

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

**УТВЕРЖДЕНО**  
решением Ученого совета факультета математики,  
информационных и авиационных технологий

от «21» 06 2018 г., протокол № 5/18  
Председатель М.А. Волков  
(подпись, расшифровка подписи)  
«21» 06 2018 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Гуманитарные аспекты информационной безопасности
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	2

Специальность: 10.05.01 "Компьютерная безопасность"  
*код направления (специальности), полное наименование*

Специализация: "Математические методы защиты информации"  
*полное наименование*

Форма обучения: очная  
*очная, заочная, очно-заочная (указать только те, которые реализуются)*

Дата введения в учебный процесс УлГУ: « 01 » 09 2018 г.

Программа актуализирована на заседании кафедры: протокол №     от     20 г.

Программа актуализирована на заседании кафедры: протокол №     от     20 г.

Программа актуализирована на заседании кафедры: протокол №     от     20 г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
<u>   </u> / <u>   </u> / Андреев А.С. / <i>(подпись) (Ф.И.О.)</i>	<u>   </u> / <u>   </u> / Андреев А.С. / <i>(подпись) (Ф.И.О.)</i>
« <u>15</u> » <u>06</u> 20 <u>18</u> г.	« <u>15</u> » <u>06</u> 20 <u>18</u> г.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### Цели освоения дисциплины:

учебная дисциплина «Гуманитарные аспекты информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом.

Основной целью курса является изучение:

гуманитарных аспектов информационной информации;  
методов и средств управления информационной безопасностью (ИБ), основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) типового предприятия.

### Задачи освоения дисциплины:

- уяснение места и роли проблем информационной безопасности в становлении современного информационного общества в процессе обеспечения военной, экономической, экологической и иных видов национальной безопасности;
- формирование требований к системе управления ИБ конкретного объекта;
- проектирование системы управления ИБ конкретного объекта;
- использование нормативных правовых документов в своей профессиональной деятельности.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина "Гуманитарные аспекты информационной безопасности" изучается в 4 семестре и относится к обязательным дисциплинам вариативной части Б1.В, предназначенным для студентов, обучающихся по специальности – «Компьютерная безопасность».

Для успешного освоения дисциплины студент должен овладеть общекультурными и профессиональными компетенциями, формируемыми при изучении дисциплин «Информатика» и «Основы социологии».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

- знание базовых профессиональных понятий и определений в области информатики и социологии;
- способность использовать нормативные правовые документы;
- способность использовать основные положения социальных и гуманитарных наук;
- способность анализировать социально-значимые проблемы и процессы.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: «Основы информационной безопасности», «Организационные и правовые основы информационной безопасности», «Техническая защита информации», «Защита программ и данных», «Профессиональная этика».

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

### 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
1	2
ОК-5 – способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	<p><b>Знать:</b> проблемы ИБ и основные мероприятия профессиональной деятельности в области обеспечения ИБ и защиты интересов личности, общества и государства</p> <p><b>Уметь:</b> обеспечивать требуемый уровень ИБ и защиты интересов личности, общества и государства</p> <p><b>Владеть:</b> навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности системы управления ИБ (СУИБ)</p>
ОПК-5 - способность использовать нормативные правовые акты в своей профессиональной деятельности	<p><b>Знать:</b> место и роль проблем ИБ в современном информационном обществе; основные стандарты, регламентирующие управление ИБ; принципы разработки процессов управления ИБ</p> <p><b>Уметь:</b> анализировать текущее состояние ИБ в организации с целью разработки требований к процессам управления ИБ; определять цели и задачи, решаемые процессами управления ИБ; применять процессный подход к управлению ИБ в различных сферах деятельности. Использовать нормативные правовые акты в профессиональной деятельности.</p> <p><b>Владеть:</b> терминологией и процессным подходом построения систем управления ИБ; навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ</p>
ПК-1 - способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности	<p><b>Знать:</b> принципы подбора, изучения и обобщения научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности</p> <p><b>Уметь:</b> осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности</p> <p><b>Владеть:</b> навыками подбора, изучения и обобщения научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

1	2
ПК-13 - способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности	<p><b>Знать:</b> принципы организации работы малых коллективов исполнителей</p> <p><b>Уметь:</b> организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p> <p><b>Владеть:</b> навыками организации работы малых коллективов исполнителей, нахождения и принятия управленческих решений в сфере профессиональной деятельности</p>

#### 4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

##### 4.1. Объем дисциплины в зачетных единицах (всего) 2.

##### 4.2 Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	Количество часов (форма обучения <u>дневная</u> )			
	Всего по плану	В т.ч. по семестрам		
		4 семестр		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	36	36/36		
Аудиторные занятия:	36	36/36		
Лекции	36	36/36		
Практические и семинарские занятия				
Лабораторные работы (лабораторный практикум)				
Самостоятельная работа	36	36		
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на лекциях; - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	Зачёт	Зачёт		
Всего часов по дисциплине	72	72		

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

### 4.3. Содержание дисциплины. распределение часов по темам и видам учебной работы:

Форма обучения дневная

Название разделов и тем	Все го	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		лекции	Практич. занятия, семинары	Лабораторные работы			
<b>Раздел 1. Гуманитарная сущность информационной безопасности</b>							
1. Введение в дисциплину «Гуманитарные аспекты информационной безопасности (ИБ)»	4	2				2	Тесты Т1, реф. 1, 2
2. ИБ как гуманитарная проблема	4	2				2	Тесты Т2, реф. 3, 4
3. Проблемы реализации гуманитарной сущности ИБ	4	2				2	Тесты Т3, реф. 5, 7
4. Культура ИБ	4	2				2	Тесты Т4, реф. 8
<b>Раздел 2. Управление информационной безопасностью</b>							
5. Стандарты информационной безопасности	4	2				2	Тесты Т5, реф. 6
6. Система управления информационной безопасностью	8	4				4	Тесты Т6, реф. 9
7. Анализ рисков ИБ предприятия	4	2				2	Тесты Т7, реф. 10
8. Система управления инцидентами ИБ	8	4			2	4	Тесты Т8, реф. 11
9. Политика информационной безопасности предприятия	4	2			2	2	Тесты Т9, реф. 12
10. План защиты информационных ресурсов от несанкционированного доступа	8	4			2	4	Тесты Т10, реф. 13
11. План обеспечения непрерывной работы и восстановления работоспособности информационной системы	8	4			2	4	Тесты Т11, реф. 14
12. Эксплуатация и независимый аудит системы управления ИБ	8	4			2	4	Тесты Т12, реф. 15
13. Формирования требований к системе защиты инф. информационной системы	4	2			2	2	Тесты Т13, реф. 16
Итого:	72	36			12	36	

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Раздел 1. Гуманитарная сущность информационной безопасности

#### Тема 1. Введение в дисциплину «Гуманитарные аспекты информационной безопасности».

Предмет и задачи курса. Понятие информационной безопасности. Важность и актуальность дисциплины «Гуманитарные аспекты информационной безопасности». Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Составляющие проблемы информационной безопасности: защита информации и защита от информации. Понятийный аппарат гуманитарных аспектов информационной информации.

#### Тема 2. Информационная безопасность как гуманитарная проблема.

Место и роль проблем информационной безопасности в становлении современного информационного общества в процессе обеспечения военной, экономической, экологической и иных видов национальной безопасности. Гуманитарная сущность информационной безопасности.

#### Тема 3. Проблемы реализации гуманитарной сущности информационной безопасности.

Стадии формирования информационной безопасности как отрасли деятельности. Структурные преобразования ИБ (институционализация, профессионализация, технологизация и социализация). Нацеленность на человека и его потребности, гуманитарный характер методов и средств, реализованных в процессе структурных преобразований ИБ.

#### Тема 4. Культура информационной безопасности.

Формирование информационной культуры современного общества и связанное с этим обеспечение культуры информационной безопасности - ключевая гуманитарная проблема. Этика в сфере информационных технологий. Основные элементы глобальной культуры кибербезопасности. Всеобуч в области культуры информационной безопасности.

### Раздел 2. Управление информационной безопасностью

#### Тема 5. Стандарты информационной безопасности.

Роль стандартов информационной безопасности для решения проблемы ИБ. Международные стандарты информационной безопасности. Управление информационной безопасностью. Общие критерии безопасности информационных технологий. Основные отечественные стандарты безопасности информационных технологий.

#### Тема 6. Система управления информационной безопасностью.

Система управления информационной безопасности организации (СУИБ). Основные функции и компоненты СУИБ организации. Область действия СУИБ. Документальное обеспечение СУИБ. Состав документации СУИБ. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СУИБ (СМИБ) организации. Основные этапы создания СУИБ (инвентаризация и категорирование активов; оценка защищенности информационной системы; оценка и обработка информационных рисков; контроль выполнения и эффективности выбранных мер).

#### Тема 7. Управление рисками информационной безопасности предприятия.

Основные понятия управления рисками. Термины и определения. Основные этапы управления рисками (выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий; выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска).

#### Тема 8. Система управления инцидентами информационной безопасности.

Нормативная база управления инцидентами информационной безопасности (ИБ). Понятие события и инцидента ИБ. Цели и задачи управления инцидентами ИБ. Система управления инцидентами ИБ. Этапы процесса управления инцидентами ИБ. Политика управления инцидентами ИБ. Обеспечение осведомленности и обучение в области инцидентов ИБ.

#### Тема 9. Политика информационной безопасности предприятия.

Основные понятия политики информационной безопасности (ПИБ) организации. Содержание ПИБ организации. Область применения ПИБ. Понятие ПИБ «в широком» и «в узком» смыслах. «Частные» ПИБ. Стратегии действий на нарушения безопасности.

#### Тема 10. План защиты информационных ресурсов от несанкционированного доступа.

Назначение и основные положения Плана защиты информационных ресурсов от НСД. Обязанности руководителя и сотрудников ОИБ по предупреждению, реагированию и ликвидации последствий нарушений безопасности. Распределение обязанностей между администраторами ИС. Требования безопасности, предъявляемые к пользователям ИС. Основные мероприятия, формаль-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

ные процедуры и другие технологические процессы по обеспечению ИБ. Выявление попыток НСД. Реагирование на нарушения информационной безопасности. Ликвидация последствий НСД.

**Тема 11.** План обеспечения непрерывной работы и восстановления работоспособности информационной системы.

Понятие управления непрерывности бизнеса. Процесс управление непрерывностью бизнеса (УНБ). Система управления непрерывностью бизнеса (СУНБ). Ключевые компоненты СУНБ. Внедрение управления непрерывностью бизнеса в культуру организации. Программа непрерывного образования и информирования об УНБ. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса. Примерное содержание плана обеспечения непрерывности бизнеса. План восстановления бизнеса.

**Тема 12.** Эксплуатация и независимый аудит системы управления информационной безопасностью.

Понятие аудита безопасности (системы управления информационной безопасностью) и цели его проведения. Виды аудита. Основные принципы аудита информационной безопасности (ИБ). Критерии аудита ИБ. Этапы проведения аудита ИБ. Результаты аудита ИБ.

**Тема 13.** Формирования требований к системам защиты информации (СЗИ).

Общие требования к СЗИ. Организационные требования. Требования к подсистемам СЗИ. Требования к техническому и программному обеспечению.

## 6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом дисциплины.

## 7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторные работы не предусмотрены учебным планом дисциплины.

## 8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисциплины.

8.2. Примерная тематика рефератов:

1. Стратегия национальной безопасности Российской Федерации о месте и роли информационной безопасности.
2. Доктрина информационной безопасности Российской Федерации о гуманитарных проблемах информационной безопасности.
3. Информационная безопасность как гуманитарная проблема.
4. Обеспечение национальной и международной безопасности – приоритетные проблемы развития цивилизации в XXI веке.
5. Информационная безопасность: герменевтический подход.
6. Основные стандарты информационной безопасности
7. Гуманитарная сущность информационной безопасности
8. Культура информационной безопасности
9. Система управления информационной безопасностью
10. Анализ рисков информационной безопасности
11. Система управления инцидентами информационной безопасности
12. Политика информационной безопасности предприятия
13. План защиты информационных ресурсов от несанкционированного доступа
14. План обеспечения непрерывной работы и восстановления работоспособности информационной системы
15. Аудит системы управления информационной безопасности
16. Формирования требований к системе защиты информации информационной системы

8.2.1 Правила оформления рефератов

Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. [URL:ftp://10.2.5.225/FullText/Text/Andreev\\_2017.pdf](ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf).

