

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Саратовский государственный технический университет  
имени Гагарина Ю.А.»  
Кафедра «Медиакоммуникации»

## **РАБОЧАЯ ПРОГРАММА**

**по дисциплине**

### ***Б.1.3.4.1 «Основы информационной безопасности»***

направления подготовки

42.03.04 «Телевидение»

Профиль «Техника и технология телевизионного производства»

квалификация – бакалавр

форма обучения – очная

курс – 4

семестр – 7

зачетных единиц – 3

часов в неделю – 2

всего часов – 108,

в том числе:

лекции – нет

коллоквиумы – нет

практические занятия – 36

лабораторные занятия – нет

самостоятельная работа – 72

зачет – 7 семестр

экзамен – нет

РГР – нет

курсовая работа – нет

курсовой проект – нет

## 1. Цели и задачи дисциплины

Учебный курс предназначен для бакалавров обучающихся по специальности «Телевидение». Учебный материал в доступной форме излагает основы информационной и библиографической культуры с учетом основных требований информационной безопасности; сущность и содержание основных понятий в сферах информационной безопасности и защиты информации; основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные методы и способы защиты информационных процессов в телекоммуникационных системах с учетом положений образовательной программы неюридического вуза.

В курсе представлен учебный, нормативный и методический материал, необходимый для изучения дисциплины «Основы информационной безопасности». Содержание учебной дисциплины соответствует программе курса «Основы информационной безопасности» и государственному образовательному стандарту для направления 42.03.04 «Телевидение».

Цель данного курса – изучение бакалаврами важнейших принципов и основ информационной и библиографической культуры с учетом основных требований информационной безопасности.

Задачи курса - овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты профессиональной информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения.

## 2. Место дисциплины в структуре ООП ВО

Дисциплина «Основы информационной безопасности» относится к дисциплинам по выбору направления подготовки «Телевидение».

Данная дисциплина находится в логической и содержательно-методической взаимосвязи с другими дисциплинами направления подготовки, такими как «Информационные технологии на телевидении и в СМИ», «Практикум по телевизионному производству», «Интернет-технологии» и др.

В свою очередь освоение дисциплины «Основы информационной безопасности» необходимо для изучения следующих дисциплин «Теория и практика телевидения», «Безопасность жизнедеятельности».

В результате освоения дисциплины «Основы информационной безопасности» бакалавр должен выработать знания, умения и навыки, связанные с применением информационной безопасности в профессиональной сфере.

## 3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК -6 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

В результате изучения дисциплины студент должен:

### **знать**

- основы информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

- сущность и содержание основных понятий в сферах информационной безопасности и защиты информации;
- основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- основные методы и способы защиты информационных процессов в телекоммуникационных системах.

**уметь**

- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять на практике нормативные правовые акты в области информационной безопасности и защиты информации.

**владеть**

- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
- высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности;
- способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации этих угроз;
- навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей деятельности.

**4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий**

№ Мо-ду-ля	№ Не-де-ли	№ Те-мы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лек-ции	Коллок-виумы	Лабораторные	Практические	СРС
1	2	3	4	5	6	7		8	9
1	1	1	Информационная безопасность в системе национальной безопасности	22				6	16
1	3	2	Государственная политика в области информационной безопасности	20				6	14

1	5	3	Угрозы информационной безопасности и их источники	22				8	14
1	6	4	Средства обеспечения информационной безопасности	22				8	14
1	7	5	Правовые методы обеспечения информационной безопасности	22				8	14
<b>Всего часов</b>				<b>108</b>				<b>36</b>	<b>72</b>

### 5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5

*Не предусмотрено учебным планом*

### 6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	2	3	4	5

*Не предусмотрено учебным планом*

### 7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4	5
1	6	1-3	<b>Информационная безопасность в системе национальной безопасности. Понятие безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Концепция информационной безопасности России. Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Определение и эволюция термина «информационная безопасность». Системные связи информационной безопасности с другими видами национальной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации,</b>	1-18

			информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года.	
2	6	4-6	<b>Государственная политика в области информационной безопасности.</b> Национальные интересы личности, общества и государства в информационной сфере. Государственные органы обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства.	1-18
3	8	7-10	<b>Угрозы информационной безопасности и их источники.</b> Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной безопасности.	1-18
4	8	11-14	<b>Средства обеспечения информационной безопасности.</b> Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.	1-18
5	8	15-18	<b>Правовые методы обеспечения информационной безопасности.</b> Правовое регулирование открытых информационных ресурсов. Правовая защита информационных ресурсов ограниченного доступа.	1-18

### 8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	4	3

Не предусмотрено учебным планом

### 9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
1	16	Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года.	1-18
2	14	Эссе на тему: «Государственная политика в области информационной безопасности».	1-18
3	14	Проанализируйте угрозы информационной на телевидении. Форма отчета – презентация.	1-18
4	14	Коллаж на тему: «Средства обеспечения информационной безопасности»	1-18
5	14	Проанализируйте правовые методы обеспечения информационной безопасности. Форма отчета – презентация.	1-18

#### **10. Расчетно-графическая работа**

*Не предусмотрено учебным планом*

#### **11. Курсовая работа**

*Не предусмотрено учебным планом*

#### **12. Курсовой проект**

*Не предусмотрено учебным планом*

### **13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)**

В процессе освоения образовательной программы у студента формируется следующие компетенции:

ОПК -6 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

№ пп	Название компетенции	Составляющие действия компетенции	Технологии формирования	Средства и технологии оценки
1	ОПК -6 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	<b>Знает</b> основы информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; сущность и содержание	Лекции Практические занятия	Тестирование

№ пп	Название компетенции	Составляющие действия компетенции	Технологии формирования	Средства и технологии оценки
	информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	основных понятий в сферах информационной безопасности и защиты информации; основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные методы и способы защиты информационных процессов в телекоммуникационных системах.		
		<b>Умеет</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта; применять на практике нормативные правовые акты в области информационной безопасности и защиты информации.	Лекции Практические занятия	Тестирование
		<b>Владеет</b> способностью решать стандартные задачи профессиональной деятельности на основе информационной и	Лекции Практические занятия	Тестирование

№ пп	Название компетенции	Составляющие действия компетенции	Технологии формирования	Средства и технологии оценки
		библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности; способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации этих угроз; навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей деятельности.		

### УРОВНИ ОСВОЕНИЯ КОМПЕТЕНЦИИ ОК-6

#### Наименование компетенций

ОК-6	<p>Формулировка:</p> <p>способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>
------	---

Ступени уровней освоения компетенций	Отличительные признаки
Пороговый (удовлетворительный)	<p><b>Знает</b> основы информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>сущность и содержание основных понятий в сферах информационной безопасности и защиты информации;</p> <p>основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России;</p> <p>место и роль информационной безопасности в системе национальной безопасности Российской Федерации.</p> <p><b>Умеет</b> решать стандартные задачи профессиональной</p>



	<p>деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p><b>Владеет</b> способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.</p>
<p>Продвинутый (хорошо)</p>	<p><b>Знает</b> основы информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>сущность и содержание основных понятий в сферах информационной безопасности и защиты информации;</p> <p>основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России;</p> <p>место и роль информационной безопасности в системе национальной безопасности Российской Федерации;</p> <p>основные нормативные правовые акты в области информационной безопасности и защиты информации.</p> <p><b>Умеет</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>анализировать и оценивать угрозы информационной безопасности объекта.</p> <p><b>Владеет</b> способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности;</p> <p>способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации этих угроз.</p>
<p>Высокий (отлично)</p>	<p><b>Знает</b> основы информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;</p> <p>сущность и содержание основных понятий в сферах информационной безопасности и защиты информации;</p> <p>основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России;</p> <p>место и роль информационной безопасности в системе национальной безопасности Российской Федерации;</p>

	<p>основные нормативные правовые акты в области информационной безопасности и защиты информации; основные методы и способы защиты информационных процессов в телекоммуникационных системах.</p> <p><b>Умеет</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта;</p> <p>применять на практике нормативные правовые акты в области информационной безопасности и защиты информации.</p> <p><b>Владеет</b> способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности;</p> <p>способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации этих угроз;</p> <p>навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей деятельности.</p>
--	---

Для определения достигнутой обучающимся степени освоения материала используется система тестов, устных опросов и практических заданий, выполняемых как на занятии, так и самостоятельно.

