УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «18» мая 2021 г., протокол № 4/21

Председатель _____ / М.А. Волков
«18» мая 2021 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 2021 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»
_____ / Андреев А.С. / (подпись) (Ф.И.О.) « 12 » 05 2021 г.	_____ / Андреев А.С. / (подпись) (Ф.И.О.) « 12 » 05 2021 г.

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 правовые документов в своей профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина "Гуманитарные аспекты информационной безопасности" изучается в 5 семестре и относится к обязательным дисциплинам вариативной части блока Б1, 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», «Защита программ и данных», «Профессиональная этика».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ 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
УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**Знать:** методы системного и критического анализа методики разработки стратегии действий для выявления и решения проблемной ситуации **Уметь:** применять методы системного подхода и критического анализа проблемных ситуаций разрабатывать стратегию действий, принимать конкретные решения для ее реализации **Владеть:** методологией системного и критического анализа проблемных ситуаций методиками постановки цели, определения способов ее достижения, разработки стратегий действий
ПК-1 - Способен формировать комплекс мер для защиты информации ограниченного доступа, управлять процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем	**Знать:** Комплекс мер для защиты информации ограниченного доступа Источники и классификацию угроз информационной безопасности Нормативные правовые акты в области защиты информации **Уметь:** Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Формировать комплекс мер для защиты информации ограниченного доступа, управлять процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем **Владеть:** Навыками формирования комплекса мер для защиты информации ограниченного доступа, управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем

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 ___очная_____)			
	Всего по плану	В т.ч. по семестрам		
		5 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.

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

Форма обучения очная

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		лекции	Практич. занятия, семинары	Лабораторные работа			
Раздел 1. Гуманитарная сущность информационной безопасности							
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
Раздел 2. Управление информационной безопасностью							
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	

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 глобальная 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, формальные 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 диплом-ных работ для 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.

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.
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
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 занятия, зачет
Раздел 1. Тема 2. Информационная безопасность	Подготовка к занятию, подготовка рефератов,	2	Тесты перед занятия, зачет

как гуманитарная проблема	подготовка к сдаче зачета		
Раздел 1. Тема 3. Проблемы реализации гуманитарной сущности информационной безопасности	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятия, зачет
Раздел 1. Тема 4. Культура информационной безопасности	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятия, зачет
Раздел 2. Управление информационной безопасностью Тема 5. Стандарты информационной безопасности	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятия, зачет
Раздел 2. Тема 6. Система управления информационной безопасностью	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	4	Тесты перед занятия, зачет
Раздел 2. Тема 7. Анализ рисков информационной безопасности предприятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты перед занятия, зачет
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 занятия, зачет
Раздел 2. Тема 9. Политика информационной безопасности предприятия	Подготовка к занятию, подготовка рефератов, подготовка к сдаче зачета	2	Тесты накануне перед занятия, 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 занятия, 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 занятия, 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 занятия, 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 занятия, 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». - 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/

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/

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/cources/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, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 387 КБ). - Текст : электронный.
http://lib.ulsu.ru/MegaPro/Download/MObject/4261

Согласовано:

Гл.библ-рь НБ УлГУ	Полина И.Ю		04.05.2021
должность сотрудника научной библиотеки	ФИО	подпись	дата

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL:

https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	04.05.2021
должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций: 3/317, 2/24б.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт 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:

– 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: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО