


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«История защиты информации»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределенных компьютерных систем

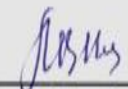
Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы

 /Л.В. Паринава/

Заведующий кафедрой
Систем информационной
безопасности

 / А.Г. Остапенко /

Руководитель ОПОП

 / А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Цель дисциплины - формирование у студентов знаний об этапах развития систем защиты информации, а также о службах и системах защиты информации России и ведущих зарубежных стран.

1.2. Задачи освоения дисциплины

Задачами освоения дисциплины является изучение:

- состава защищаемой информации на различных этапах развития России и зарубежных стран;
- классификации защищаемой информации в различные исторические периоды по видам тайны, собственнику и др.;
- структуры угроз защищаемой информации в различные исторические периоды;
- каналов несанкционированного доступа к защищаемой информации, методов ее добывания в различные исторические периоды;
- государственной политики в области защиты информации;
- процессов развития и совершенствования нормативной базы по защите информации;
- состава органов защиты информации в различные периоды развития системы защиты информации;
- направлений и методов защиты информации;
- факторов, определяющих современную систему защиты информации и тенденции ее развития.
- процесса формирования и развития систем защиты информации;
- понятийного аппарата в области защиты информации;
- особенностей и направлений международного сотрудничества в данной области.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «История защиты информации» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «История защиты информации» направлен на формирование следующих компетенций:

ОК-3-способность анализировать основные этапы закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма

ОК-5-способность понимать социальную значимость своей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

ПК-1-способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного

ого опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОК-3	<p>знать особенности процесса становления, развития и современной организации системы защиты информации; состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды;</p> <p>уметь применять полученные знания в научно-исследовательской и практической работе</p> <p>владеть навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений</p>
ОК-5	<p>знать исторические периоды формирования системы защиты информации в России; принципы формирования систем защиты информации России на разных исторических этапах</p> <p>уметь определять источники и предпосылки происхождения существующих нормативно-правовых актов;</p> <p>владеть навыками использования исторических источников в повседневной деятельности.</p>
ПК-1	<p>Знать основные направления государственной политики в области защиты информации; состав, структуру и основные направления деятельности органов защиты информации; особенности формирования и развития нормативной базы защиты информации.</p> <p>Уметь выявлять возможные перспективы развития системы защиты информации в России, анализируя текущее её состояние.</p> <p>Владеть навыками использования исторических источников.</p>

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «История защиты информации» составляет 63 е.

**Распределение трудоемкости дисциплины по видам занятий
очная форма обучения**

Виды учебной работы	Всего часов	Семестры	
		1	2
Аудиторные занятия (всего)	72	36	36
В том числе:			
Лекции	72	36	36
Самостоятельная работа	108	54	54
Курсовая работа	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач. ед.	216 6	90 2.5	126 3.5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	СРС	Всего, час
1	Развития систем защиты информации России в IX-XX веках	Введение. Формирование системы защиты информации в России. Формирование системы защиты информации в России в XVII веке. Организация защиты информации в Российской империи в XVIII, в военной области. Организация защиты информации в XVIII веке, в государственных коллегиях. Центральные органы власти и управления. Коллегии. Эволюция системы коллегий. Генеральный регламент. Работа коллегий. Значение коллегий. Минусы в работе коллегий. Органы защиты информации XVIII века. Местные органы управления. Армия. Следственные органы. Законодательство.	12	18	30
2	Задачи и основные направления в области защиты информации Собственной Канцелярии и система защиты информации начала XIX века.	Задачи и направления деятельности Собственной Канцелярии. История. Первое отделение. Второе отделение. Третье отделение. Четвёртое отделение. Пятое отделение. Шестое отделение. Защита информации начала XIX века. Государственный аппарат. Военное министерство.	12	18	30
3	Организация защиты информации в XIX веке	Направления деятельности учреждений по защите информации. Организация спецслужб. Военное министерство. Цензура. Организация секретного делопроизводства в Российской Империи в XIX веке. Департамент полиции. Структура министерства иностранных дел. Военное министерство.	12	18	30
4	Вопросы защиты тайны в конце XIX — начале XX века	Защита государственной и коммерческой тайны. История создания уложения. Организационно-технические мероприятия по защите коммерческой тайны. Организация защиты информации в	12	18	30

		МИДе. Перечень сведений в области защиты государственной тайны. Криптографические методы защиты информации. Уголовное уложение. Организация контрразведывательной службы. Организация криптографической связи. Организация фельдъегерской связи. Военная цензура. Органы разведывательной и контрразведывательной деятельности Состав и направления деятельности органов защиты информации в СССР			
5	Современные системы и службы защиты информации России и ведущих зарубежных стран.	Современная нормативная база защиты информации. Современная нормативно-правовая база защиты информации в России. Правовые условия защиты различных видов информации. Режимы защиты информации. Режим защиты государственной тайны. Защита служебной тайны. Защита профессиональной тайны. Защита коммерческой и банковской тайны. Защита персональных данных.	12	18	30
6	Система засекречивания и классификация защищаемой информации в современных условиях	Система засекречивания и классификация защищаемой информации в современных условиях. Защищаемая информация и её классификация. Засекречивание и рассекречивание информации. Перечень сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне. Порядок засекречивания сведений и их носителей. Спецслужбы стран мира.	12	18	30
Итого			72	108	180

5.2 Перечень лабораторных работ

Непредусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы в 2 семестре для очной формы обучения.

Примерная тематика курсовой работы: «Анализ развития понятия защиты информации в России»

Задачи, решаемые при выполнении курсовой работы:

- рассмотрение специфики правового обеспечения информационной безопасности;
- изучение моделей закона об информационной безопасности;
- проведение анализа особенностей правового обеспечения информационной безопасности органов государственной власти.

Курсовая работа включает в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются в следующей системе:

«аттестован»;

«неаттестован».

Компе-	Результаты обучения, характеризующие	Критерии	Аттестован	Неаттестован
--------	--------------------------------------	----------	------------	--------------

тенция	сформированность компетенции	оценивания		
ОК-3	знать особенности процесса становления, развития и современной организации системы защиты информации; состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды;	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять полученные знания в научно-исследовательской и практической работе	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОК-5	знать исторические периоды формирования системы защиты информации в России; принципы формирования систем защиты информации России на разных исторических этапах	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять источники и предпосылки происхождения существующих нормативно-правовых актов;	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками использования исторических источников в повседневной деятельности.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-1	Знать основные направления государственной политики в области защиты информации; состав, структуру и основные направления деятельности органов защиты информации; особенности формирования и развития нормативной базы защиты информации.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь выявлять возможные перспективы развития	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный в

	системы защиты информации в России, анализируя текущее её состояние.		рабочих программах	рабочих программах
	Владеть навыками использования исторических источников.	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 1,2 семестре в очной форме обучения по двух/четырёхбалльной системе:

«зачтено»

«незачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Незачтено
ОК-3	знать особенности процесса становления, развития и современной организации системы защиты информации; состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять полученные знания в научно-исследовательской и практической работе	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОК-5	знать исторические периоды формирования системы защиты информации в России; принципы формирования систем защиты информации России на разных исторических этапах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь определять источники и предпосылки происхождения существующих нормативно-правовых актов;	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками использования исторических источников в	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	повседневной деятельности.			
ПК-1	Знать основные направления государственной политики в области защиты информации; состав, структуру и основные направления деятельности органов защиты информации; особенности формирования и развития нормативной базы защиты информации.	Тест	Выполнение тестов 70-100%	Выполнение менее 70%
	Уметь выявлять возможные перспективы развития системы защиты информации в России, анализируя текущее её состояние.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	Владеть навыками использования исторических источников.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи решены

ИЛИ

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОК-3	знать особенности процесса становления, развития и современной организации системы защиты информации; состав, особенности классификации, структуру угроз защищаемой информации в различные исторические периоды;	Тест	Выполнение тестов 90-100%	Выполнение тестов 80-90%	Выполнение тестов 70-80%	В тесте менее 70% правильных ответов
	уметь применять полученные знания в научно-исследовательской и практической работе	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	владеть навыками публичной речи, аргументации,	Решение прикладных задач в конкретной	Задачи решены в полном объеме и	Продемонстрирован верный ход решения всех, но не	Продемонстрирован верный ход решения в	Задачи решены

	ведения дискуссии и полемики, практического анализа логики различного рода рассуждений	предметной области	получены верные ответы	получен верный ответ во всех задачах	большинстве задач	
ОК-5	знать исторические периоды формирования системы защиты информации в России; принципы формирования систем защиты информации России на разных исторических этапа	Тест	Выполнение тестана 90-100%	Выполнение тестана 80-90%	Выполнение тестана 70-80%	В тесте менее 70% правильных ответов
	уметь определять источники и предпосылки происхождения существующих нормативно-правовых актов;	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	владеть навыками использования исторических источников в повседневной деятельности.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
ПК-1	Знать основные направления государственной политики в области защиты информации; состав, структуру и основные направления деятельности органов защиты информации; особенности формирования и развития нормативной базы защиты информации.	Тест	Выполнение тестана 90-100%	Выполнение тестана 80-90%	Выполнение тестана 70-80%	В тесте менее 70% правильных ответов
	Уметь выявлять возможные перспективы развития системы защиты информации в России, анализируя текущее её состояние.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	Владеть навыками использования исторических источников.	Решение прикладных задач в конкретной	Задачи решены в полном объеме и	Продемонстрирован верный ход решения всех, но не	Продемонстрирован верный ход решения в	Задачи решены

		предметной области	получены верные ответы	получен верный ответ во всех задачах	большинстве задач	
--	--	--------------------	------------------------	--------------------------------------	-------------------	--

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?

Информационная защита информации

Информационная безопасность

Защита информации

Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

Препятствие

Управление доступом

Маскировка

Какой метод защиты информации связан с регулированием использования всех ресурсов информационной системы?

Маскировка

Препятствие

Управление доступом

Как называется установления подлинности объекта по предъявленному им идентификатору (имени)?

Аутентификация

Идентификация

Маскировка

Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?

Аутентификация

Идентификация

Маскировка

При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

Принуждение

Маскировка

Идентификация

Какой метод защиты информации мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм?

Принуждение

Побуждение

Маскировка

Какие средства защиты информации предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации?

Аппаратные
Программные
Физические

Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?

Аппаратные
Программные
Физические

Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

Аппаратные
Программные
Физические

7.2.2 Примерный перечень заданий для решения стандартных задач

Какие средства защиты информации регламентируют правила использования, обработки и передачи информации и устанавливают меры ответственности?

Законодательные средства
Организационные средства
Аппаратно-программные

Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?

Аппаратные
Программные
Физические

Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

Аппаратные
Программные
Физические

Как называются правила и нормы поведения сотрудников в коллективе, регулирующие вопросы защиты информации?

Организационные средства
Аппаратно-программные
Морально-этические средства

Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?

Информационная защита информации
Информационная безопасность
Защита информации

Как называется метод физического преграждения пути злоумышленнику к защищаемой

информации (сигнализация, замки и т.д.)?

Препятствие

Управление доступом

Маскировка

Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?

Аутентификация

Идентификация

Маскировка

При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

Принуждение

Маскировка

Идентификация

Какие средства защиты информации связаны применением инструментов шифрования?

Организационные средства

Аппаратно-программные

Криптографические средства

К каким средствам защиты информации относятся мероприятия, регламентирующие поведение сотрудника организации?

Организационные средства

Аппаратно-программные

Криптографические средства

7.2.3 Примерный перечень заданий для решения прикладных задач

Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

Руководитель среднего звена

Высшее руководство

Владелец

Пользователь

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

Сотрудники

Хакеры

Атакующие

Контрагенты (лица, работающие по договору)

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

Улучшить контроль за безопасностью этой информации

Снизить уровень классификации этой информации

Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

Необходимый уровень доступности, целостности и конфиденциальности

Оценить уровень риска и отменить контрмеры

Управление доступом, которое должно защищать данные

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

Владельцы данных

Пользователи

Администраторы

Руководство

Что такое процедура?