**Шкала оценивания результатов:**

- неудовлетворительно – 0 – 30%
- удовлетворительно – 31 – 60%
- хорошо – 61 – 85%
- отлично – 86 – 100%

**Организация и проведение межсессионной аттестации студентов**

Межсессионная аттестация представляет собой важнейшее средство, обеспечивающее преподавателю обратную связь, которая является руководством в выборе методов, форм и приемов преподавания, ориентируя на уровень знаний и умений конкретной группы. Это также и способ самоконтроля как учебное действие самого студента, который должен заботиться о том, чтобы не накапливать неотработанные лекции и семинары, непочитанные тексты учебной и научной литературы, а также задания для самостоятельной работы, не откладывая усвоение пропущенного материала и выполнения курсовой работы до сессии.

**Основными задачами аттестации являются:**

- промежуточная проверка качества (глубины) усвоения студентом пройденного учебного материала;

- контроль ритмичности работы студентов в течение семестра;

- упорядочение самостоятельной работы студентов;

- планирование основных корректирующих мер по преодолению обнаруженных недостатков и умножению достигнутых успехов в обучении, изучение и распространение положительного опыта организации учебной деятельности, эффективных приемов и методов преподавания, организации самостоятельной работы студента.

Конечной **целью** контроля учебной деятельности студентов является улучшение общей профессиональной подготовки специалистов.

Аттестацию студента проводят преподаватели, осуществляющие в Институте соответствующие виды учебной деятельности: лекционные и практические занятия, руководство курсовыми работами.

При межсессионной аттестации студента учитываются:

1) посещаемость студентом лекций и практических занятий;

2) текущая успеваемость студента.

Основными критериями ее оценки являются:

а) активность участия студентов в практических занятиях и коллоквиумах;

б) уровень знаний, умений и навыков, продемонстрированных студентом на практических занятиях;

в) результаты выполнения письменных контрольных и самостоятельных работ, тестов, эссе и т. п.;

г) систематичность работы над курсовой работой (курсовым проектом);

д) степень выполнения индивидуальных заданий по данной дисциплине.

По решению учебно-методической комиссии кафедры эти критерии могут быть расширены и дополнены.

Контроль текущей успеваемости и качества знаний студента осуществляется преподавателями, за которыми закреплены дисциплины учебного плана, посредством выставления оценок на основании федерального государственного образовательного стандарта по направлению (42.03.04 «Телевидение») и рабочей программы по аттестуемой дисциплине.

Объектом оценивания являются основные компоненты учебного процесса, которые включают в себя: учебную дисциплину (мотивацию студента, его активность при получении знаний, своевременное прохождение контрольных мероприятий),

посещаемость занятий студентом, степень усвоения им теоретических знаний, уровень овладения практическими умениями и навыками во всех видах учебной деятельности, его способность к самостоятельной научно-исследовательской работе и др. К концу второй недели межсессионного контроля студенты должны выполнить все запланированные на данный период контрольные мероприятия (коллоквиумы, защита лабораторных работ, сдача контрольных, защита курсовых работ, рефератов, выступления студентов с докладами, сообщениями, проектами на практических (семинарских) занятиях, тестирование студентов и т.д.).

В период проведения межсессионного контроля преподаватель, за которым закреплены дисциплины учебного плана, вправе применить различные формы контроля качества знаний, умений и навыков студентов.

Межсессионная аттестация проводится в разнообразных формах (контрольная работа, диктант, тестирование, компьютерный контроль по отдельным разделам и темам учебных программ, написание и защита реферата, творческие работы, составление библиографии, подготовка докладов и выступление с ними, оформление альбомов, разработка конспектов, планирование отдельных направлений учебной, научной, исследовательской деятельности, компьютерная презентация материалов и т.п.), отражающих специфику учебной деятельности кафедры «Медиакоммуникации».

