

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной и прикладной информатики

Дата подписания: 23.05.2024 12:07:04

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688edddbc475e411a

## **Аннотация к рабочей программе дисциплины «История информационного противоборства»**

### **Цель преподавания дисциплины**

Целью преподавания дисциплины «История информационного противоборства» является получение студентами знаний о видах, способах и методах информационного воздействия, об истории возникновения информационных войн, признаках и особенностях их проявления, этапах становления предметной области защиты информации, формирования органов исполнительной власти, отвечающих за реализацию политики безопасности в РФ.

### **Задачи изучения дисциплины**

- получение знаний об информационном противоборстве, исторических этапах возникновения информационных войн и методов информационного воздействия на различных этапах истории;
- изучение значения информации в развитии современного общества;
- изучение этапов формирования комплекса мер по обеспечению информационной безопасности;
- изучение задач и принципов организации и выполнения комплекса мер по обеспечению информационной безопасности;
- овладение навыками применения информационных технологий для поиска и обработки информации;
- овладение навыками управления процессом реализации комплекса мер по обеспечению информационной безопасности.

### **Индикаторы компетенций, формируемые в результате освоения дисциплины**

ОПК-13.1 Выявляет существенные черты исторических процессов, явлений и событий.

ОПК-13.2 Соотносит общие исторические процессы и отдельные факты.

ОПК-13.3 Формулирует собственную позицию по различным проблемам истории.

### **Разделы дисциплины**


История возникновения органов защиты информации. Защита государственных интересов в XII – XVI вв. Защита государственных интересов в XVI - XVIII вв. Защита государственных интересов в XIX веке. Защита государственных интересов в 1900-1917 гг. Защита государственных интересов в период создания Советской власти и НЭПа. Защита государственных интересов в 1928 – 1941. годах. Защита государственных интересов в период великой отечественной войны. Система безопасности СССР и России в XX – XXI веках. Система безопасности СССР в 40-80х

годах XX века. Международные подходы к концепции информационной войны XX – начала XI вв. Система безопасности СССР в 40-80х годах XX века. Международные подходы к концепции информационной войны XX – начала XI вв.

## МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

И.О. декана факультета  
Фундаментальной и прикладной  
информатики*(наименование ф-та полностью)*  
М.О. Таныгин  
*(подпись, инициалы, фамилия)*« 31 » августа 2021 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

История информационного противоборства*(наименование дисциплины)*ОПОП ВО 10.03.01 Информационная безопасность*(шифр согласно ФГОС и наименование направления подготовки (специальности))*направленность (профиль, специализация) «Безопасность автоматизирован-  
ных систем в сфере информационных и коммуникационных технологий»*наименование направленности (профиля, специализации)*

форма обучения

очная*(очная, очно-заочная, заочная)*

Рабочая программа дисциплины История информационного противоборства составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 10.03.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета (протокол №6« 26» 02 2021 г.).

Рабочая программа дисциплины История информационного противоборства обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, на заседании кафедры информационной безопасности Протокол № 1 « 30» 08 2021г.

Зав. кафедрой  
Разработчик программы  
к.воен.н., доцент  
Директор научной библиотеки

Таныгин М.О.

Ханис А.Л.

Макаровская В.Г.

Рабочая программа дисциплины История информационного противоборства пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета Протокол №6« 02» 02 2021г., на заседании кафедры ИБ №11 от 30.06.22г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой \_\_\_\_\_

Рабочая программа дисциплины История информационного противоборства пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий, одобренного Ученым советом университета Протокол № « » \_\_\_\_\_ 20 г., на заседании кафедры \_\_\_\_\_

(наименование кафедры, дата, номер протокола)

Зав. кафедрой \_\_\_\_\_

## **1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

### **1.1 Цель дисциплины**

Целью преподавания дисциплины «История информационного противоборства» является получение студентами знаний о видах, способах и методах информационного воздействия, об истории возникновения информационных войн, признаках и особенностях их проявления, этапах становления предметной области защиты информации, формирования органов исполнительной власти, отвечающих за реализацию политики безопасности в РФ.

### **1.2 Задачи дисциплины**

- получение знаний об информационном противоборстве, исторических этапах возникновения информационных войн и методов информационного воздействия на различных этапах истории;
- изучение значения информации в развитии современного общества;
- изучение этапов формирования комплекса мер по обеспечению информационной безопасности;
- изучение задач и принципов организации и выполнения комплекса мер по обеспечению информационной безопасности;
- овладение навыками применения информационных технологий для поиска и обработки информации;
- овладение навыками управления процессом реализации комплекса мер по обеспечению информационной безопасности.