Варианты ответа:

Правила использования программного и аппаратного обеспечения в компании

Пошаговая инструкция по выполнению задачи

Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

Обязательные действия

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Варианты ответа:

Поддержка высшего руководства

Эффективные защитные меры и методы их внедрения

Актуальные и адекватные политики и процедуры безопасности

Проведение тренингов по безопасности для всех сотрудников

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Варианты ответа:

Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

Когда риски не могут быть приняты во внимание по политическим соображениям

Когда необходимые защитные меры слишком сложны

Когда стоимость контрмер превышает ценность актива и потенциальные потери

Что такое политики безопасности?

Варианты ответа:

Пошаговые инструкции по выполнению задач безопасности

Общие руководящие требования по достижению определенного уровня безопасности

Широкие, высокоуровневые заявления руководства

Детализированные документы по обработке инцидентов безопасности

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

Варианты ответа:

Анализ рисков

Анализ затрат / выгоды

Результаты ALE

Выявление уязвимостей и угроз, являющихся причиной риска

7.2.4 Примерный перечень вопросов для подготовки к зачету

Образование государственных коллегий. Защита информации в

государственных органах XVIII век.

Задачи и цели Собственной Канцелярии. Структура системы защиты информации на начало XIX века.

Общие изменения в системе защиты информации к концу XIX века. Цели и задачи секретного делопроизводства.

Особенности защиты информации начала XX века.

Особенности системы защиты информации СССР.

Направления деятельности Гостехкомиссии и ФСТЭК.

Состав современной нормативно-правовой базы защиты информации.

Системы и службы защиты информации в ведущих зарубежных странах.

7.2.5 Примерный перечень заданий для решения прикладных задач

– предпосылки формирования системы защиты информации в России (вторая половина XVI - XVIII в.в.)

– организация защиты информации в Российской Империи в XVIII в.

– Совершенствование организации защиты информации в первой половине XIX в.

– формирование системы защиты информации во второй половине XIX в.

– Особенности системы защиты информации в начале XX в (1900-1908 г.г.)

– организация защиты информации в период промышленного подъема (1909-1913 г.г.)

– организация защиты информации в период Первой мировой войны

– достоинства и недостатки системы защиты информации в Российской империи

– основные особенности организации защиты информации в советский период

– организация защиты военной тайны в годы гражданской войны

– становление системы защиты государственных секретов в

– период НЭПа

– развитие системы защиты государственных секретов в 30-е г.г.

– укрепление системы защиты государственных секретов накануне

и в период Великой Отечественной войны

– совершенствование системы защиты государственных секретов во второй половине 40-х - первой половине 50-х г.г.

– организация защиты государственных секретов во второй половине 50-х - 60-х г.г.

– обеспечение защиты информации в 70х - 80-х г.г.

– основные особенности организации защиты информации на современном этапе.

7.2.6. Методика выставления оценки при проведении промежуточной

аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов по задаче. Каждый правильный ответ на вопрос тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов за верно решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Развития систем защиты информации России в IX-XX веках	ОК-3, ОК-5, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	Задачи и основные направления в области защиты информации Собственной Канцелярии и система защиты информации начала XIX века.	ОК-3, ОК-5, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	Организация защиты информации в 19 веке	ОК-3, ОК-5, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	Вопросы защиты тайны в конце XIX — начале XX века	ОК-3, ОК-5, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	Современные системы и службы защиты информации России и ведущих зарубежных стран.	ОК-3, ОК-5, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	Система засекречивания и классификация защищаемой информации в современных условиях	ОК-3, ОК-5, ПК-1	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методике выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практики осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНОМЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Укажите учебную литературу

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Укажите перечень информационных технологий

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Укажите материально-техническую базу

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «История защиты информации» читаются лекции, выполняются курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны свое временно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: <ul style="list-style-type: none"> - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.