

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Факультет истории, политологии и филологии
Кафедра политологии, социологии и международных процессов

УТВЕРЖДАЮ:
Декан факультета



С. К. Лямин

«17» июня 2026 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.В.ДВ.03.1 Информационная безопасность

Направление подготовки/специальность: 41.04.05 - Международные отношения

Профиль/направленность/специализация: Международная безопасность

Уровень высшего образования: магистратура

Квалификация: Магистр

год набора: 2026

Тамбов, 2026

Автор программы:

Кандидат исторических наук, доцент Жуковская Наталия Юрьевна

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 41.04.05 - Международные отношения (уровень магистратуры) (приказ Министерства образования и науки РФ от «12» июля 2017 г. № 649).

Рабочая программа принята на заседании Кафедры политологии, социологии и международных процессов «16» июня 2026 г. Протокол № 11

Рассмотрена и одобрена на заседании Ученого совета Факультета истории, политологии и филологии, Протокол от «17» июня 2026 г. № 10.

СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП магистратуры.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	7
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	18
6. Учебно-методическое и информационное обеспечение дисциплины.....	19
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	20

1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-2 Владеет навыками отслеживания динамики основных характеристик среды международной безопасности и пониманием их влияния на национальную безопасность Российской Федерации

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- экспертно-аналитический

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 01 Образование и наука (в сферах: профессионального обучения, среднего профессионального и высшего образования, дополнительного образования; научных исследований), 07 Административно-управленческая и офисная деятельность (в сферах администрирования дипломатических, экономических и иных связей органов государственной власти, организаций сферы бизнеса и общественных организаций Российской Федерации с представителями соответствующих стран и регионов мира; протокольной деятельности; организации проектов и программ международного профиля)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-2 Владеет навыками отслеживания динамики основных характеристик среды международной безопасности и пониманием их влияния на национальную безопасность Российской Федерации	Понимает проблемы международной информационной безопасности

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-2 Владеет навыками отслеживания динамики основных характеристик среды международной безопасности и пониманием их влияния на национальную безопасность Российской Федерации

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения		
		Очная (семестр)		
		1	2	4
1	Безопасность и сотрудничество приграничных территорий	+		
2	Институты и политика Европейского союза			+
3	Контроль над вооружениями		+	

4	Международные военно-политически е организации		+	
5	Новые угрозы международной безопасности		+	
6	Преддипломная практика			+
7	Современные экономические конфликты		+	
8	Энергетическая безопасность		+	

2. Место дисциплины в структуре ОП магистратуры:

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 41.04.05 - Международные отношения.

Дисциплина «Информационная безопасность» изучается в 4 семестре.

3. Объем и содержание дисциплины

3.1. Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
Общая трудоёмкость дисциплины	108
Контактная работа	16
Лекции (Лекции)	8
Практические (Практ. раб.)	8
Самостоятельная работа (СР)	56
Экзамен	36

3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Пра кт. раб.	СР	
		О	О	О	
4 семестр					
1	Теоретические аспекты информационной безопасности	2	2	14	Собеседование; Реферат
2	Понятие информационных угроз и их виды	2	2	14	Собеседование; Тестирование
3	Государственное регулирование информационной безопасности	2	2	14	Собеседование

4	Подходы, принципы, методы и средства обеспечения безопасности	2	2	14	Тестирование; Реферат
---	---	---	---	----	--------------------------

Тема 1. Теоретические аспекты информационной безопасности (ПК-2)

Лекция.

Информационное общество. Информационное пространство. Информационная война и информационное противоборство. Информационная преступность. Угрозы безопасности информации. Информационная безопасность (ИБ). Политика безопасности. Объекты и субъекты обеспечения ИБ. Методы и средства обеспечения ИБ. Системный подход к защите информации.

Практическое занятие.

1. Информация как товар и объект безопасности.
2. Информационные ресурсы и информационная безопасность.
3. Правовой режим информационных ресурсов. Информационно-правовые отношения.
4. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации.
5. Понятие уязвимости информации.
6. Информационные ресурсы государственные и негосударственные.