Виды заданий для проведения межсессионной аттестации студентов, их содержание и характер имеют вариативный и дифференцированный характер, учитывая специфику данной дисциплины, индивидуальные особенности студента.

Межсессионная аттестация студентов, обучающихся по всем направления очной формы по данной дисциплине, проводится 1 раз в семестр. Межсессионный контроль оценивается по шкале: "аттестован", "неаттестован". Результаты аттестации проставляются в ведомость, которая находится в дирекции института.

#### **Вопросы для зачета**

1. Понятие безопасности. Национальная безопасность.
2. Доктрина безопасности Российской Федерации.
3. Концепция информационной безопасности России.
4. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
5. Виды национальной безопасности и их краткая характеристика.
6. Определение и эволюция термина «информационная безопасность».
7. Системные связи информационной безопасности с другими видами национальной безопасности.
8. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации.
9. Обзор российского законодательства в сфере информационных технологий.

10. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ.
11. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года.
12. Национальные интересы личности, общества и государства в информационной сфере. Государственные органы обеспечения информационной безопасности.
13. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства.
14. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
15. Угрозы конфиденциальности, целостности и доступности информации.
16. Системная классификация угроз.
17. Информационная война как высшая форма угрозы информационной безопасности.
18. Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности.
19. Пассивные и активные средства противодействия техническим разведкам.
20. Защита информации от утечки по техническим каналам.
21. Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности.
22. Пассивные и активные средства противодействия техническим разведкам.
23. Защита информации от утечки по техническим каналам.
24. Правовое регулирование открытых информационных ресурсов.
25. Правовая защита информационных ресурсов ограниченного доступа.

### **Вопросы для экзамена**

Не предусмотрено учебным планом

### **Тестовые задания по дисциплине**

**1. В каком правовом документе дается определение термина «информационная безопасность»?**

- а) Федеральный закон «О безопасности».
- б) Стратегия национальной безопасности Российской Федерации до 2020 года.
- в) Доктрина информационной безопасности Российской Федерации.
- г) Конституция.
- д) Федеральный закон «Об информации, информационных технологиях и о защите информации».

**2. Основными аспектами деятельности (задачами) информационной безопасности выступают –**

- а) Конфиденциальность.
- б) Доступность.
- в) Системность.
- г) Целостность.
- д) Защита информации.

**3. Постройте соответствие между методами защиты информации (левая колонка) и их характеристиками (правая колонка):**

1. Правовые методы	А. Подбор сотрудников компании, а также обеспечение того, чтобы непроверенные лица не допускались к охраняемой информации
2. Программный метод	В. Разработка нормативных актов, подразумевающих административную и уголовную ответственность за хищение информации, нарушение авторских прав программистов и киберпреступления
3. Программно-аппаратный метод	С. Использование антивирусных программ и пассивной защиты (брандмауэр, файрвол и т.п.)
4. Физические методы	Д. Изготовление аппаратных средств защиты информации, например, сетевых адаптеров в памяти которого встроена антивирусная программа
5. Организационные методы	Е. Включает в себя защиту кабельных систем, использование всевозможных источников бесперебойного питания, защиту помещений от постороннего доступа, резервное копирование информации
6. Административные методы	Ф. Формирование политики информационной безопасности компании

**4. Что представляет собой доктрина информационной безопасности РФ?**

- а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
- б) федеральный закон, регулирующий правоотношения в области информационной безопасности;
- в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;
- г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

**5. Какие из перечисленных ниже угроз относятся к классу преднамеренных?**

- а) заражение компьютера вирусами;
- б) физическое разрушение системы в результате пожара;
- в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- е) вскрытие шифров криптозащиты информации.

**6. Основные нормы по защите интеллектуальной собственности содержатся в следующих нормативно-правовых актах:**

- а) об авторском праве и смежных правах;
- б) патентный закон РФ;
- в) ч. 4 ГК РФ;
- г) о товарных знаках и знаках обслуживания;

д) о правовой охране программ для ЭВМ и баз данных.