### **1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
ОПК-13	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-13.1  Выявляет существенные черты исторических процессов, явлений и событий.	<b><i>Знать:</i></b> исторические этапы развития и причины возникновения информационного противоборства, средства воздействия и способы ведения информационного противоборства, особенности информационно-пропагандистской деятельности; виды (формы), задачи, основные методы, способы и приёмы проведения информационно-психологических войн и применения информационного оружия; виды информационных атак; особенности информационной войны против России и противостояние России информационной войне; методы манипулирования общественным сознанием в информационной войне; основные понятия, этапы и порядок проведения информационных кампаний; организационные, технические и правовые методы обеспечения морально-психологической информационной безопасности; современные теории ведения информационных войн.  <b><i>Уметь:</i></b> определять особенности процесса введения информационных войн в условиях мировой политики.

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
			<b><i>Владеть:</i></b> навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.
		ОПК-13.2 Соотносит общие исторические процессы и отдельные факты.	<b><i>Знать:</i></b> формы информационной войны, стратегию и структуру современной информационной войны, составляющие информационного противоборства, технологии ведения информационной войны; типы и основные характеристики информационных кампаний, понятие и виды информационного оружия. <b><i>Уметь:</i></b> выделять специфику каждого из видов информационной войны. <b><i>Владеть:</i></b> навыками поиска и обработки информации в современных системах и сетях, организации вопросов создания и проведения мероприятий по обеспечению информационной безопасности объекта.
		ОПК-13.3	<b><i>Знать:</i></b> особенности



<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код компетенции</i>	<i>наименование компетенции</i>		
		<p>Формулирует собственную позицию по различным проблемам истории.</p>	<p>эволюции информационного противоборства, характеристику всех существующих в настоящее время видов информационной войны, основные особенности информационной среды, в которой происходит развитие источников распространения информационных войн, основные принципы введения информационных войн в историческом развитии.</p> <p><b>Уметь:</b> определять современные формы и средства информационного воздействия, принадлежность источников и каналы передачи информации, применять технологии противодействия угрозам информационным системам и сетям на объектах информатизации.</p> <p><b>Владеть:</b> навыками анализа информации, передаваемой в открытых источниках и телекоммуникационных сетях; противодействия средствам воздействия на функционирование информационных сетей и систем.</p>



## **2. Указание места дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «История информационного противоборства», входит в обязательную часть блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы бакалавриата (специалитета, магистратуры) 10.03.01 Информационная безопасность, направленность Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий. Дисциплина изучается на 3 курсе в 5 семестре.

## **3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость (объем) дисциплины составляет 5 зачетных единиц (з.е.), 108 академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	72
в том числе:	
лекции	36
лабораторные занятия	0
практические занятия	36
Самостоятельная работа обучающихся (всего)	35,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

## **4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

### **4.1 Содержание дисциплины**

Таблица 4.1.1 - Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел, (тема) дисциплины	Содержание
1	2	3
1	История возникновения органов защиты информации.	История возникновения и становления информационного противоборства в периоды древних времён. Причины возникновения.
2	Защита государственных интересов в XII – XVI вв.	История возникновения и становления информационного противоборства в XII – XVI веках. Рассмотрение различных примеров информационного противоборства данных времён.
3	Защита государственных интересов в XVI - XVIII вв.	История возникновения и становления информационного противоборства в XVI - XVIII веках. Рассмотрение различных примеров информационного противоборства данных времён.
4	Защита государственных интересов в XIX веке.	История информационного противоборства XIX века, в эпоху. Становление органов защиты информации в XIX веке, примеры информационного противоборства.
5	Защита государственных интересов в 1900-1917 гг.	История защиты информации и информационного противоборства в период революции.
6	Защита государственных интересов в период создания Советской власти и НЭПа.	История защиты информации и информационного противоборства в периоды создания и становления Советской власти и новой экономической политики.
7	Защита государственных интересов в 1928 – 1941. годах.	Защита государственных интересов и информации и период индустриализации Советского союза, вплоть до начала Великой Отечественной войны
8	Защита государственных интересов в период великой отечественной войны.	Защита информации в период Великой отечественной войны. Объединение НКВД и НКГБ.
9	Система безопасности СССР в 40-80х годах XX века. Международные подходы к концепции информационной войны XX – начала XI вв.	Информационная безопасность в послевоенное время, во второй половине 1940-х годов, вплоть до 1980 гг. История образования новых органов защиты информации.