Задания для самостоятельной работы.

Самостоятельная работа: изучение статьи А.В. Россошаского Политические аспекты информационной безопасности

Тема 2. Понятие информационных угроз и их виды (ПК-2)

Лекция.

Информационные угрозы. Угрозы нарушения конфиденциальности информации. Информационная атака. Потенциальные злоумышленники (хакеры, крекеры). Информационные угрозы для государства, для компании (юридического лица), для личности (физического лица). Естественные и человеческие факторы информационных угроз (ИУ). Классификация угроз безопасности информации. Несанкционированный доступ к защищаемой информации. Вредоносные программы. Разглашение и утечка конфиденциальной информации (КИ). Каналы утечки КИ.

Практическое занятие.

1. Компьютерные преступления и наказания. Исторические примеры и современность.
2. Риски угроз информационным ресурсам.
3. Типовые пути несанкционированного доступа к информации
4. Исторические аспекты реализации информационных угроз.

Задания для самостоятельной работы.

Самостоятельная работа: Самостоятельное изучение монографии Лопатин В.Н. Информационная безопасность России : Человек. Общество. Государство. - СПб.: Фонд "Университет", 2000. - 424 с.

Тема 3. Государственное регулирование информационной безопасности (ПК-2)

Лекция.

Ущерб от компьютерных злоупотреблений. Исторические аспекты борьбы органов уголовной юстиции с компьютерной преступностью (опыт США, стран Западной Европы, России). Меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности. Международные договоры, доктрины в области ИБ. Информационные права граждан. Основные законодательные по ИБ физических и юридических лиц в России (Конституция РФ, федеральные законы, Уголовный кодекс, Налоговый кодекс, Гражданский кодекс и др.). Специальное законодательство в области информатизации информационных технологий и информационной безопасности – федеральные законы, их структура и содержание.

Практическое занятие.

1. Доктрина информационной безопасности России.
2. Стандарты информационной безопасности.
3. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.
4. Повышение образовательной и правовой культуры населения в сфере ИБ.

Задания для самостоятельной работы.

Самостоятельная работа: сравнительный анализ доктрин информационной безопасности РФ (по годам)

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности (ПК-2)

Лекция.

Управление защитой информации. Фрагментарный и комплексный подходы к защите информации. Характеристики методов средств ИБ. Криптография, механизмы цифровой подписи и особенности ее применения. Идентификация и аутентификация. Разграничения доступа. Протоколирование и аудит. Организация конфиденциального делопроизводства. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Методы и средства защиты от вредоносных программ. Профилактика вирусного заражения программ. Защита информация в Интернете.

Практическое занятие.

1. Организация системы защиты информации
2. Политика информационной безопасности. Принципы реализации политики безопасности.
3. Основные принципы управления рисками информационной безопасности
4. Образовательные технологии

Задания для самостоятельной работы.

Самостоятельная работа: Изучение сборника статей Астайкин, А. И., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н. Информационная безопасность и защита информации. В 2 томах. Т. 2 : сборник статей. - Весь срок охраны авторского права; Информационная безопасность и защита информации. В 2 томах. Т. 2. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2017. - 500 с. - URL: <https://www.iprbookshop.ru/89889.html>

4. Контроль знаний обучающихся и типовые оценочные средства

4.1. Распределение баллов:

4 семестр

- текущий контроль – 50 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Теоретические аспекты информационн ой безопасности	Собеседо вание	10	Студент получает баллы за каждое выполненное задание: 10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной социологии образования 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной социологии образования. 3 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.
		Реферат	10	Критерии оценки: - соответствие требованиям, предъявляемым к работе такого формата – 2 балла; - обоснованность выбора темы, ее значимость (актуальность) – 2 балла; - раскрытие темы на теоретическом уровне – 2 балла; - грамотность изложения материала – 2 балла; - соответствие содержания теме задания – 1 балл; - четкость выводов – 1 балл.
2.	Понятие информационн ых угроз и их виды	Собеседо вание	10	Студент получает баллы за каждое выполненное задание: 10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной социологии образования 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной социологии образования. 3 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.
		Тестиров ание(кон трольны й срез)	10	10 баллов – студент правильно отвечает на 75-100% вопросов в тесте 7 баллов – студент правильно отвечает на 50-74% вопросов в тесте 5 баллов – студент правильно отвечает на 25-50% вопросов в тесте.