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЁТУ

1. Гуманитарная сущность безопасности. Основные нормативно-правовых акты России по вопросам безопасности.
2. Гуманитарная сущность информации. Технократический и гуманитарный подходы к информации.
3. Гуманитарная сущность информационной безопасности (ИБ).
4. Место и роль проблем ИБ в становлении современного информационного общества.
5. Системный кризис цивилизации и его гуманитарные причины.
6. Нравственные приоритеты молодого поколения и будущее России как один из аспектов проблемы информационной безопасности.
7. Стадии формирования информационной безопасности (ИБ). Профессионализация отрасли ИБ.
8. Стадии формирования информационной безопасности (ИБ). Технологизация отрасли ИБ.
9. Стадии формирования информационной безопасности (ИБ). Социализация отрасли ИБ.
10. Формирование информационной культуры общества. Этика в сфере информационных технологий.
11. Основные элементы глобальная культуры кибербезопасности.
12. Всеобуч в области культуры информационной безопасности.
13. Международные и отечественные стандарты информационной безопасности.
14. Система управления информационной безопасности организации.
15. Основные функции и компоненты системы управления ИБ организации.
16. Область действия системы управления ИБ организации.
17. Документальное обеспечение системы управления ИБ организации.
18. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения системы управления ИБ организации.
19. Основные этапы создания СУИБ (инвентаризация и категорирование активов; оценка защищенности информационной системы; оценка и обработка информационных рисков; контроль выполнения и эффективности выбранных мер).
21. Основные понятия управления рисками. Термины и определения.
22. Основные этапы управления рисками (выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий; выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска).
23. Нормативная база управления инцидентами ИБ. Понятие события и инцидента ИБ. Цели и задачи управления инцидентами ИБ.
24. Система управления инцидентами ИБ.
25. Этапы процесса управления инцидентами ИБ.
26. Политика управления инцидентами ИБ.
27. Обеспечение осведомленности и обучение в области инцидентов ИБ.
28. Политика информационной безопасности (ПИБ) предприятия. Содержание ПИБ.
29. Область применения Политики информационной безопасности (ПИБ). Понятие ПИБ «в широком» и «в узком» смыслах. «Частные» ПИБ.
30. Обязанности руководителя и сотрудников отдела информационной безопасности по предупреждению, реагированию и ликвидации последствий нарушений безопасности.
31. Требования безопасности, предъявляемые к пользователям информационной системы.
32. Основные мероприятия, формальные процедуры и другие технологические процессы по обеспечению информационной безопасности.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

33. Система управления непрерывностью бизнеса (СУНБ).  
34. Внедрение управления непрерывностью бизнеса в культуру организации. Программа непрерывного образования и информирования об управлении непрерывностью бизнеса.  
35. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса. Примерное содержание плана обеспечения непрерывности бизнеса.  
36. Методология проверки и оценки состояния информационной безопасности.  
37. Аудиты информационной безопасности на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ.  
38. Общие требования к системе защиты информации. Требования к подсистемам системы защиты информации.

## 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Гуманитарная сущность информационной безопасности Тема 1. Введение в дисциплину «Гуманитарные аспекты информационной безопасности»	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, зачет
Раздел 1. Тема 2. Информационная безопасность как гуманитарная проблема	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, зачет
Раздел 1. Тема 3. Проблемы реализации гуманитарной сущности информационной безопасности	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, зачет
Раздел 1. Тема 4. Культура информационной безопасности	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, зачет
Раздел 2. Управление информационной безопасностью Тема 5. Стандарты информационной безопасности	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, зачет
Раздел 2. Тема 6. Система управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятием, зачет
Раздел 2. Тема 7. Анализ рисков информационной безопасности предприятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятием, зачет

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

1	2	3	4
Раздел 2. Тема 8. Основные механизмы обеспечения ИБ Система управления инцидентами ИБ	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты накануне перед занятием, зачет
Раздел 2. Тема 9. Политика информационной безопасности предприятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты накануне перед занятием, зачет
Раздел 2. Тема 10. План защиты информационных ресурсов от несанкционированного доступа	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты накануне перед занятием, зачет
Раздел 2. Тема 11. План обеспечения непрерывной работы и восстановления работоспособности информационной системы	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты накануне перед занятием, зачет
Раздел 2. Тема 12. Эксплуатация и независимый аудит системы управления ИБ	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты накануне перед занятием, зачет
Раздел 2. Тема 13. Формирования требований к системе защиты информации информационной системы	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты накануне перед занятием, зачет

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы:

#### основная

1. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М.: Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991204811.html>.

