_Тест_Часть 3.docx; УИБ_Тест_Часть 6.docx; УИБ_Тест_Часть 7.docx
Защита отчета по практической работе	
Экзамен	1. Базовая терминология курса: система, системный подход, процесс,

	процессный подход, управление, циклическая модель улучшения процессов, системный подход к управлению организацией, процессный подход к управлению организацией. 2. Политика информационной безопасности. Базовые понятия, причины разработки. 3. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. Общая характеристика. 4. Политика информационной безопасности. Основные требования и принципы, содержание. 5. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC и ГОСТ Р ИСО/МЭК 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27000:2009 / ГОСТ Р ИСО/МЭК 27000-2012 – СУИБ: Общий обзор и терминология. 6. Политика информационной безопасности. Жизненный цикл. 7. Управление рисками ИБ. Составляющие процесса управления рисками ИБ. Системный подход к управлению рисками ИБ. 8. Политика информационной безопасности. Жизненный цикл, ответственность за исполнение. 9. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2013 – – СУИБ. Требования. 10. Управление рисками ИБ. Установление контекста управления рисками ИБ: базовые критерии принятия решений, область действия и границы, учет требований по обеспечению ИБ. 11. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27002:2013 и ГОСТ Р ИСО/МЭК 27002-2012 - СУИБ. Практические правила управления ИБ 12. Оценка рисков ИБ: этап анализа рисков. 13. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”.ISO/IEC 27003:2010 и ГОСТ Р ИСО/МЭК 27003-2012 – Руководство по внедрению СУИБ. 14. Управление и СУИБ. Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ как процесс. 15. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 – СУИБ. Измерение. 16. Оценка рисков ИБ: этап оценивания рисков. 17. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005-2010 – СУИБ. Управление рисками информационной безопасности. 18. Управление и СУИБ. Определение УИБ. Управление ИБ информационно-телекоммуникационных технологий. 19. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27007:2011 и ГОСТ Р ИСО/МЭК 27007-2014 – СУИБ. Руководство по аудиту СУИБ. 20. Подходы к оценке рисков ИБ. 21. Стандартизация систем и процессов управления информационной

	безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27008:2011 и ГОСТ Р 56045-2014/ИСО/ИЭК-ТР 8-2011 – СУИБ. Руководство для аудиторов по механизмам контроля СУИБ. 22. СУИБ организации. Область действия и документационное обеспечение. 23. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27011:2008 и ГОСТ Р ИСО/МЭК 27011-2012 – СУИБ. Руководство по СУИБ телекоммуникационных организаций на основе ИСО/МЭК 27002. 24. СУИБ организации. Политика СУИБ и ее поддержка со стороны руководства. 25. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27013:2012 и ГОСТ Р ИСО/МЭК 27013-2014 – СУИБ. Руководство по интегрированному внедрению ISO/IEC 20000-1 и ISO/IEC 27001. 26. Обработка рисков ИБ: снижение, сохранение, избежание, передача. 27. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27033-1:2009 и ГОСТ Р ИСО/МЭК 27033-1-2011 – Сетевая безопасность. Основные концепции управления. ISO/IEC 27033-3:2010 и ГОСТ Р ИСО/МЭК 27033-3-2014 – Сетевая безопасность. Базовые сетевые сценарии – угрозы, методы проектирования и механизмы контроля. 28. Принятие и коммуникация рисков ИБ. 29. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27034-1:2011 и ГОСТ Р ИСО/МЭК 27034-1-2014 – Обзор и основные концепции в области обеспечения безопасности приложений. 30. Процессный подход в рамках управления ИБ. Планирование, реализация, проверка и совершенствование СУИБ. 31. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27035-2011 и ГОСТ Р ИСО/МЭК ТО 18044 – Управление инцидентами безопасности. 32. Мониторинг и пересмотр показателей рисков ИБ. 33. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 “Информационные технологии. Методы обеспечения безопасности”. ISO/IEC 27037-2012 и ГОСТ Р ИСО/МЭК 27037-2014 – Руководство по идентификации, сбору, получению и обеспечению сохранности цифровых свидетельств. 34. Мониторинг, пересмотр и совершенствование процесса управления рисами ИБ. 35. Стандарты на отельные процессы управления ИБ и оценку безопасности ИТ. ISO/IEC 13335 – методы и средства обеспечения безопасности информационных технологий. 36. Подход к оценке рисков в стандартах Банка России. 37. Стандарты на отельные процессы управления ИБ и оценку безопасности ИТ. ISO/IEC 15408 и ISO/IEC 18045:2008 – общие критерии и методология оценки безопасности информационных технологий 38. Работа с процессами СУИБ организации. Задание, идентификация, документирование и описание, мониторинг и измерение параметров процесса СУИБ. 39. Стандарты на отельные процессы управления ИБ и оценку безопасности

	ИТ. ISO 19011:2011 и ГОСТ Р ИСО 19011-2003 – Рекомендации по аудиту систем менеджмента. 40. Документационное обеспечение управления рисками ИБ. 41. Стандарты на отельные процессы управления ИБ и оценку безопасности ИТ. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса. 42. Инструментальные средства управления рисками ИБ. 43. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации. СТО БР ИББС 1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения». 44. Кадровое обеспечение управления информационной безопасностью. 45. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации. СТО БР ИББС-1.1-2007 – Аудит ИБ. 46. Стратегии построения и внедрения СУИБ. Построение и внедрение СУИБ в целом и и процессов СУИБ по отдельности. 47. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации. СТО БР ИББС-1.2-2014– Методика оценки соответствия информационной безопасности организаций банковской системы Рроссийской Федерации. 48. Организационные аспекты управления информационной безопасностью. 49. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации. СТО БР ИББС-1.3-2016 – Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. 50. Автоматизация процессов управления ИБ в организации. 51. Проверка и оценка деятельности по управлению информационной безопасностью. 52. Использование новейших технологий в управлении ИБ организации. ВОПРОСЫ_УИБ.docx
Посещаемость занятий	

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"
2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн
3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"
4. Безопасность информационных технологий ,12+ ,М-во образования и науки Рос. Федерации, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ
5. Вестник УрФО : Безопасность в информационной сфере ,Юж.-Урал. гос. ун-т; ЮУрГУ

6. 6. Информационные ресурсы России
7. 7. Информационное общество
8. 8. Информационное право
9. 9. Информационные процессы и системы
10. 10. Информационные ресурсы России
11. 11. Кадровое дело
12. 12. Управление персоналом
13. 13. Управление риском

г) методические указания для студентов по освоению дисциплины:

1. Астахова Л.В._УИБ_Управление рисками ИБ_Методическое пособие
2. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безоасность"
3. УИБ_Лекционный материал

из них: учебно-методическое обеспечение самостоятельной работы студента:

4. Астахова Л.В._УИБ_Управление рисками ИБ_Методическое пособие
5. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безоасность"
6. УИБ_Лекционный материал

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 130 с. — Режим доступа: http://e.lanbook.com/book/5179 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 4. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 214 с. — Режим доступа: http://e.lanbook.com/book/5181 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Дополнительная литература	Курило, А.П. Основы управления информационной безопасностью. Серия	Электронно-библиотечная	Интернет / Авторизованный

		«Вопросы управление информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с. — Режим доступа: http://e.lanbook.com/book/5178 — Загл. с экрана.	система издательства Лань	
4	Дополнительная литература	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 5. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 166 с. — Режим доступа: http://e.lanbook.com/book/5182 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
5	Дополнительная литература	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3. [Электронный ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 170 с. — Режим доступа: http://e.lanbook.com/book/5180 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
6	Основная литература	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей. (Раздел управления рисками ИБ)	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
7	Основная литература	Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : СКФУ, 2017. — 86 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155146 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
8	Основная литература	Абденов, А. Ж. Современные системы управления информационной безопасностью : учебное пособие / А. Ж. Абденов, Г. А. Дронова, В. А. Трушин. — Новосибирск : НГТУ, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL:	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

		https://e.lanbook.com/book/118224 (дата обращения: 10.09.2021). — Режим доступа: для авториз. пользователей.		

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Project(бессрочно)
2. Microsoft-Windows(бессрочно)
3. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -База данных polpred (обзор СМИ)(бессрочно)
2. ООО "ГарантУралСервис"-Гарант(бессрочно)
3. -Стандартинформ(бессрочно)
4. -База данных ВИНИТИ РАН(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; MSAT; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.