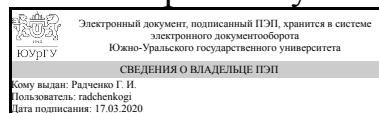


УТВЕРЖДАЮ:  
Директор института  
Высшая школа электроники и  
компьютерных наук



Г. И. Радченко

**РАБОЧАЯ ПРОГРАММА**  
**к ОП ВО от 26.06.2019 №084-2481**

**дисциплины Б.1.26 Управление информационной безопасностью**  
**для специальности 10.05.03 Информационная безопасность автоматизированных систем**

**уровень специалист тип программы Специалитет**

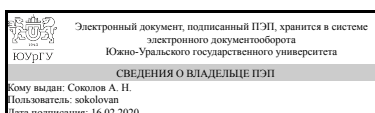
**специализация Информационная безопасность автоматизированных систем критически важных объектов**

**форма обучения очная**

**кафедра-разработчик Защита информации**

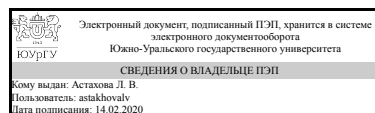
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

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



Л. В. Астахова

## 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-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-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-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);
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);

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

#### 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
<i>Аудиторные занятия:</i>	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	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	Международные и российские стандарты по УИБ	6
3	3	Политика ИБ организации	6
4	4	Система управления информационной безопасностью организации (СУИБ)	6
5	5	Ресурсное обеспечение СУИБ	6
6	6	Контроль и проверка процессов УИБ	6

## 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. Системы менеджмента информационной безопасности. Общий обзор и терминология, ГОСТ Р от 15 ноября 2012 года №ИСО/МЭК 27000-2012. – URL: <a href="http://docs.cntd.ru">http://docs.cntd.ru</a> (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: <a href="http://docs.cntd.ru">http://docs.cntd.ru</a> (дата обращения: 10.01. 2020). 3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности, ГОСТ Р от 24 сентября 2012 года №ИСО/МЭК 27002-2012. – URL: <a href="http://docs.cntd.ru">http://docs.cntd.ru</a> (дата обращения: 10.01. 2020). 4. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы	80

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 соответствии 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. 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. в) дополнительная литература: 21. Анисимов, А. А. Менеджмент в сфере информационной безопасности Текст учеб. пособие А. А. Анисимов. - М.: Интернет-Университет Информационных Технологий : БИНО, 2012 22. Астахова Л.В. Информационная безопасность: риски, связанные с культурным капиталом персонала/ Л.В. Астахова //Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2015.№ 4. С. 1-13. 23. Астахова Л.В. Когнитивно-информационная деятельность личности в обществе знания / Л.В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2016.№ 12. С. 1-6. 24. Астахова Л.В. Онтологический статус доверия в информационной безопасности / Л.В. Астахова // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2016.№ 3. С. 1-9. 25. Астахова Л.В. Понятие культуры информационной безопасности / Л.В. Астахова //Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2014.№ 2. С. 1-8. 26. 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. 27. 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. 28. Астахова, Л. В. ЮУрГУ Информационная безопасность: герменевтический подход. Избранные труды Российской школы по проблемам науки и технологий Текст монография Л. В. Астахова ; Рос. акад. наук и



	<p>др. - М.: Издательство РАН, 2010. - 185 с. ил.</p> <p>29. Большаков Н.В. Измерение культурного капитала: от теории к практике // Мониторинг общественного мнения: экономические и социальные перемены. – 2013. – № 6(118). – С. 3-12.</p> <p>30. Бурдые П. Формы капитала // Экономическая социология / пер. М.С. Добряковой; науч. редактив. В.В. Радаев. – 2005. – Т. 6, №3. – С. 60-74. – URL: <a href="http://gtmarket.ru/laboratory/expertize/2009/2601">http://gtmarket.ru/laboratory/expertize/2009/2601</a> (свободный, Загл. с экрана).</p> <p>31. Долгов К.М. Человеческий капитал и культура // Вестник МГИМО-университета. – 2013. – №3(30). – С.135-136.</p> <p>32. Космина Е.А., Метелев С.Е., Космин А.Д. Культурный капитал общества в реальном материале функционирующей организации. – М.: Экономика, 2007. – 386с.</p> <p>33. Лукацкий А.В. Как оценить программу повышения осведомленности? – URL: <a href="http://lukatsky.blogspot.ru/2011/08/blog-post_19.html">http://lukatsky.blogspot.ru/2011/08/blog-post_19.html</a> - (свободный, Загл. с экрана).</p> <p>34. Прозоров А. Человеческий фактор в стандартах ИБ – URL: <a href="http://www.slideshare.net/AndreyProzorov/ss-27026263">http://www.slideshare.net/AndreyProzorov/ss-27026263</a> (свободный, Загл. с экрана).</p> <p>35. Рытов М.Ю., Лексиков Е.В. Формализация процесса оценки лояльности персонала для снижения рисков информационной безопасности // Информация и безопасность. – 2014. – Т. 17, № 2. – С. 276-279.</p> <p>Тихомирова О.Г. Организационная культура: формирование, развитие и оценка. – СПб: Изд-во ИТМО, 2008. – 154с.</p>	
--	--	--

## 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 СУРИБ 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	Часть 3
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,	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.