3.	Государственное регулирование информационной безопасности	Собеседование	10	Студент получает баллы за каждое выполненное задание: 10 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы, вести дискуссию с использованием терминологии современной социологии образования 5 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию с использованием терминологии современной социологии образования. 3 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.
4.	Подходы, принципы, методы и средства обеспечения безопасности	Тестирование	10	10 баллов – студент правильно отвечает на 75-100% вопросов в тесте 7 баллов – студент правильно отвечает на 50-74% вопросов в тесте 5 баллов – студент правильно отвечает на 25-50% вопросов в тесте.
		Реферат(контрольный срез)	10	Критерии оценки: - соответствие требованиям, предъявляемым к работе такого формата – 2 балла; - обоснованность выбора темы, ее значимость (актуальность) – 2 балла; - раскрытие темы на теоретическом уровне – 2 балла; - грамотность изложения материала – 2 балла; - соответствие содержания теме задания – 1 балл; - четкость выводов – 1 балл.
5.	Премияльные баллы		20	- постоянная активность во время практических занятий – 10 баллов; - участие в конференциях, публикации научных статей и тезисов докладов – 10 баллов
6.	Ответ на экзамене		30	10-17 баллов – студент раскрыл основные вопросы и задания билета на оценку «удовлетворительно» 18-24 баллов – студент раскрыл основные вопросы и задания билета на оценку «хорошо», 25-30 баллов – студент раскрыл основные вопросы и задания билета на оценку «отлично»
7.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы		70	Добор баллов: студент может предоставить все задания текущего контроля и задания контрольных срезов
8.	Итого за семестр		100	

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо

50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

4.2 Типовые оценочные средства текущего контроля

Реферат

Тема 1. Теоретические аспекты информационной безопасности

Тематика рефератов и презентаций:

1. Угрозы информационной безопасности и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

Тематика рефератов

1. Информационное право и информационная безопасность
2. Концепция информационной безопасности.
3. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
4. Классификация информации. Виды данных и носителей.
5. Понятие ценности информации. Цена информации.
6. Виды угроз безопасности информации.
7. Основные принципы добывания информации.
8. Методы синтеза информации.
9. Каналы утечки информации
10. Понятия искажения информации, виды искажений. Информационный портрет.

Собеседование

Тема 1. Теоретические аспекты информационной безопасности

1. Информация как товар и объект безопасности.
2. Информационные ресурсы и информационная безопасность.
3. Правовой режим информационных ресурсов. Информационно-правовые отношения.
4. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации.
5. Понятие уязвимости информации.
6. Информационные ресурсы государственные и негосударственные.

Тема 2. Понятие информационных угроз и их виды

1. Компьютерные преступления и наказания. Исторические примеры и современность.
2. Риски угроз информационным ресурсам.
3. Типовые пути несанкционированного доступа к информации
4. Исторические аспекты реализации информационных угроз.

Тема 3. Государственное регулирование информационной безопасности

1. Доктрина информационной безопасности России.
2. Стандарты информационной безопасности.
3. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.
4. Повышение образовательной и правовой культуры населения в сфере ИБ.

Тестирование

Тема 2. Понятие информационных угроз и их виды

::Вопрос1::Какой из принципов информационной безопасности означает гарантию того, что информация не была изменена несанкционированно?

- {
- =Целостность
- ~Конфиденциальность
- ~Доступность
- ~Неотказуемость
- }

::Вопрос2::Какое государство в 2007 году впервые столкнулось с масштабными кибератаками на государственные и финансовые институты, что привело к созданию Центра передового опыта НАТО по киберобороне?

- {
- =Эстония
- ~Латвия
- ~Литва
- ~Польша
- }

::Вопрос3::Как называется документ, закрепляющий право государства на применение силы в ответ на кибератаку, которая по масштабу сравнима с вооружённым нападением?

- {
- =Статья 51 Устава ООН
- ~Будапештская конвенция
- ~Женевские конвенции
- ~Договор о нераспространении кибероружия
- }

::Вопрос4::Как расшифровывается аббревиатура DDoS?

- {
- =Distributed Denial of Service
- ~Direct Data Operating System
- ~Dynamic Domain of Security
- ~Digital Defense of Software
- }

::Вопрос5::Какой термин обозначает использование цифровых технологий для вмешательства во внутренние дела другого государства с целью дестабилизации политической обстановки?

- {
- =Киберсубверсия
- ~Кибертерроризм
- ~Кибершпионаж
- }

~Киберфишинг

}

::Вопрос6::Согласно концепции «киберсуверенитета», государство имеет право:

{

=Контролировать национальный сегмент интернета и ограничивать трансграничный поток данных

~Блокировать любые кибератаки в глобальной сети без согласия других стран

~Требовать выдачи хакеров независимо от их гражданства

~Участвовать в управлении корневыми серверами DNS на равных правах с США

}

::Вопрос7::Как называется метод информационно-психологического воздействия, при котором создаются поддельные аккаунты для распространения дезинформации от лица реальных людей или организаций?

{

=Самозванство (impersonation)

~Фишинг

~Спам

~Кибербуллинг

}

::Вопрос8::Какая страна первой законодательно закрепила концепцию «суверенного интернета» с возможностью отключения от глобальной инфраструктуры?

{

=Россия

~Китай

~Иран

~Туркменистан

}

::Вопрос9::Что означает термин «атрибуция» в контексте международной кибербезопасности?

{

=Установление источника и виновника кибератаки

~Шифрование дипломатической переписки

~Блокировка вредоносного трафика на границе

~Создание резервных копий данных

}

::Вопрос10::Как называется соглашение о сотрудничестве в сфере кибербезопасности между странами — участницами СНГ?

{

=Соглашение о сотрудничестве в области обеспечения международной информационной безопасности (2013 год)

~Бишкекский меморандум о кибермире

~Алма-Атинская конвенция о кибербезопасности

~Ташкентский договор о защите информации

}

::Вопрос11::Какой тип киберугроз предполагает вымогательство денег за расшифровку заблокированных данных?

{

=Ransomware

~Spyware

~Adware

~Malware общего типа

}

::Вопрос12::Какая международная организация разработала Будапештскую конвенцию о киберпреступности?

{

=Совет Европы

~ООН

~НАТО

~Европейский союз

}

::Вопрос13::Что такое «цифровой след» государства в контексте международных отношений?

{

=Совокупность данных о цифровой инфраструктуре и активности государства, доступных внешним акторам

~Количество интернет-пользователей в стране

~Протоколы дипломатических переговоров в цифровом виде

~Перечень государственных сайтов, защищённых специальными сертификатами

}

::Вопрос14::Как называется принцип, согласно которому кибератака на одну страну НАТО рассматривается как атака на весь альянс?

{

=Статья 5 Североатлантического договора (принцип коллективной обороны)

~Доктрина киберсдерживания

~Концепция общего киберпространства

~Принцип неделимости кибербезопасности

}

::Вопрос15::Кто является основным объектом защиты в рамках Международного гуманитарного права при кибероперациях во время вооружённого конфликта?

{

=Гражданское население и гражданские объекты

~Военные базы противника

~Командные центры и узлы связи

~Инфраструктура ядерных сил сдерживания

}

::Вопрос16::Как термин «кибероружие» впервые был применён к реальному инциденту?

{

=Червь Stuxnet против иранских центрифуг (2010 год)

~Атака Slammer на банкоматы (2003 год)

~Вирус NotPetya против украинских энергосетей (2017 год)

~Атака SolarWinds на правительство США (2020 год)

}

::Вопрос17::Что такое «фейковая новость» (fake news) с точки зрения информационной войны?