2. Малюк А.А., Теория защиты информации [Электронный ресурс] / Малюк А.А. - М.: Горячая линия - Телеком, 2012. - 184 с. - ISBN 978-5-9912-0246-6 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991202466.html>.

#### дополнительная

1. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:

1.1 ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь. — Режим доступа: <https://gostexpert.ru/gost/gost-9000-2001>

1.2 ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. — Режим доступа: <https://gostexpert.ru/gost/gost-27001-2006>

1.3 ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

сти». - М.: Стандартинформ, 2009. — Режим доступа: <https://gostexpert.ru/gost/gost-18044-2007>

1.4 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. — Режим доступа: <https://gostexpert.ru/gost/gost-27002-2012>

1.5. ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство». М.: Стандартинформ, 2011. — Режим доступа: <https://gostexpert.ru/gost/gost-53647.1-2009>

1.6 ГОСТ Р 53647.2-2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования». М.: Стандартинформ, 2011. — Режим доступа: <https://gostexpert.ru/gost/gost-53647.2-2009>

1.7 ГОСТ Р 53647.3-2010 «Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению». М.: Стандартинформ, 2011. — Режим доступа: <https://gostexpert.ru/gost/gost-53647.3-2010>

2. Дронов В.Ю., Международные и отечественные стандарты по информационной безопасности [Электронный ресурс]: Дронов В.Ю. - Новосибирск: Изд-во НГТУ, 2016. - 34 с. - ISBN 978-5-7782-3112-2 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785778231122.html>.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191/](http://www.consultant.ru/document/cons_doc_LAW_208191/)

3.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_191669/](http://www.consultant.ru/document/cons_doc_LAW_191669/)

#### учебно-методическая

1. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: <http://edu.ulsu.ru/courses/750/interface/>.

#### 2. Иванцов А. М.

Методические указания для самостоятельной работы студентов по дисциплине «Гуманитарные аспекты информационной безопасности» для студентов специалитета по специальности 10.05.01 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 387 КБ). - Текст: электронный. <http://lib.ulsu.ru/MegaPro/Download/MObject/4964>

Согласовано: Г. Сиб-рв УлГУ ИБ, Домнина И.И. ФУ, 14.06.2019  
 Должность сотрудника научной библиотеки ФИО подпись дата

#### б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

#### в) Профессиональные базы данных, информационно-справочные системы

##### 1. Электронно-библиотечные системы:

- 1.1. IPRbooks [Электронный ресурс]: электронно-библиотечная система / группа

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: <http://www.iprbookshop.ru>.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://www.biblio-online.ru>.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://www.studentlibrary.ru/pages/catalogue.html>.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: <https://e.lanbook.com>.

1.5. **Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://znanium.com>.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс]: электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: <https://dlib.eastview.com/browse/udb/12>.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://нэб.рф>.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://dvs.rsl.ru>.

#### 6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: <http://window.edu.ru>

6.2. Федеральный портал Российское образование. Режим доступа: <http://www.edu.ru>

#### 7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : <http://lib.ulsu.ru/MegaPro/Web>

7.2. Образовательный портал УлГУ. Режим доступа : <http://edu.ulsu.ru>

8. **ГОСТ-Эксперт** - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИиТ  
Должность сотрудника УИиТ

/Клочкова А.В.  
ФИО

 14.06.2019  
подпись дата

## 12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций: 3/317, 2/246.

Аудитория 2/246 укомплектована специализированной мебелью, учебной доской, имеются мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

## 13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающимся) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических возможностей:

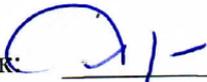
Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф-Рабочая программа по дисциплине		

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик:  \_\_\_\_\_ Иванцов Андрей Михайлович  
подпись должность ФИО

## ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/вы- пускающей кафедрой	Подпись	Дата
1	Внесение изменений в п.п. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
2	Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
3	Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14
4	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14