Таблица 4.1.2 - Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно- методич еские материа лы	Формы текущего контроля успеваемости ( <i>по неделям семестра</i> )	Компете нции
		Лек. час	№ лаб	№ пр.			
1	2	3	4	5	6	7	8
1	История возникновения органов защиты информации.	4	-	-	У-1-13, МУ-1	УО – 2	ОПК-13
2	Защита государственных интересов в XII – XVI вв.	4	-	1	У-1-13, МУ-1,2	УО – 3, ЗПР - 3	ОПК-13
3	Защита государственных интересов в XVI - XVIII вв.	4	-	-	У-1-13, МУ-1	УО – 4	ОПК-13
4	Защита государственных интересов в XIX веке.	4	-	2	У-1-13, МУ-1,2	УО – 5 ЗПР - 5	ОПК-13
5	Защита государственных интересов в 1900-1917 гг.	4	-	-	У-1-13, МУ-1	УО -6	ОПК-13
6	Защита государственных интересов в период создания Советской власти и НЭПа.	4	-	-	У-1-13, МУ-1	УО -7 КЗ-6	ОПК-13
7	Защита государственных интересов в 1928 – 1941. годах.	4	-	3	У-1-13, МУ-1,2	УО - 8 ЗПР - 8	ОПК-13
8	Защита государственных интересов в период великой отечественной войны.	4	-	-	У-1-13, МУ-1	УО – 10 КЗ-10	ОПК-13
9	Система безопасности СССР в 40-80х годах	4	-	-	У-1-13, МУ-1	УО – 12 КЗ-12	ОПК-13

XX века. Международные подходы к концепции информационной войны XX – начала XI вв.						
Всего	36					

С – собеседование, ЗПР – защита практической работы, КЗ – кейс-задача

## 4.2 Лабораторные работы и (или) практические занятия

### 4.2.1 Практические занятия

Таблица 4.2.1–Практические занятия

№п/ п	Наименование практической работы	Объем , час.
1	Информационная безопасность в системе национальной безопасности государства	12
2	Методы и средства информационного противоборства и информационно-психологического воздействия и используемые в современных СМИ и СМК	12
3	Фактологический анализ информационных сообщений для выявления применения методов информационно-психологического воздействия	12
Итого		36

## 4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздел а (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемо е на выполнение СРС, час.
1	История возникновения органов защиты информации.	1-2 недели	3,9
2	Защита государственных интересов в XII – XVI вв.	3-4 недели	4
3	Защита государственных интересов в XVI - XVIII вв.	5-6 недели	4
4	Защита государственных интересов в XIX веке.	7-8 недели	4
5	Защита государственных интересов в 1900-1917 гг.	9-10 недели	4
6	Защита государственных интересов в период создания Советской власти и НЭПа.	11-12 недели	4
7	Защита государственных интересов в 1928 – 1941 годах.	12-13 недели	4

8	Защита государственных интересов в период великой отечественной войны.	14-15 недели	4
9	Система безопасности СССР в 40-80х годах XX века. Международные подходы к концепции информационной войны XX – начала XI вв.	16-18 недели	4
Итого			35,9

## **5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное «Правилами внутреннего распорядка работников».

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес [http://www.swsu.ru/structura/up/fivt/k\\_tele/index.php](http://www.swsu.ru/structura/up/fivt/k_tele/index.php));

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путем разработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

- заданий для самостоятельной работы;

- вопросов и задач к зачёту;

- методических указаний к выполнению практических работ и т.д.

*типографией университета:*

- помощь авторам в подготовке и издании научной, учебной и методической литературы;

–удовлетворение потребности в тиражировании научной, учебной и методической литературы.

## **6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины**

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для природы, человека и общества;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, представителями работодателей (командная работа, разбор конкретных ситуаций, и др.);

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

## 7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

### 7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 - Этапы формирования компетенций

Код и наименование компетенции	Этапы* формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	Гуманитарные аспекты информационной безопасности.	Гуманитарные аспекты информационной безопасности. История информационного противоборства.	Гуманитарные аспекты информационной безопасности.