{

=Целенаправленно созданное и распространяемое ложное сообщение, имитирующее журналистский материал

~Любое неподтверждённое сообщение в интернете

~Сатирический или пародийный новостной контент

~Новость, опубликованная непрофильным СМИ

}

::Вопрос18::Какая страна инициировала создание Группы правительственных экспертов ООН (UNGGE) по вопросам информационной безопасности?

- {
- =Россия
- ~США
- ~Китай
- ~Великобритания
- }

::Вопрос19::Как называется метод защиты информации, при котором данные преобразуются в нечитаемый вид с использованием ключа, доступного только авторизованным сторонам?

- {
- =Шифрование (криптография)
- ~Стеганография
- ~Фильтрация
- ~Виртуализация
- }

::Вопрос20::Что означает термин «хактивизм»?

- {
- =Использование хакерских методов для достижения политических или социальных целей
- ~Наёмная киберпреступность для корпоративного шпионажа
- ~Деятельность государственных хакерских подразделений
- ~Защита критической инфраструктуры от кибератак
- }

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

::Вопрос1::Выберите два понятия, которые относятся к категории «меры построения доверия» в киберпространстве (CBMs), рекомендованные ОБСЕ и ООН.

- {
- ~%50%Создание национальных точек контакта (CERT-to-CERT взаимодействие)
- ~%50%Проведение совместных учений и семинаров по кибербезопасности
- ~Одностороннее отключение интернета на время кризиса
- ~Применение наступательного кибероружия в качестве первого удара
- }

::Вопрос12::Укажите два государства, которые публично заявляли о создании национальных кибервойск как отдельного рода сил.

- {
- ~%50%США (Киберкомандование)
- ~%50%Россия (Кибервойска)
- ~Франция (Легион кибернетических операций)
- ~Япония (Цифровая гвардия)
- }

::Вопрос3::Выберите два международных соглашения, которые регулируют сотрудничество в сфере кибербезопасности на постсоветском пространстве.

- {
- ~%50%Соглашение СНГ о сотрудничестве в области обеспечения международной информационной безопасности (2013)
- ~%50%Договор о коллективной безопасности ОДКБ (раздел о противодействии киберугрозам)
- ~Болонское соглашение о кибердипломатии
- ~Лиссабонский меморандум о цифровом рынке
- }

::Вопрос4::Какие два феномена считаются основными угрозами для демократических избирательных процессов в контексте информационной безопасности?

- {
- ~%50%Целенаправленные утечки компрометирующей информации через анонимные платформы
- ~%50%Таргетированная дезинформация и агитация через алгоритмы социальных сетей
- ~Блокировка избирательных участков по техническим причинам
- ~Низкая явка избирателей из-за отказа от интернета
- }

::Вопрос5::Укажите две характеристики, которые отличают государственный кибершпионаж от негосударственного.

- {
- ~%50%Наличие политических целей, а не только финансовых
- ~%50%Использование ресурсов и инфраструктуры государства (включая АРТ-группы с господдержкой)
- ~Обязательное уничтожение данных после завершения операции
- ~Публичное признание ответственности за атаку
- }

::Вопрос6::Какие два правовых подхода к киберпреступлениям продвигаются разными блоками государств в рамках международных дискуссий?

- {
- ~%50%Разработка нового универсального международного договора о противодействии киберпреступности (позиция России и Китая)
- ~%50%Расширение Будапештской конвенции и присоединение к ней новых стран (позиция Совета Европы и США)
- ~Полная демилитаризация киберпространства по примеру Антарктики
- ~Передача всех киберрасследований под юрисдикцию Международного уголовного суда
- }

::Вопрос7::Выберите два вида деятельности, которые технически считаются «активной киберобороной» (active cyber defense) по классификации НАТО.