	<p>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.</p> <p>Частично правильный ответ соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов.</p> <p>Вместо письменного опроса может проводиться тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос.</p> <p>Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов – 10. Весовой коэффициент мероприятия (за каждый письменный опрос) – 0,05.</p>	
Защита отчета по практической работе	<p>Защита практической работы осуществляется индивидуально.</p> <p>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.</p> <p>Максимальное количество баллов за одну работу – 10. Весовой коэффициент мероприятия (за каждую работу) – 0,05.</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %.</p> <p>Не зачтено: Рейтинг обучающегося за мероприятие менее 60 %</p>
Экзамен	<p>На экзамене происходит оценивание 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</p>	<p>Отлично: 85...100 % Оценка «Отлично» 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.</p>

	<p>дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179)</p> <p>Отлично: Величина рейтинга обучающегося по дисциплине 85...100 %</p> <p>Хорошо: Величина рейтинга обучающегося по дисциплине 75...84 %</p> <p>Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60...74 %</p> <p>Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0...59 %</p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p>
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 3.docx; УИБ_Тест_Часть 5.docx; УИБ_Тест_Часть 2.docx; УИБ_Тест_Часть 7.docx; УИБ_Тест_Часть 6.docx; УИБ_Тест_Часть1.docx; УИБ_Тест_Часть 4.docx
Защита отчета по практической работе	
Экзамен	<p>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.</p> <p>2. Политика информационной безопасности. Базовые понятия, причины разработки.</p> <p>3. Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 «Информационные</p>

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 рисками ИБ.

35. Стандарты на отдельные 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 отдельные 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 отдельные 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 отдельные 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

	<p>системы Российской Федерации. СТО БР ИББС 1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».</p> <p>44. Кадровое обеспечение управления информационной безопасностью.</p> <p>45. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации. СТО БР ИББС-1.1-2007 – Аудит ИБ.</p> <p>46. Стратегии построения и внедрения СУИБ. Построение и внедрение СУИБ в целом и и процессов СУИБ по отдельности.</p> <p>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 Российской Федерации.</p> <p>48. Организационные аспекты управления информационной безопасностью.</p> <p>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.</p> <p>50. Автоматизация процессов управления ИБ в организации.</p> <p>51. Проверка и оценка деятельности по управлению информационной безопасностью.</p> <p>52. Использование новейших технологий в управлении ИБ организации.</p> <p>ВОПРОСЫ_УИБ.docx</p>
Посещаемость занятий	

## 8. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

#### а) основная 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.

*б) дополнительная литература:*

1. Анисимов, А. А. Менеджмент в сфере информационной безопасности Текст учеб. пособие А. А. Анисимов. - М.: Интернет-Университет Информационных Технологий : БИНО, 2012
2. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах Текст учеб. пособие для вузов по специальностям 090102 - "Компьютер. безопасность" и 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем" Г. А. Остапенко. - М.: Горячая линия-Телеком, 2007
3. Бардаев, Э. А. Документоведение Текст учебник для вузов по направлению "Информ. безопасность" Э. А. Бардаев, В. Б. Кравченко. - 2-е изд., стер. - М.: Академия, 2010. - 300, [1] с. ил. 22 см.
4. Астахова, Л. В. ЮУрГУ Информационная безопасность : герменевтический подход. Избранные труды Российской школы по проблемам науки и технологий Текст монография Л. В. Астахова ; Рос. акад. наук и др. - М.: Издательство РАН, 2010. - 185 с. ил.
5. Астахова, Л. В. Управленческая компетенция специалиста по защите информации [Текст] монография Л. В. Астахова ; Юж.-Урал. гос. ун-т, Каф. Безопасность информ. систем ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 98, [1] с.

*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. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безопасность"
2. Астахова Л.В.\_УИБ\_Управление рисками ИБ\_Методическое пособие



3. Управление ИБ\_Лекционный материал
4. Управление ИБ\_Технические и организационные аспекты\_Лекционный материал.pptx

*из них: учебно-методическое обеспечение самостоятельной работы студента:*

5. Методические указания по курсу "Управление информационной безопасностью" для студентов направления "Информационная безопасность"
6. Астахова Л.В.\_УИБ\_Управление рисками ИБ\_Методическое пособие
7. Управление ИБ\_Лекционный материал
8. Управление ИБ\_Технические и организационные аспекты\_Лекционный материал.pptx

### Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Курило, А.П. Основы управления информационной безопасностью. Серия «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: <a href="http://e.lanbook.com/book/5178">http://e.lanbook.com/book/5178</a> — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Основная 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: <a href="http://e.lanbook.com/book/5179">http://e.lanbook.com/book/5179</a> — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Основная 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: <a href="http://e.lanbook.com/book/5180">http://e.lanbook.com/book/5180</a> — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
4	Основная литература	Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью». Выпуск 4. [Электронный	Электронно-библиотечная система	Интернет / Авторизованный

		ресурс] / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 214 с. — Режим доступа: <a href="http://e.lanbook.com/book/5181">http://e.lanbook.com/book/5181</a> — Загл. с экрана.	издательства Лань	
5	Основная 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: <a href="http://e.lanbook.com/book/5182">http://e.lanbook.com/book/5182</a> — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
6	Дополнительная литература	Петренко, С.А. Управление информационными рисками. Экономически оправданная безопасность. [Электронный ресурс] / С.А. Петренко, С.В. Симонов. — Электрон. дан. — М. : ДМК Пресс, 2009. — 394 с. — Режим доступа: <a href="http://e.lanbook.com/book/40021">http://e.lanbook.com/book/40021</a> — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

## 9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

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

Перечень используемых информационных справочных систем:

1. -Стандартинформ(бессрочно)
2. -База данных rolrged (обзор СМИ)(бессрочно)
3. -База данных ВИНТИ РАН(бессрочно)

## 10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лабораторные занятия	913 (36)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Лекции	912 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт. ), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+.
Практические	913	Комплект компьютерного оборудования; Локальная вычислительная сеть;

занятия и семинары	(36)	Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
--------------------	------	---