### 7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции / этап (указывается название этапа из п.7.1)	Показатели оценивания компетенции <i>(индикаторы достижения компетенции, закрепленные за</i>	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)



	<i>дисциплино й)</i>			
1	2	3	4	5
ОПК-13, основной	ОПК-13.1 Выявляет существенн ые черты историческ их процессов, явлений и событий.	Знать: основные направления информационной войны. Уметь: определять особенности процесса введения информационных войн в условиях мировой политики. Владеть: навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.	Знать: особенности эволюции информационно го противоборства; характеристику всех существующих в настоящее время видов информационно й войны; основные особенности информационно й среды, в которой происходит развитие источников распространения информационны х войн. Уметь: выделять специфику каждого из видов информационно й войны. Владеть: навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления	Знать: основные принципы введения информационных войн в историческом развитии. Уметь: выделять специфику каждого из видов информационной войны. Владеть: навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.
				3

	<p>ОПК-13.2 Соотносит общие историческ ие процессы и отдельные факты.</p>	<p>Знать: основные направления информационной войны. Уметь: определять особенности процесса введения информационных войн в условиях мировой политики. Владеть: навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.</p>	<p>информационны х. Знать: особенности эволюции информационно го противоборства; характеристику всех существующих в настоящее время видов информационно й войны; основные особенности информационно й среды, в которой происходит развитие источников распространения информационны х войн. Уметь: выделять специфику каждого из видов информационно й войны. Владеть: навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления</p>	<p>нать: основные принципы введения информационных войн в историче- ском развитии. Уметь: выделять специфику каждого из видов информационной войны. Владеть: навыками использования имеющейся теоретической информации для решения практических задач в сфере осуществления информационных войн.</p>
--	---	--	---	--

			информационных войн.	
	ОПК-13.3 Формулирует собственную позицию по различным проблемам истории.	Знать: влияние информационного противоборства на возможность обеспечения технологического процесса защиты информации. Уметь: описывать уязвимые для информационного влияния процессы обеспечения ИБ. Владеть: навыками поддержания технологического процесса обеспечения ИБ в условиях информационного противодействия.	Знать: основные аспекты влияния информационного противоборства на возможность обеспечения технологического процесса защиты информации. Уметь: выделять уязвимые для информационного влияния процессы обеспечения ИБ. Владеть: навыками обеспечения технологического процесса обеспечения ИБ в условиях информационного противодействия.	Знать: методы и средства информационного воздействия. Уметь: выделять уязвимые для информационного влияния процессы обеспечения ИБ и нивелировать выделенные угрозы. Владеть: навыками планирования и обеспечения технологического процесса обеспечения ИБ в условиях информационного противодействия.

**7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы**

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	История возникновения органов защиты информации	ОПК-13	Лекция, СРС,	Вопросы для УО	1-10	Согласно таблице 7.2
2	Защита государственных интересов в XII – XVI вв.	ОПК-13	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно таблице 7.2
3	Защита государственных интересов в XVI - XVIII вв.	ОПК-13	Лекция, СРС	Вопросы для УО	1-10	Согласно таблице 7.2
4	Защита государственных интересов в XIX веке.	ОПК-13	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно таблице 7.2
5	Защита государственных интересов в 1900-1917 гг.	ОПК-13	Лекция, СРС	Вопросы для УО	1-10	Согласно таблице 7.2
6	Защита государственных интересов в период создания Советской власти и НЭПа.	ОПК-13	Лекция, СРС	Вопросы для УО Кейс-задача	1-10 1	Согласно таблице 7.2

7	Защита государственных интересов в 1928 – 1941 годах.	ОПК-13	Лекция, СРС, практическое занятие	Вопросы для УО КВЗПР	1-10 1-10	Согласно таблице 7.2
8	Защита государственных интересов в период великой отечественной войны	ОПК-13	Лекция, СРС	Вопросы для УО Кейс-задача	1-10 2	Согласно таблице 7.2
9	Система безопасности СССР в 40-80х годах XX века. Международные подходы к концепции информационной войны XX – начала XI вв.	ОПК-13	Лекция, СРС	Вопросы для УО Кейс-задача	1-10 3	Согласно таблице 7.2

СРС – самостоятельная работа студента,

КВЗПР – контрольные вопросы для защиты практических работ

#### Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 9. «Защита государственных интересов в XII – XVI вв.».

1. Раскройте причины возникновения информационного противоборства.
2. Средства духовного воздействия, используемые противоборствующими сторонами.
3. Способы ведения информационного противоборства.