- {
- ~%50%Контрольные меры (beaconing) для отслеживания украденных данных
- ~%50%Блокировка вредоносного трафика на уровне национального сегмента сети
- ~Проведение упреждающих хакерских атак на серверы противника
- ~Физическое уничтожение серверного оборудования на чужой территории
- }

::Вопрос8::Какие два международных инцидента считаются поворотными точками в формировании современной системы кибербезопасности?

- {
- ~%50%Кибератаки на Эстонию (2007 год)
- ~%50%Атака Stuxnet на иранские ядерные объекты (2010 год)
- ~Создание первого антивируса (1987 год)
- ~Изобретение протокола HTTPS (1994 год)
- }

::Вопрос9::Укажите два основных аргумента в пользу концепции «киберсуверенитета», которые выдвигаются государствами.

- {
- ~%50%Необходимость защиты национального суверенитета от внешнего цифрового вмешательства
- ~%50%Право государства регулировать деятельность иностранных ИТ-корпораций на своей территории
- ~Невозможность технического контроля за трансграничными потоками данных
- }

~Отсутствие международных норм в киберпространстве

}

::Вопрос10::Какие два типа субъектов международных отношений чаще всего совершают кибератаки с целью дезинформации (disinformation)?

{

~%50%Государственные структуры (спецслужбы, министерства пропаганды)

~%50%Связанные с государством прокси-группы (аффилированные хактивисты, «тролли»)

~Одиночные хакеры-криминалисты

~Транснациональные корпорации IT-сектора

}

::Вопрос11::Дополните: Международная процедура, при которой государство запрашивает у другого государства данные о пользователе или блокировку контента через официальные каналы, называется взаимной

{

=правовой помощью (Mutual Legal Assistance)

}

::Вопрос12::Вставьте пропущенное слово: Наиболее известная кибератака с использованием принципа «целевой атаки на цепочку поставок» (supply chain attack) была осуществлена через взлом программного обеспечения ... в 2020 году.

{

=SolarWinds

}

::Вопрос13::Дополните: Первая в истории кибератака, приведшая к физическому уничтожению промышленного оборудования (центрифуг), была совершена червём

{

=Stuxnet

}

::Вопрос14::Вставьте пропущенное слово: Термин, обозначающий уязвимость, неизвестную разработчику программного обеспечения, которая используется спецслужбами для взлома до официального выпуска исправления, — это уязвимость ... дня.

{

=нулевого

=zero-day

}

::Вопрос15::Дополните: «Дипломатия в цифровую эпоху» (Digital Diplomacy) включает в себя как официальную переписку через защищённые каналы, так и ведение аккаунтов посольств в

{

=социальных сетях

}

::Вопрос16::Вставьте пропущенное слово: Технология распределённого реестра (блокчейн) рассматривается некоторыми государствами как способ защиты дипломатической переписки от

{

=взлома

=подделки

=несанкционированного доступа

}

::Вопрос17::Дополните: Концепция, при которой государство обучает и привлекает к оборонным кибероперациям частные IT-компании и добровольцев (аналог «народного ополчения» в сети), называется

{

=кибермилиция

=киберополчение

}

::Вопрос18::Вставьте пропущенное слово: Формат взаимодействия технических групп быстрого реагирования на киберинциденты разных стран называется CERT-to-CERT ...

{

=сотрудничество

=взаимодействие

}

::Вопрос19::Дополните: Расшифруйте аббревиатуру АРТ в контексте компьютерных угроз: Advanced ... Threat.

{

=Persistent

=усложнённая устойчивая угроза

}

::Вопрос20::Вставьте пропущенное слово: Первый в истории случай применения кибероружия в межгосударственном конфликте некоторые исследователи связывают с атаками на ... в 2007 году.

{

=Эстонию

}

4.3 Промежуточная аттестация по дисциплине проводится в форме экзамена

Типовые вопросы экзамена (ПК-2)

1. Информационное общество и информационное пространство
2. Информационная преступность, угрозы безопасности информации
3. Методы и средства обеспечения ИБ. Системный подход к защите информации.
4. Компьютерные преступления и наказания. Исторические примеры и современность.
5. Риски угроз информационным ресурсам.
6. Типовые пути несанкционированного доступа к информации
7. Исторические аспекты реализации информационных угроз.
8. Доктрина информационной безопасности России.
9. Стандарты информационной безопасности.
10. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.