**7. Требуется ли на основании закона «О персональных данных» согласие субъекта на обработку персональных данных в целях использования договора, одной из сторон которого является субъект персональных данных:**

- а) да;
- б) на основании дополнительного согласия;
- в) нет.

**8. К основным видам обеспечения информационной безопасности относятся:**

- а) нормативно-правовое, инженерно-техническое и административно-организационное;
- б) нормативно-правовое, материально-техническое и методологическое;
- в) методологическое, правовое и психологическое;
- г) нет правильных вариантов ответа.

**9. Сложность обеспечения информационной безопасности является следствием:**

- а) комплексного характера данной проблемы, требующей для своего решения привлечения специалистов разного профиля;
- б) наличия многочисленных высококвалифицированных злоумышленников;
- в) развития глобальных компьютерных сетей;
- г) злого умысла разработчиков информационных систем.

**10. Самыми опасными источниками угроз являются:**

- а) внутренние;
- б) внешние;
- в) пограничные;
- г) вирусные инфекции;
- д) атаки хакеров.

## 14. Образовательные технологии

Чтение лекций осуществляется с использованием компьютерных презентаций. В ходе лекционных и практических занятий используется мультимедийное оборудование (компьютер, интерактивная доска и проектор).

Практические занятия направлены на углубление научно-теоретических знаний и овладение определенными методами самостоятельной работы, которое формирует практические умения. Перед практическим занятием следует изучить конспект лекции и рекомендованную преподавателем литературу.

В процессе обучения широко используются такие активные и интерактивные формы занятий, как тематические дискуссии, мозговая атака, презентации, ситуативные симуляции, ролевые игры. Предусмотрены мастер-классы с практикующими специалистами.

Методы интерактивной образовательной деятельности:

*Работа в команде* – совместная деятельность студентов в группе под руководством лидера, направленная на разработку технического задания.

*Проблемное обучение* – стимулирование студентов к получению знаний, необходимых для решения конкретной проблемы, возникающей в процессе разработки.

*Эссе* (франц. *essai* – попытка, проба, очерк, от лат. *exagium* – взвешивание) – письменная работа небольшого объема и свободной композиции. Эссе выражает индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендует на определяющую или исчерпывающую трактовку предмета. Как правило, эссе предполагает новое, субъективно окрашенное мнение о чем-либо и может иметь философский, историко-биографический, публицистический, литературно-критический, научно-популярный или чисто беллетристический характер. Стиль эссе

отличается образностью, афористичностью и установкой на разговорную интонацию и лексику.

*Самостоятельное исследование* – развивает самостоятельность мышления, способность к самоорганизации, созиданию, сотрудничеству, оказывает существенное влияние на личностно – профессиональное становление, создает высокую мотивацию познавательной деятельности, формирует черты творческой личности. Данная деятельность обеспечивает успешную адаптацию и самореализацию человека в обществе.

*Кейс-метод* – его название происходит от английского слова «кейс» - папка, чемодан, портфель (в то же время, «кейс» можно перевести и как «случай, ситуация»). Процесс обучения с использованием кейс-метода представляет собой имитацию реального события, сочетающую в целом адекватное отражение реальной действительности, небольшие материальные и временные затраты и вариативность обучения. Учебный материал подается студентам в виде проблем (кейсов), а знания приобретаются в результате активной и творческой работы: самостоятельного осуществления целеполагания, сбора необходимой информации, ее анализа с разных точек зрения, выдвижения гипотезы, выводов, заключения, самоконтроля процесса получения знаний и его результатов.

Удельный вес занятий, проводимых в интерактивных формах, составляет порядка 50 %.

## **15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

### **Основная литература**

1. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс]: учебное пособие/ Коваленко Ю.И. - Электрон. текстовые данные. - М.: Горячая линия - Телеком, 2012. - 140 с. - Режим доступа: <http://www.iprbookshop.ru/12026>. - ЭБС «IPRbooks», по паролю

2. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.]. - Электрон. текстовые данные. - М.: Горячая линия - Телеком, 2011. - 558 с. - Режим доступа: <http://www.iprbookshop.ru/12014>. - ЭБС «IPRbooks», по паролю

3. Симонович, С. В. Информатика : базовый курс : учеб. пособие / под ред. С. В. Симоновича. - 2-е изд. - СПб. [и др.] : Питер, 2010. - 640 с. : ил. ; 24см. - (Учебник для вузов). - Гриф: рек. М-вом образования РФ в качестве учеб. пособия для студ. вузов. - ISBN 978-5-94723-752-8. Б.ц. Всего 51 экземпляров.