Контрольные вопросы для защиты практической работы №1:

История возникновения органов защиты информации

1. Информационное противоборство как составная часть вооруженной борьбы?
2. «Психологические операции» в Средние века.

### 3. Особенности информационно-пропагандистской деятельности.

#### Кейс-задача №3: Кибератаки в современных конфликтах

Ситуация для обсуждения: В наше время кибератаки стали важным инструментом информационного противоборства как между странами, так и между корпорациями. Хакеры могут атаковать информационные системы, причиняя серьезный ущерб для враждующих сторон.

Задание: Студентам предлагается исследовать следующие аспекты:

- Типы кибератак, используемые в современных конфликтах.
- Меры защиты от киберугроз и противодействие хакерским атакам.
- Последствия успешных кибератак на государственные и коммерческие организации.

Вопросы для обсуждения:

1. Какие стратегии кибератак широко используются в современных конфликтах, и каковы их цели?
2. Как регулярное обновление информационных систем влияет на их устойчивость к кибератакам?
3. В чем состоит роль государства и международных организаций в предотвращении и реагировании на киберугрозы?
4. Каким образом кибератаки могут повлиять на гражданское население и общественные институты?

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

*Промежуточная аттестация* по дисциплине проводится в форме зачёта. Зачёт проводится в виде бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),

- на установление правильной последовательности,
- на установление соответствия.

*Умения, навыки (или опыт деятельности) и компетенции* проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

#### Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

1. Основной критерий содержания эффективной пропаганды:

- А) Наличие центрального тезиса.
- Б) Лёгкость для понимания целевой аудиторией.
- В) Сложность для критики.
- Г) Привлекательность фона.

Задание в открытой форме:

1. Электронная война направлена против средств электронных коммуникаций .....
2. Психологическая война - пропаганда, информационная обработка населения, направленная на.....
3. Хакерская война подразумевает диверсионные действия против.....
4. Кибервойна отличается от "обычного" хакерства.....

Задание на установление правильной последовательности.

Установить в историческом порядке этапы развития информационного противоборства:

1. Распространение грамотности, в условиях широкого охвата населения новыми носителями информации: письмами, листовками, книгами, газетами, журналами и др.

2. Использование в качестве объекта воздействия - психику человека (носитель и средство доведения информации – человек).



3. Появление персональных компьютеров и межгосударственных телекоммуникационных сетей, особенно Интернета.

4. Возникновение новых носителей информации и новых средств доставки информации, появившихся благодаря открытию электричества: телеграфа, телефона, радио, кино, телевидения, звукоусилительной аппаратуры и т.п.

Задание на установление соответствия:  
между средствами и функциями

1	Человек, информация, технические средства	А	Информационное оружие
2	Целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние на функционирование и развитие психологической среды общества, психику и поведение населения, руководства страны, военнослужащих	Б	Информационное воздействие
3	Комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника в целях выведения их из строя, получения или модификации содержащихся в них данных, целенаправленного продвижения выгодной информации (или дезинформации)	В	Элементы информационного пространства
4	Применение средств, позволяющих производить с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия	Г	Психологическое воздействие

Компетентностно-ориентированная задача:

Выберите некоторое событие (информационный повод), вызвавшее активные обсуждения, дискуссии в СМИ и СМК, по тематике которого велось активное информационное противоборство. Для события в целом определите заинтересованные стороны, цели, сценарии, используемые методы информационно-психологического воздействия. Отберите два информационных сообщения, размещенных в СМИ и/или СМК разными сторонами противоборства, на тему выбранного события. Проведите фактологический анализ данных сообщений.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

#### 7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- положение П 02.016–2018 Обально-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно - рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Работа на практическом занятии №1	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Работа на практическом занятии №2	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Работа на практическом занятии №3	4	Выполнил, доля правильных ответов от 50% до 90%	8	Выполнил, доля правильных ответов более 90%
Устный опрос по темам 1-9	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Решение кейс-задач 1-2	6	Доля правильных ответов от 50% до 90%	12	Доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	0		36	
Итого	24		100	

*Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).*

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

## **8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

### **8.1 Основная учебная литература**

1. Основы информационной безопасности : учебник / В. Ю. Rogozin, И. Б. Galushkin, В. Новиков, С. Б. Veprev ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=562348> (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

2. Философские проблемы информационного противоборства: учебное пособие для бакалавров, студентов, магистрантов и аспирантов / В. С. Polikarpov, В. Е. Shibano, Е. В. Polikarpova, К. Е. Rumyantsev ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 211 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=499981> (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-9275-2716-8. – Текст : электронный.