Типовые задания для экзамена (ПК-2)

Тематика презентаций

1. Угрозы информационной безопасности и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-2	Демонстрирует высокий уровень понимания проблемы международной информационной безопасности
«хорошо» (70 - 84 баллов)	ПК-2	Демонстрирует средний уровень понимания проблемы международной информационной безопасности
«удовлетворительно» (50 - 69 баллов)	ПК-2	Демонстрирует низкий уровень понимания проблемы международной информационной безопасности
«неудовлетворительно» (менее 50 баллов)	ПК-2	Не понимает проблемы международной информационной безопасности

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература:

1. Международная информационная безопасность, 2021
2. Бирюков А. В., Алборова М. Б. Социально-гуманитарные риски информационного общества и международная информационная безопасность : монография. - Москва: Аспект-Пресс, 2021. - 94, [1] с. - Текст : электронный // АБИС "Руслан" ТГУ им. Г.Р. Державина [сайт]

6.2 Дополнительная литература:

1. Господарик Ю.П., Пашковская В.М. Международная экономическая безопасность : учебник : для студентов высших учебных заведений, обучающихся по направлениям "Экономика и управление", "Информационная безопасность" и "Экономическая безопасность". - 2-е изд., стер.. - Москва: Ун-т Синергия, 2017. - 414 с.
2. Лопатин В.Н. Информационная безопасность России : Человек. Общество. Государство. - СПб.: Фонд "Университет", 2000. - 424 с.
3. Артемов А. В. Информационная безопасность : курс лекций. - Орел: Межрегиональная академия безопасности и выживания, 2014. - 257 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=428605>
4. Зенков А. В. Информационная безопасность и защита информации : учебник для вузов. - пер. и доп; 2-е изд.. - Москва: Юрайт, 2025. - 107 с. - Текст : электронный // ЭБС «ЮРАЙТ» [сайт]. - URL: <https://urait.ru/bcode/567915>

6.3 Иные источники:

1. elibrary.tsutmb.ru - <https://elibrary.tsutmb.ru/>
2. ЭБ диссертаций РГБ - электронные версии кандидатских и докторских диссертаций на русском языке Правообладатель: ФГБУ «Российская государственная библиотечная система» - <http://www.diss.rsl.ru>
3. Статистические базы данных ООН - <https://www.un.org/ru/databases/>
4. Аналитический центр при правительстве Российской Федерации. Официальный сайт. - <https://ac.gov.ru>
5. Аналитический центр Юрия Левады «Левада-центр» - www.levada.ru
6. Библиотека Гумер - <http://www.gumer.info/>
7. Библиотека научной и учебной литературы - <http://sbiblio.com>
8. Библиотека РАН - <http://www.ras.ru/>
9. Вестник Московского университета. Серия 12: Политические науки - https://www.elibrary.ru/title_about_new.asp?id=8379e
https://www.elibrary.ru/title_about_new.asp?id=8379

7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Microsoft Windows 10

Microsoft Office Профессиональный плюс 2007
Google Chrome

Профессиональные базы данных и информационные справочные системы:

1. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
2. Электронная библиотека ТГУ. – URL: <https://elibrary.tsutmb.ru/>
3. Государственная информационная система «Национальная электронная библиотека» . – URL: <https://rusneb.ru>
4. Научная электронная библиотека «КиберЛенинка». – URL: <https://cyberleninka.ru>
5. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prlib.ru>
6. Российская государственная библиотека: официальный сайт. – URL: <https://www.rsl.ru>
7. Российская национальная библиотека: официальный сайт. – URL: <http://nlr.ru>
8. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
9. Тамбовская областная универсальная научная библиотека им. А.С. Пушкина: официальный сайт. – URL: <http://www.tambovlib.ru>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.