### **Дополнительная литература**

4. Куприянов, А. И. Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. - ISBN 978-5-7695-5761-3. - Б.ц. Всего 22 экземпляра.

5. Мельников, В.П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : ИЦ "Академия", 2006. - 336 с. - ISBN 5-7695-2592-4- Б.ц. Всего 13 экземпляров.

6. Михайлов, Л.А. Основы национальной безопасности : учеб. пособие / Л. А. Михайлов [и др.]. - М. : ИЦ "Академия", 2008. - 176 с. ; 22 см. - ISBN 978-5-7695-5373-8 – Б.ц. Всего 20 экземпляров.

7. Основы информационной безопасности : учеб. пособие / С. П. Расторгуев. - М. : ИЦ "Академия", 2007. - 192 с. - ISBN 978-5-7695-3098-2 - Б.ц. Всего 8 экземпляров



8. Правовое обеспечение информационной безопасности : учеб. пособие / С. Я. Казанцев [и др.] ; под ред. С. Я. Казанцева. - 3-е изд., стер. - М. : ИЦ "Академия", 2008. - 240 с. - ISBN 978-5-7695-5103-1. - Б.ц. Всего 9 экземпляров.

9. Романов, О.А. Организационное обеспечение информационной безопасности : учеб. / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : ИЦ "Академия", 2008. - 192 с. - ISBN 978-5-7695-4272-5. - Б.ц. Всего 4 экземпляра.

10. Организационно-правовое обеспечение информационной безопасности : учеб. пособие / А. А. Стрельцов [и др.] ; под ред. А. А. Стрельцова. - М. : ИЦ "Академия", 2008. ISBN 978-5-7695-4240-4 : 267.96. Всего 9 экземпляров.

#### **Периодические издания**

11. Инновационная деятельность: научно-аналит. журнал/ Саратов: СГТУ имени Гагарина Ю.А., (архив 2009-2015), № 1-4. - ISSN 2071-5226

#### **Интернет-источники**

12. <http://base.consultant.ru/> – правовая база «Консультант Плюс»

13. <http://www.cyberpolice.ru> (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)

14. <http://www.garant.ru/> – информационно-правовой портал «Гарант»

15. <http://www.infosec.ru/> (Сервер компании НИП «Информзащита»)

16. <http://www.infosecurity.report.ru/> (портал по информационной безопасности)

17. <http://www.jetinfo.ru/> (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)

18. <http://www.void.ru/> (портал по информационной безопасности)

#### **Источники ИОС**

19. Информационно-образовательная среда [Электронный ресурс] Режим доступа <https://portal3.sstu.ru/Facult/MFPIT/MFPIT-RKD/TLVD/B.1.3.4.1/default.aspx>

#### **16. Материально-техническое обеспечение**

Для проведения практических занятий используются аудитория, оснащенная компьютером с выходом в Интернет, системные требования: Intel Core 2 Quad Q9400 2.66Ghz/4Gb/300Gb/2Gb Nvidia GeForce 9600 GT. Программное обеспечение: Windows 7, Adobe Master Collection CS6, Corel Draw X4, MS Office 2007, Антивирус Kaspersky Endpoint 8; Intel Quad Core Q9400,2.66Ghz/4Gb/300Gb/2286Mb/Nvidia GeForce 9600 GT. Программное обеспечение: Windows 7, Adobe Msater Collection CS4, Corel Draw X4, MS Office 2007, Антивирус Kaspersky Endpoint 8

Студенты имеют доступ к электронно-библиотечным системам, а также доступ к информационно-образовательной среде СГТУ.

Рабочую программу составил(а) \_\_\_\_\_/\_\_\_\_\_