3. Основы национальной безопасности : учебное пособие / Н. Д. Eriashvili, Е. Н. Hazov, Л. Т. Chikhladze и др. ; под ред. Е. Н. Hazova, Н. Д. Eriashvili. – Москва : Юнити, 2018. – 335 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=473285> (дата обращения: 23.08.2021). – Библиогр. в кн. – ISBN 978-5-238-03030-2. – Текст : электронный.

## 8.2 Дополнительная учебная литература

4. Чхартишвили, А. Г. Социальные сети: модели информационного влияния, управления и противоборства : [16+] / А. Г. Чхартишвили, Д. А. Губанов, Д. А. Новиков ; Российская Академия Наук, Институт проблем управления. – Москва : Физматлит, 2010. – 228 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=82767> (дата обращения: 23.08.2021). – ISBN 978-594052-194-5. – Текст : электронный.
5. Сулейманова Ш.С. Информационные войны: история и современность [Текст]: учебное пособие / Ш.С. Сулейманова. – М :Международный издательский центр «Этносоциум», 2017. – 124 с.
6. Аверченков В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М.: Флинта, 2016. - 269 с. –Режим доступа: <http://biblioclub.ru/index.php?page=book&id=93245>
7. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : <http://biblioclub.ru/index.php?page=book&id=276557>
8. Киселёв А. Г. Теория и практика массовой информации: общество - СМИ – власть [Электронный ресурс] :учебник / А. Г. Киселёв. – М.: Юнити-Дана, 2015. - 431 с. - ISBN 978-5-238-01742-6 - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=436719>.
9. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс]:/ Н.Н. Куняев. – М.: Логос, 2010. - 347 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=84990>
10. Мировойна. Все против всех: новейшие концепции боевых действий англосаксов [Электронный ресурс] : / М. С. Рогачев, В. В. Чеботарев ; сост. Е. С. Ларина, В. С. Овчинский. – М.: Книжный мир, 2015. - 416 с. - Режим доступа: <http://biblioclub.ru/index.php?page=book&id=445770> - в доп. лит.
11. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. // Режим доступа - <http://biblioclub.ru/index.php?page=book&id=90753>
12. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный

Открытый Университет «ИНТУИТ», 2016. - 425 с. // Режим доступа - <http://biblioclub.ru/index.php?page=book&id=429070>

13. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

### 8.3 Перечень методических указаний

1. История информационного противоборства: Методические указания по организации самостоятельной работы по дисциплине «История информационного противоборства» / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2024. – 7 с.: Библиогр.: с. 6.

2. История информационного противоборства: Методические указания по выполнению практических работ по дисциплине «История информационного противоборства» / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2024. – 24с.: Библиогр.: с. 15.

### 8.4 Другие учебно-методические материалы

#### Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца

2. Журнал «InformationSecurity/Информационная безопасность.»- <http://window.edu.ru/>

3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- <http://window.edu.ru/>

4. Журнал «Вестник УрФО. Безопасность в информационной сфере»

5. Журнал «Вопросы защиты информации»

6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»

7. Журнал «Информация и безопасность.»

### 9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://e.lanbook.com> - Электронно-библиотечная система «Лань».

2. <http://www.iqlib.ru> - Электронно-библиотечная система IQLib.

3. <http://window.edu.ru> -Электронная библиотека «Единое окно доступа к образовательным ресурсам».

4. <http://biblioclub.ru> – Электронно-библиотечная система «Университетская библиотека онлайн».
5. <http://www.fsb.ru> - Федеральная служба безопасности [официальный сайт].
6. <http://fstec.ru> - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. <http://microsoft.com> - Корпорация Microsoft [официальный сайт].
8. <http://www.consultant.ru> Компания «Консультант Плюс» [официальный сайт].

## **10. Методические указания для обучающихся по освоению дисциплины**

Основными видами аудиторной работы студента при изучении дисциплины «История информационного противоборства» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «История информационного противоборства»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу

на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «История информационного противоборства» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «История информационного противоборства» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

#### **11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.



## **12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aoc 21". Проекционный экран на штативе; Мультимедиацентр: ноутбук ASUS X50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проектор inFocus IN24+

## **13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

*Для лиц с нарушением слуха* возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

*Для лиц с нарушением зрения* допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

*Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата,* на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается

присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

**14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины**

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	Изменённых	Заменённых	Аннулированных	Новых			