## 4.2 Объем дисциплины по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения <u>дневная</u> )			
	Всего по плану	В т.ч. по семестрам		
		4 семестр		
1	2	3	4	5
Контактная работа обучающихся с преподавателем	36	36/36*		
Аудиторные занятия:	36	36/36*		
Лекции	36	36/36*		
Практические и семинарские занятия				
Лабораторные работы (лабораторный практикум)				
Самостоятельная работа	36	36		
Форма текущего контроля знаний и контроля самостоятельной работы: Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		-Тестирование на лекциях; - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	Зачёт	Зачёт		
Всего часов по дисциплине	72	72		

\*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

### **13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ**

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### а) Список рекомендуемой литературы:

#### основная

1. Малюк А.А., Защита информации в информационном обществе [Электронный ресурс]: Учебное пособие для вузов. / А.А. Малюк - М.: Горячая линия - Телеком, 2015. - 230 с. - ISBN 978-5-9912-0481-1 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991204811.html>.

2. Малюк А.А., Теория защиты информации [Электронный ресурс] / Малюк А.А. - М.: Горячая линия - Телеком, 2012. - 184 с. - ISBN 978-5-9912-0246-6 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991202466.html>.

#### дополнительная

1. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:

1.1 ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь. — Режим доступа: <https://gostexpert.ru/gost/gost-9000-2001>

1.2 ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. — Режим доступа: <https://gostexpert.ru/gost/gost-27001-2006>

1.3 ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». - М.: Стандартинформ, 2009. — Режим доступа: <https://gostexpert.ru/gost/gost-18044-2007>

1.4 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. — Режим доступа: <https://gostexpert.ru/gost/gost-27002-2012>

1.5. ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство». М.: Стандартинформ, 2011. — Режим доступа: <https://gostexpert.ru/gost/gost-53647.1-2009>

1.6 ГОСТ Р 53647.2-2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования». М.: Стандартинформ, 2011. — Режим доступа: <https://gostexpert.ru/gost/gost-53647.2-2009>

1.7 ГОСТ Р 53647.3-2010 «Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению». М.: Стандартинформ, 2011. — Режим доступа: <https://gostexpert.ru/gost/gost-53647.3-2010>

2. Дронов В.Ю., Международные и отечественные стандарты по информационной безопасности [Электронный ресурс]: Дронов В.Ю. - Новосибирск: Изд-во НГТУ, 2016. - 34 с. - ISBN 978-5-7782-3112-2 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785778231122.html>.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации")

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_208191/](http://www.consultant.ru/document/cons_doc_LAW_208191/)

3.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации")

Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_191669/](http://www.consultant.ru/document/cons_doc_LAW_191669/)

#### учебно-методическая

1. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). URL: <http://edu.ulsu.ru/courses/750/interface/>.

**2. Иванцов А. М.**

Методические указания для самостоятельной работы студентов по дисциплине «Гуманитарные аспекты информационной безопасности» для студентов специалитета по специальности 10.05.01 очной формы обучения / А. М. **Иванцов**; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 387 КБ). - Текст: электронный.

<http://lib.ulsu.ru/MegaPro/Download/MObject/4964>

Согласовано:  
Гл. биб-рь ИБ УлГУ / Попова И. В. / *ИВ* / 14.06.2019  
Должность сотрудника научной библиотеки      ФИО      подпись      дата

## 11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

### в) Профессиональные базы данных, информационно-справочные системы

#### 1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов, [2019]. - Режим доступа: <http://www.iprbookshop.ru>.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://www.biblio-online.ru>.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://www.studentlibrary.ru/pages/catalogue.html>.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: <https://e.lanbook.com>.

1.5. **Znanium.com** [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: <http://znanium.com>.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва: КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс]: электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: <https://dlib.eastview.com/browse/udb/12>.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://нэб.рф>.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: <https://dvs.rsl.ru>.

#### 6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: <http://window.edu.ru>

6.2. Федеральный портал Российское образование. Режим доступа: <http://www.edu.ru>

#### 7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : <http://lib.ulsu.ru/MegaPro/Web>

7.2. Образовательный портал УлГУ. Режим доступа : <http://edu.ulsu.ru>

8. **ГОСТ-Эксперт** - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИИТ  
Должность сотрудника УИИТ

/Клочкова А.В.  
ФИО

 14.06.2019  
подпись дата